Eiropas Savienības
Padome

Briselē, 2016. gada 21. aprīlī
(OR. en)

5581/16

Starpiestāžu lieta:
2013/0027 (COD)

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84

LEĢISLATĪVIE AKTI UN CITI DOKUMENTI

Temats:	Padomes nostāja pirmajā lasījumā, lai pieņemtu EIROPAS PARLAMENTA UN PADOMES DIREKTĪVU par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā

EIROPAS PARLAMENTA UN PADOMES
DIREKTĪVA (ES) 2016/...

(... gada ...)

par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

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

saskaņā ar parasto likumdošanas procedūru[2],

[1] OV C 271., 19.9.2013., 133. lpp.

[2] Eiropas Parlamenta 2014. gada 13. marta nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes ... nostāja pirmajā lasījumā (*Oficiālajā Vēstnesī* vēl nav publicēta). Eiropas Parlamenta … nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta).

tā kā:

(1) Tīklu un informācijas sistēmām un pakalpojumiem ir liela nozīme sabiedrībā. To uzticamība un drošība ir būtiska ekonomiskās un sabiedriskās darbībās un jo īpaši iekšējā tirgus darbībā.

(2) Drošības incidentu apmērs, biežums un ietekme pieaug un rada būtiskus draudus tīklu un informācijas sistēmu darbībai. Minētās sistēmas var arī kļūt par mērķi tīšām kaitnieciskām darbībām, kas vērstas uz sistēmu darbības bojāšanu vai apturēšanu. Šādi incidenti var kavēt ekonomisku darbību veikšanu, radīt ievērojamus finansiālus zaudējumus, apdraudēt lietotāju uzticēšanos un radīt lielu kaitējumu Savienības ekonomikai.

(3) Tīklu un informācijas sistēmām un galvenokārt internetam ir būtiska nozīme, veicinot preču un pakalpojumu brīvu apriti un personu brīvu pārvietošanos pāri robežām. Minētā transnacionālā rakstura dēļ šo sistēmu būtiski traucējumi neatkarīgi no tā, vai tie ir tīši vai netīši un kur tie notiek, var ietekmēt dalībvalstis atsevišķi un Savienību kopumā. Tāpēc tīklu un informācijas sistēmu drošībai ir būtiska nozīme iekšējā tirgus netraucētas darbības nodrošināšanā.

(4) Balstoties uz Dalībvalstu Eiropas forumā panākto ievērojamo progresu diskusiju un politikas paraugprakses apmaiņas veicināšanā, tostarp principu izstrādē attiecībā uz Eiropas sadarbību kiberkrīžu jomā, būtu jāizveido sadarbības grupa, kurā darbotos dalībvalstu pārstāvji, Komisija un Eiropas Savienības Tīklu un informācijas drošības aģentūra (*ENISA*), lai atbalstītu un sekmētu stratēģisku sadarbību starp dalībvalstīm attiecībā uz tīklu un informācijas sistēmu drošību. Lai minētā grupa būtu efektīva un iekļaujoša, ir svarīgi, lai visām dalībvalstīm būtu minimālās spējas un stratēģija, kas nodrošina augsta līmeņa tīklu un informācijas sistēmu drošību to teritorijā. Turklāt drošības un paziņošanas prasības būtu jāattiecina uz pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, lai veicinātu riska pārvaldības kultūru un nodrošinātu ziņošanu par nopietnākajiem incidentiem.

(5) Esošās spējas nav pietiekamas, lai Savienībā nodrošinātu augsta līmeņa tīklu un informācijas sistēmu drošību. Dalībvalstīm ir ļoti atšķirīgu līmeņu sagatavotība, kas novedis pie tā, ka Eiropas Savienībā pastāv atšķirīgas pieejas. Tā rezultātā Savienībā rodas nevienlīdzīgs patērētāju un uzņēmumu aizsardzības līmenis un tiek pazemināts tīklu un informācijas sistēmu drošības kopējais līmenis. Savukārt kopīgu prasību trūkums saistībā ar pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem padara neiespējamu efektīva vispārēja sadarbības mehānisma izveidi Savienības līmenī. Minēto jomu pētniecības, izstrādes un inovācijas stimulēšanā izšķiroša nozīme ir augstskolām un pētniecības centriem.

(6) Tāpēc, lai efektīvi reaģētu uz tīklu un informācijas sistēmu drošības problēmām, ir nepieciešama Savienības līmeņa vispārēja pieeja, kurā iekļautas kopīgas minimālās prasības attiecībā uz spēju veidošanu un plānošanu, informācijas apmaiņa, sadarbība un kopīgas drošības prasības pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem. Tomēr pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem netiek liegts īstenot drošības pasākumus, kas ir stingrāki nekā šajā direktīvā paredzētie.

(7) Lai aptvertu visus attiecīgos incidentus un riskus, šī direktīva būtu jāpiemēro gan pamatpakalpojumu sniedzējiem, gan digitālo pakalpojumu sniedzējiem. Tomēr pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju pienākumi nebūtu jāattiecina uz uzņēmumiem, kas nodrošina publisko komunikāciju tīklus vai sniedz publiski pieejamus elektronisko komunikāciju pakalpojumus Eiropas Parlamenta un Padomes Direktīvas 2002/21/EK[1] nozīmē, uz kuriem attiecas īpašas drošības un integritātes prasības, kas noteiktas minētajā direktīvā, un minētie pienākumi nebūtu jāattiecina arī uz uzticamības pakalpojumu sniedzējiem Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 [2] nozīmē, uz kuriem attiecas drošības prasības, kas noteiktas minētajā regulā.

---

[1] Eiropas Parlamenta un Padomes Direktīva 2002/21/EK (2002. gada 7. marts) par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (pamatdirektīva) (OV L 108, 24.4.2002., 33. lpp.).

[2] Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp).

(8) Šai direktīvai nebūtu jāskar iespēja katrai dalībvalstij veikt vajadzīgos pasākumus, lai nodrošinātu savu būtisko drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrības drošību, ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem. Saskaņā ar Līguma par Eiropas Savienības (LESD) 346. pantu dalībvalstīm nav jāsniedz informācija, kuras izpaušanu tās atzīst par būtisku savas drošības interešu apdraudējumu. Šajā kontekstā svarīgs ir Padomes Lēmums 2013/488/ES[1] un vienošanās par informācijas neizpaušanu vai neformālas vienošanās par informācijas neizpaušanu, piemēram, Gaismas signālu protokols.

(9) Konkrētas ekonomikas nozares jau tiek regulētas vai varētu turpmāk tikt regulētas ar Savienības tiesību aktiem, kas attiecināmi uz konkrētu nozari un kas ietver noteikumus, kuri ir saistīti ar tīklu un informācijas sistēmu drošību. Ja minētajos Savienības tiesību aktos ir noteikumi, kas paredz prasības attiecībā uz tīklu un informācijas sistēmu drošību vai paziņojumiem par incidentiem, minētie noteikumi būtu jāpiemēro, ja tie ietver prasības, kuras ietekmes ziņā ir vismaz līdzvērtīgas šajā direktīvā ietvertajiem pienākumiem. Dalībvalstīm tādā gadījumā būtu jāpiemēro šāda uz konkrētu nozari attiecināma Savienības tiesību akta noteikumi, tostarp noteikumi attiecībā uz jurisdikciju, un nebūtu jāveic šajā direktīvā definētais pamatpakalpojumu sniedzēju identifikācijas process. Šajā kontekstā dalībvalstīm būtu jāsniedz Komisijai informācija par *lex specialis* noteikuma piemērošanu. Nosakot to, vai uz konkrētu nozari attiecināmajos Savienības tiesību aktos ietvertās prasības, kuras saistītas ar tīklu un informācijas sistēmu drošību un/vai incidentu paziņošanu, ir līdzvērtīgas tām, kas ietvertas šajā direktīvā, būtu jāņem vērā vienīgi atbilstīgo Savienības tiesību aktu noteikumi un to piemērošana dalībvalstīs.

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

(10) Ūdens transporta nozarē drošības prasības uzņēmumiem, kuģiem, ostas iekārtām, ostām un kuģu satiksmes pakalpojumiem saskaņā ar Savienības tiesību aktiem attiecas uz visām darbībām, tostarp radio un telekomunikāciju sistēmām, datorsistēmām un tīkliem. Daļa no obligātajām procedūrām, kas jāievēro, ietver ziņošanu par visiem incidentiem, un tādēļ tās būtu jāuzskata par *lex specialis*, ciktāl minētās prasības ir vismaz līdzvērtīgas attiecīgajiem šīs direktīvas noteikumiem.

(11) Identificējot pakalpojumu sniedzējus ūdens transporta nozarē, dalībvalstīm būtu jāņem vērā esošie un turpmākie starptautiskie kodeksi un pamatnostādnes, ko jo īpaši izstrādājusi Starptautiskā Jūrniecības organizācija, lai sniegtu individuāliem jūrniecības nozares pakalpojumu sniedzējiem saskaņotu pieeju.

(12) Regulējums un uzraudzība banku un finanšu tirgus infrastruktūru nozarēs ir ļoti saskaņota Savienības līmenī, izmantojot Savienības primāros un sekundāros tiesību aktus un standartus, kas izstrādāti kopā ar Eiropas Uzraudzības iestādēm. Banku savienībā minēto prasību piemērošanu un uzraudzību nodrošina vienotais uzraudzības mehānisms. Dalībvalstīs, kuras nav banku savienībā, to nodrošina attiecīgie dalībvalstu banku regulatori. Citās finanšu nozares regulējuma jomās Eiropas Finanšu uzraudzības sistēma arī nodrošina augstu uzraudzības prakses kopīguma un konverģences līmeni. Eiropas Vērtspapīru un tirgu iestādei arī ir tieša uzraudzības loma attiecībā uz konkrētām vienībām, proti, kredītreitingu aģentūrām un darījumu reģistriem.

(13) Operacionālais risks ir būtiska prudenciālā regulējuma un uzraudzības daļa banku un finanšu tirgu infrastruktūru nozarēs. Tas attiecas uz visām darbībām, tostarp tīklu un informācijas sistēmu drošību, integritāti un noturību. Attiecībā uz šīm sistēmām izvirzītās prasības, kas bieži pārsniedz prasības, kas paredzētas saskaņā ar šo direktīvu , ir izklāstītas vairākos Savienības tiesību aktos, tostarp: noteikumos par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību un noteikumos par prudenciālajām prasībām attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām, kas ietver prasības par operacionālo risku; noteikumos par finanšu instrumentu tirgiem, kas ietver prasības par riska izvērtējumu ieguldījumu brokeru sabiedrībām un regulētiem tirgiem; noteikumos par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem, kas ietver prasības par operacionālo risku centrālajiem darījumu partneriem un darījumu reģistriem, un noteikumos par vērtspapīru norēķinu uzlabošanu Savienībā un centrālajiem vērtspapīru depozitārijiem, kas ietver prasības par operacionālo risku. Turklāt prasības par incidentu paziņošanu ir daļa no parastās uzraudzības prakses finanšu nozarē un bieži tiek iekļautas uzraudzības rokasgrāmatās. Dalībvalstīm būtu jāapsver minētie noteikumi un prasības, kad tās piemēro *lex specialis*.

(14) Kā Eiropas Centrālā banka norādījusi savā 2014. gada 25. jūlija atzinumā[1], šī direktīva neskar saskaņā ar Savienības tiesību aktiem pastāvošo Eurosistēmas maksājumu un norēķinu sistēmu uzraudzības režīmu. Iestādēm, kas ir atbildīgas par šādu uzraudzību, būtu lietderīgi jautājumos, kas attiecas uz tīklu un informācijas sistēmu drošību, veikt pieredzes apmaiņu ar kompetentajām iestādēm saskaņā ar šo direktīvu. Tādi paši apsvērumi attiecas uz Eiropas Centrālo banku sistēmas loceklēm, kas nav eurozonas locekles un veic šādu maksājumu un norēķinu sistēmu uzraudzību, pamatojoties uz valsts normatīvajiem aktiem.

[1] OV C 352, 7.10.2014., 4. lpp.

(15) Tiešsaistes tirdzniecības vieta ļauj patērētājiem un tirgotājiem slēgt tiešsaistes pārdošanas vai pakalpojumu līgumus ar tirgotājiem, un tā ir galīgais pakalpojums minēto līgumu noslēgšanai. Tajā nebūtu jāietver tiešsaistes pakalpojumi, kas ir tikai starpposms uz kādas trešās personas pakalpojumiem, caur kuriem beidzot var noslēgt līgumu. Tādēļ tajā nebūtu jāietver tiešsaistes pakalpojumi, kuri salīdzina konkrētu produktu vai pakalpojumu cenas, ko piedāvā dažādi tirgotāji, un pēc tam novirza lietotāju pie izvēlētā tirgotāja produkta iegādei. Tiešsaistes tirdzniecības vietā sniegtajos datošanas pakalpojumos var iekļaut transakciju apstrādi, datu apkopošanu vai lietotāju profilēšanu. Lietotņu veikali, kuri darbojas kā tiešsaistes veikali, kas ļauj digitāli izplatīt trešo personu lietotnes vai programmatūras, jāuzskata par tiešsaistes tirdzniecības vietas veidu.

(16) Tiešsaistes meklētājprogramma ļauj lietotājam veikt meklējumus principā visās tīmekļa vietnēs, pamatojoties uz vaicājumu par jebkādu tematu. To var arī koncentrēt uz tīmekļa vietnēm konkrētā valodā. Šajā direktīvā sniegtajā tiešsaistes meklētājprogrammas definīcijā nebūtu jāietver meklēšanas funkcijas, kas attiecas vienīgi uz konkrētas tīmekļa vietnes saturu, neatkarīgi no tā, vai meklēšanas funkciju nodrošina ārēja meklētājprogramma. Tajā nebūtu jāietver arī tiešsaistes pakalpojumi, kas salīdzina konkrētu produktu vai pakalpojumu cenas, kuras piedāvā dažādi tirgotāji, un pēc tam novirza lietotāju pie izvēlētā tirgotāja produkta iegādei.

(17) Mākoņdatošanas pakalpojumi ietver plašu darbību klāstu, kuras var veikt saskaņā ar dažādiem modeļiem. Šajā direktīvā termins "mākoņdatošanas pakalpojumi" ir pakalpojumi, kas ļauj piekļūt mērogojamam un elastīgam kopīgojamu datošanas resursu pūlam. Minētie datošanas resursi ietver tādus resursus kā tīkli, serveri vai cita infrastruktūra, glabāšana, lietotnes un pakalpojumi. Termins "mērogojams" attiecas uz datošanas resursiem, kurus mākoņpakalpojuma sniedzējs elastīgi piešķir neatkarīgi no resursu ģeogrāfiskās atrašanās vietas, lai risinātu pieprasījuma svārstības. Termins "elastīgs pūls" ir izmantots, lai aprakstītu tos datošanas resursus, kuri tiek nodrošināti un atbrīvoti saskaņā ar pieprasījumu, lai pieejamos resursus ātri palielinātu un samazinātu atkarībā no noslodzes. Termins "kopīgojami" ir izmantots, lai aprakstītu tos datošanas resursus, kas tiek sniegti daudziem lietotājiem, kuriem ir kopīga piekļuve pakalpojumam, bet apstrāde notiek katram lietotājam atsevišķi, kaut arī pakalpojums tiek sniegts no vienas un tās pašas elektroniskās iekārtas.

(18) Interneta plūsmu apmaiņas punkta (IPAP) funkcija ir savstarpēji savienot tīklus. IPAP nesniedz piekļuvi tīklam, nedz arī darbojas kā tranzīta nodrošinātājs vai nesējs. IPAP arī nesniedz citus pakalpojumus, kas nav saistīti ar starpsavienojumu, kaut arī tas neliedz IPAP operatoram sniegt nesaistītus pakalpojumus. IPAP pastāv, lai savstarpēji savienotu tīklus, kas ir tehniski un organizatoriski nodalīti. Termins "autonoma sistēma" tiek lietots, lai aprakstītu tehniski atsevišķu tīklu.

(19) Dalībvalstīm vajadzētu būt atbildīgām par noteikšanu, kuras vienības atbilst pamatpakalpojumu sniedzēja definīcijas kritērijiem. Lai nodrošinātu konsekventu pieeju, pamatpakalpojumu sniedzēja definīcija būtu saskanīgi jāpiemēro visās dalībvalstīs. Minētajā nolūkā šī direktīva paredz, ka tiek izvērtētas vienības, kas darbojas konkrētās nozarēs un apakšnozarēs , tiek izveidots pamatpakalpojumu saraksts, tiek ņemts vērā starpnozaru faktoru kopējs saraksts, lai noteiktu, vai iespējamam incidentam būtu ievērojama traucējoša ietekme, tiek veikta apspriešanās, kurā tiek iesaistītas attiecīgās dalībvalstis, ja vienības sniedz pakalpojumus vairāk nekā vienā dalībvalstī, un identifikācijas procesā atbalstu sniedz sadarbības grupa. Lai nodrošinātu, ka tiek pareizi ņemtas vērā iespējamās izmaiņas tirgū, dalībvalstīm būtu regulāri jāpārskata un vajadzības gadījumā jāatjaunina identificēto pakalpojumu sniedzēju saraksts. Visbeidzot, dalībvalstīm būtu jāsniedz Komisijai informācija, kas vajadzīga, lai izvērtētu, cik lielā mērā šī kopīgā metodoloģija ir ļāvusi dalībvalstīm konsekventi piemērot definīciju.

(20) Pamatpakalpojumu sniedzēju identifikācijas procesā dalībvalstīm būtu jāizvērtē vismaz attiecībā uz katru šajā direktīvā minēto apakšnozari, kuri pakalpojumi ir uzskatāmi par būtiskiem īpaši svarīgu sabiedrisku un ekonomisku darbību nodrošināšanai, un vai vienības, kas uzskaitītas šajā direktīvā minētajās nozarēs un apakšnozarēs un kas sniedz minētos pakalpojumus, atbilst pakalpojumu sniedzēju identifikācijas kritērijiem. Izvērtējot, vai vienība sniedz pakalpojumu, kas ir būtisks īpaši svarīgu sabiedrisku vai ekonomisku darbību nodrošināšanai, pietiek pārbaudīt, vai minētā vienība sniedz pakalpojumu, kas ir iekļauts pamatpakalpojumu sarakstā. Turklāt būtu jāpierāda, ka pamatpakalpojumu sniegšana ir atkarīga no tīklu un informācijas sistēmām. Visbeidzot, izvērtējot, vai incidents varētu būtiski traucēt pakalpojuma sniegšanu, dalībvalstīm būtu jāņem vērā vairāki starpnozaru faktori, kā arī attiecīgā gadījumā - konkrētās nozares faktori.

(21) Pamatpakalpojumu sniedzēju identifikācijas nolūkā uzņēmējdarbības veikšana dalībvalstī nozīmē efektīvu un faktisku darbību, ko veic pastāvīga vienība. Šādas vienības juridiskā forma neatkarīgi no tā, vai tā ir filiāle vai meitasuzņēmums ar juridiskas personas statusu, šajā sakarā nav noteicošais faktors.

(22) Ir iespējams, ka vienības, kas darbojas šajā direktīvā minētajās nozarēs un apakšnozarēs, sniedz gan pamatpakalpojumus, gan pakalpojumus, kas nav pamatpakalpojumi. Piemēram, gaisa pārvadājumu nozarē lidostas sniedz pakalpojumus, kurus dalībvalsts varētu uzskatīt par pamatpakalpojumiem, piemēram, pārvaldīt skrejceļus, bet arī vairākus pakalpojumus, kas varētu netikt uzskatīti par pamatpakalpojumiem, piemēram, nodrošināt iepirkšanās zonas. Īpašas prasības drošības jomā uz pamatpakalpojumu sniedzējiem būtu jāattiecina tikai saistībā ar tiem pakalpojumiem, kurus uzskata par pamatpakalpojumiem. Lai identificētu pakalpojumu sniedzējus, dalībvalstīm tādēļ būtu jānosaka to pakalpojumu saraksts, kurus uzskata par pamatpakalpojumiem.

(23) Pakalpojumu sarakstā būtu jāiekļauj visi pakalpojumi, ko sniedz attiecīgās dalībvalsts teritorijā un kas atbilst šīs direktīvas prasībām. Dalībvalstīm vajadzētu spēt papildināt esošo sarakstu, iekļaujot jaunus pakalpojumus. Pakalpojumu sarakstam būtu jākalpo par atsauces punktu dalībvalstīm, ļaujot identificēt pamatpakalpojumu sniedzējus. Tā nolūks ir identificēt pamatpakalpojumu veidus ikvienā konkrētā nozarē, kas minēta šajā direktīvā, tādējādi nošķirot tos no darbībām, kuras nav pamatdarbības un par kurām varētu būt atbildīga vienība, kas darbojas ikvienā konkrētajā nozarē. Katras dalībvalsts sastādītais pakalpojumu saraksts sniegtu turpmāku ieguldījumu katras dalībvalsts regulatīvās prakses izvērtēšanā, lai nodrošinātu identifikācijas procesa vispārēju saskaņotību dalībvalstu starpā.

(24) Identifikācijas procesa nolūkos, ja vienība sniedz pamatpakalpojumu divās vai vairāk dalībvalstīs, minētajām dalībvalstīm būtu savā starpā jāiesaistās divpusējās vai daudzpusējās diskusijās. Šis apspriešanās process ir paredzēts, lai palīdzētu tām izvērtēt pakalpojumu sniedzēja būtiskumu, ņemot vērā pārrobežu ietekmi, tādējādi ļaujot katrai iesaistītajai dalībvalstij paust viedokļus par riskiem, kas saistīti ar sniegtajiem pakalpojumiem. Šajā procesā attiecīgajām dalībvalstīm būtu jāņem vērā citai citas viedokļi un būtu jāspēj šajā sakarā lūgt sadarbības grupas palīdzību.

(25) Identifikācijas procesa rezultātā dalībvalstīm būtu jāpieņem valsts pasākumi, lai noteiktu, uz kurām vienībām attiecas pienākumi saistībā ar tīklu un informācijas sistēmu drošību. Šo rezultātu varētu sasniegt, pieņemot sarakstu, kurā uzskaitīti visi pamatpakalpojumu sniedzēji, vai pieņemot valsts pasākumus, tostarp objektīvus izmērāmus kritērijus, tādus kā pakalpojumu sniedzēja darbības rezultāts vai lietotāju skaits, kas ļauj noteikt, uz kurām vienībām attiecas pienākumi saistībā ar tīklu un informācijas sistēmu drošību. Valsts pasākumiem, jau esošiem vai šīs direktīvas sakarā pieņemtiem, vajadzētu ietvert visus juridiskos pasākumus, administratīvos pasākumus un politikas nostādnes, kas ļauj identificēt pamatpakalpojumu sniedzējus saskaņā ar šo direktīvu.

(26) Lai sniegtu norādi par identificēto pamatpakalpojumu sniedzēju nozīmi attiecībā uz konkrēto nozari, dalībvalstīm būtu jāņem vērā minēto pakalpojumu sniedzēju skaits un apmērs, kas izpaužas, piemēram, kā tirgus daļa vai saražotais vai sniegtais apjoms, bet tām nebūtu pienākuma izpaust informāciju, kas atklātu, kuri pakalpojumu sniedzēji ir identificēti.

(27) Lai noteiktu, vai incidentam būtu traucējošā ietekme uz pamatpakalpojuma sniegšanu, dalībvalstīm būtu jāņem vērā vairāki dažādi faktori, tādi kā lietotāju skaits, kuri izmanto konkrēto pakalpojumu privātos vai profesionālos nolūkos. Minēto pakalpojumu var izmantot tieši, netieši vai ar starpniecību. Izvērtējot to, kāda varētu būt incidenta ietekme uz ekonomiskām un sabiedriskām darbībām vai sabiedrisko drošību tā pakāpes un ilguma ziņā, dalībvalstīm būtu jāizvērtē arī tas, cik ilgā laikā varētu sākt izpausties traucējuma negatīvā ietekme.

(28) Papildus starpnozaru faktoriem būtu jāņem vērā arī konkrētās nozares faktori, Lai noteiktu, vai incidents būtiski traucētu kāda pamatpakalpojuma sniegšanu. Attiecībā uz enerģijas piegādātājiem šādi faktori varētu ietvert apjomu vai daļu no valstī saražotās enerģijas; attiecībā uz naftas piegādātājiem – apjomu dienā; attiecībā uz gaisa transportu, tostarp lidostām un gaisa pārvadātājiem, dzelzceļa transportu un jūras ostām – daļu valsts satiksmes apjomā un pasažieru skaitu vai kravas pārvadājumu darbības gadā; attiecībā uz banku vai finanšu tirgu infrastruktūrām – to sistēmisko nozīmīgumu, balstoties uz aktīvu kopsummu vai minētās aktīvu kopsummas attiecību pret IKP; attiecībā uz veselības aprūpes nozari – pacientu skaitu, ko pakalpojumu sniedzējs aprūpē gadā; attiecībā uz ūdens ieguvi, attīrīšanu un apgādi – apjomu un lietotāju, kuriem tas piegādāts, skaitu un veidus, tostarp, piemēram, slimnīcas, valsts pārvalde, organizācijas vai indivīdi, un to, vai tajā pašā ģeogrāfiskajā apvidū pastāv alternatīvi ūdens avoti.

(29) Lai panāktu un uzturētu augsta līmeņa tīklu un informācijas sistēmu drošību, katrai dalībvalstij būtu vajadzīga valsts tīklu un informācijas sistēmu drošības stratēģija, kurā noteikti stratēģiskie mērķi un konkrēti politikas pasākumi, kas jāīsteno.

(30) Ņemot vērā atšķirības valstu pārvaldes struktūrās un lai garantētu jau esošo nozaru noteikumu izpildi vai aizsargātu Savienības pašreizējās uzraudzības un regulējošās struktūras, kā arī lai izvairītos no dublēšanās, dalībvalstīm vajadzētu spēt izraudzīties vairāk nekā vienu valsts kompetento iestādi, kas ir atbildīga par to, lai saskaņā ar šo direktīvu pildītu uzdevumus saistībā ar pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju tīklu un informācijas sistēmu drošību.

(31) Lai veicinātu pārrobežu sadarbību un saziņu un lai varētu efektīvi īsteno šo direktīvu, katrai dalībvalstij, neskarot nozaru reglamentējošos noteikumus, vajadzētu izraudzīties valsts vienoto kontaktpunktu, kas atbildētu par to jautājumu koordināciju, kuri saistīti ar tīklu un informācijas sistēmu drošību un nodrošināšanu Savienības līmenī. Kompetentajām iestādēm un vienotajiem kontaktpunktiem vajadzētu būt pietiekamiem tehniskajiem, finanšu un cilvēkresursiem, lai nodrošinātu, ka tie efektīvi un produktīvi var veikt tiem uzticētos uzdevumus un tādējādi sasniegt šīs direktīvas mērķus. Tā kā šīs direktīvas mērķis ir uzlabot iekšējā tirgus darbību, radot uzticību un paļāvību, dalībvalstu struktūrām vajadzētu spēt efektīvi sadarboties ar ekonomikas dalībniekiem, un tām vajadzētu būt attiecīgi strukturētām.

(32) Kompetentajām iestādēm vai Datordrošības incidentu reaģēšanas vienībām ("*CSIRT*") būtu jāsaņem paziņojumi par incidentiem. Vienotajiem kontaktpunktiem nebūtu tieši jāsaņem paziņojumi par incidentiem, ja vien tie vienlaikus nedarbojas arī kā kompetentā iestāde vai *CSIRT*. Tomēr kompetentajai iestādei vai *CSIRT* būtu jāuzdod vienotajam kontaktpunktam nosūtīt paziņojumus par incidentiem citu skarto dalībvalstu vienotajiem kontaktpunktiem.

(33) Lai nodrošinātu efektīvu informācijas sniegšanu dalībvalstīm un Komisijai, vienotajam kontaktpunktam būtu jāiesniedz kopsavilkuma ziņojums sadarbības grupai, un tas būtu jāanonimizē, lai saglabātu paziņojumu un pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju identitātes konfidencialitāti, jo paraugprakses apmaiņai sadarbības grupā nav nepieciešama informācija par paziņojošo vienību identitāti. Kopsavilkuma ziņojumā būtu jāiekļauj informācija par saņemto paziņojumu skaitu, kā arī norāde par paziņoto incidentu raksturu, piemēram, drošības pārkāpumu veidiem, to smagumu vai ilgumu.

(34) Visās dalībvalstīs vajadzētu būt atbilstīgam aprīkojumam gan tehnisko, gan organizatorisko spēju ziņā, lai novērstu un atklātu tīklu un informācijas sistēmu incidentus un riskus, reaģētu uz tiem un tos mazinātu. Tāpēc dalībvalstīm būtu jānodrošina, ka tajās ir labi funkcionējošas, pamatprasībām atbilstīgas *CSIRT*, kas tiek dēvētas arī par datorapdraudējumu reaģēšanas vienībām *("CERT"*), lai nodrošinātu efektīvas un saderīgas spējas incidentu risināšanai un risku novēršanai un efektīvas sadarbības nodrošināšanai Savienības līmenī. Lai visu veidu pamatpakalpojumu sniedzēji un digitālo pakalpojumu sniedzēji gūtu labumu no šādām spējām un sadarbības, dalībvalstīm būtu jānodrošina, ka izraudzītā *CSIRT* aptver visus veidus. Ņemot vērā to, cik svarīga ir starptautiskā sadarbība kiberdrošības jomā, *CSIRT* vajadzētu spēt piedalīties starptautiskos sadarbības tīklos papildus *CSIRT* tīklam, ko izveido ar šo direktīvu.

(35) Tā kā tīklu un informācijas sistēmu lielākā daļa tiek apsaimniekota privāti, būtiska ir publiskā un privātā sektora sadarbība. Pamatpakalpojumu sniedzēji un digitālo pakalpojumu sniedzēji būtu jāmudina izmantot savus neformālās sadarbības mehānismus, lai nodrošinātu tīklu un informācijas sistēmu drošību. Sadarbības grupai vajadzētu spēt attiecīgā gadījumā uzaicināt uz diskusijām attiecīgās ieinteresētās personas. Lai efektīvi veicinātu informācijas un paraugprakses apmaiņu, ir būtiski nodrošināt, lai pamatpakalpojumu sniedzēji un digitālo pakalpojumu sniedzēji, kuri piedalās šādās apmaiņās, šādas sadarbības rezultātā nenonāktu nelabvēlīgā stāvoklī.

(36) *ENISA* būtu jāpalīdz dalībvalstīm un Komisijai, sniedzot savas specializētās zināšanas un padomus un sekmējot paraugprakses apmaiņu. Konkrēti, piemērojot šo direktīvu, Komisijai būtu jāapspriežas un dalībvalstīm vajadzētu spēt apspriesties ar *ENISA*. Lai veidotu dalībvalstu spējas un vairotu to zināšanas, sadarbības grupai būtu arī jādarbojas kā instrumentam paraugprakses apmaiņai, diskusijām par dalībvalstu spējām un gatavību un uz brīvprātības pamata jāpalīdz tās locekļiem izvērtēt valstu tīklu un informācijas sistēmu drošības stratēģijas, veidot spējas un novērtēt mācības saistībā ar tīklu un informācijas sistēmu drošību.

(37) Piemērojot šo direktīvu, dalībvalstīm attiecīgā gadījumā būtu jāspēj izmantot vai pielāgot pašreizējās organizatoriskās struktūras vai stratēģijas.

(38) Sadarbības grupas un *ENISA* attiecīgie uzdevumi ir savstarpēji atkarīgi un cits citu papildina. Kopumā *ENISA* būtu jāpalīdz sadarbības grupai pildīt tās uzdevumus, ievērojot *ENISA* mērķi, kas izklāstīts Eiropas Parlamenta un Padomes Regulā (ES) Nr. 526/2013 [1], proti,–palīdzēt Savienības iestādēm, struktūrām, birojiem un aģentūrām un dalībvalstīm īstenot politiku, kas vajadzīga, lai ievērotu normatīvo un administratīvo aktu prasības par tīklu un informācijas sistēmu drošību, kuras noteiktas pašreizējos un turpmākos Savienības tiesību aktos. Jo īpaši *ENISA* būtu jāsniedz palīdzība tajās jomās, kuras atbilst tās pašas uzdevumiem, kā izklāstīts Regulā (ES) Nr. 526/2013, proti, analizēt tīklu un informācijas sistēmu drošības stratēģijas, atbalstīt Savienības mācību saistībā ar tīklu un informācijas sistēmu drošību organizēšanu un veikšanu, un veikt informācijas un paraugprakses apmaiņu par informētības uzlabošanu un apmācību. *ENISA* būtu arī jāiesaista pamatnostādņu izstrādē par konkrētai nozarei paredzētiem kritērijiem, pēc kuriem nosaka incidenta ietekmes būtiskumu.

(39) Lai veicinātu tīklu un informācijas sistēmu drošības uzlabojumus, sadarbības grupai attiecīgā gadījumā būtu jāsadarbojas ar attiecīgām Savienības iestādēm, struktūrām, birojiem un aģentūrām, lai veiktu zinātības un paraugprakses apmaiņu un sniegtu padomus par tīklu un informācijas sistēmu drošības aspektiem, kas varētu ietekmēt to darbu, vienlaikus ievērojot esošo ierobežotas pieejamības informācijas apmaiņas kārtību. Sadarbojoties ar tiesībaizsardzības iestādēm attiecībā uz tīklu un informācijas sistēmu drošības aspektiem, kas varētu ietekmēt viņu darbu, sadarbības grupai būtu jāņem vērā pastāvošie informācijas kanāli un izveidotie tīkli.

[1] Eiropas Parlamenta un Padomes Regula (ES) Nr. 526/2013 (2013. gada 21. maijs) par Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*) un ar ko atceļ Regulu (EK) Nr. 460/2004 (OV L 165, 18.6.2013., 41. lpp.).

(40) Informācija par incidentiem kļūst arvien nozīmīgāka plašai sabiedrībai un uzņēmumiem, jo īpaši maziem un vidējiem uzņēmumiem. Dažos gadījumos šāda informācija jau tiek sniegta ar tīmekļa vietņu starpniecību valsts līmenī, konkrētās valsts valodā un galvenokārt koncentrējoties uz incidentiem un starpgadījumiem, kam piemīt valsts dimensija. Ņemot vērā to, ka uzņēmumi arvien vairāk veic pārrobežu darbību un pilsoņi arvien vairāk izmanto tiešsaistes pakalpojumus, informācija par incidentiem būtu jāsniedz apkopotā veidā Savienības līmenī. *CSIRT* tīkla sekretariāts tiek mudināts uzturēt tīmekļa vietni vai uzturēt īpašu lapu jau esošā tīmekļa vietnē, kurā plašai sabiedrībai tiek nodota vispārīga informācija par būtiskiem incidentiem, kas notikuši visā Savienībā īpaši koncentrējoties uz uzņēmumu interesēm un vajadzībām. *CSIRT*, kuras piedalās *CSIRT* tīklā, tiek aicinātas brīvprātīgi sniegt informāciju publicēšanai minētajā tīmekļa vietnē, neiekļaujot konfidenciālu vai sensitīvu informāciju.

(41) Ja informācija tiek uzskatīta par konfidenciālu saskaņā ar Savienības un valsts noteikumiem par darījumdarbības konfidencialitāti, šāda konfidencialitāte būtu jānodrošina, veicot šajā direktīvā noteiktos pasākumus un īstenojot tajā izvirzītos mērķus.

(42) Dalībvalstu gatavības un sadarbības testēšanā attiecībā uz tīklu un informācijas sistēmu drošību būtiska nozīme ir mācībām, kurās modelē reāllaika incidentu scenārijus. *CyberEurope* mācību cikls, kuru koordinē *ENISA*, piedaloties dalībvalstīm, ir noderīgs rīks, lai veiktu testus un izstrādātu ieteikumus par to, kā laika gaitā Savienības līmenī būtu rūpīgāk jāreaģē uz incidentiem. Ņemot vērā to, ka pašlaik dalībvalstīm nav pienākuma plānot mācības vai tajās piedalīties, *CSIRT* tīkla izveidei saskaņā ar šo direktīvu vajadzētu radīt iespēju dalībvalstīm piedalīties mācībās, pamatojoties uz rūpīgu plānošanu un stratēģisku izvēli. Saskaņā ar šo direktīvu izveidotās sadarbības grupai būtu jāapspriež stratēģiski lēmumi par mācībām, jo īpaši, bet ne tikai, par mācību regularitāti un scenāriju izstrādi. *ENISA* būtu saskaņā ar savām pilnvarām jāatbalsta Savienības mēroga mācību organizēšana un veikšana, sniedzot specializētās zināšanas un padomus sadarbības grupai un *CSIRT* tīklam.

(43) Ņemot vērā drošības problēmu, kas ietekmē tīklus un informācijas sistēmas, globālo raksturu, ir ciešāk jāsadarbojas starptautiskā līmenī, lai uzlabotu drošības standartus un informācijas apmaiņu un veicinātu vienotu vispārēju pieeju drošības jautājumiem.

(44) Tīklu un informācijas sistēmu drošības nodrošināšanas pienākumi lielā mērā ir pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju uzdevums. Būtu jāattīsta un jāpopularizē riska pārvaldības kultūra, kas ietver riska izvērtējumu un faktiskajiem riskiem atbilstīgu drošības pasākumu īstenošanu, un tas būtu jādara, izmantojot atbilstīgas regulatīvas prasības un brīvprātīgu nozares praksi. Vienlīdzīgu un uzticamu konkurences apstākļu radīšana arī ir būtiska sadarbības grupas un *CSIRT* tīkla efektīvai darbībai, lai nodrošinātu visu dalībvalstu efektīvu sadarbību.

(45) Šo direktīvu piemēro vienīgi tām valsts pārvaldes iestādēm, kas ir identificētas kā pamatpakalpojumu sniedzēji. Tādēļ dalībvalstu pienākums ir nodrošināt to valsts pārvaldes iestāžu tīklu un informācijas sistēmu drošību, uz kurām neattiecas šīs direktīvas darbības joma.

(46) Riska pārvaldības pasākumi ietver pasākumus nolūkā identificēt visus incidentu riskus, novērst, atklāt incidentus un reaģēt uz tiem, un mazināt to ietekmi. Tīklu un informācijas sistēmu drošība ietver glabāto, pārsūtīto un apstrādāto datu drošību.

(47) Kompetentajām iestādēm būtu jāsaglabā spēja pieņemt valsts pamatnostādnes par apstākļiem, kādos pamatpakalpojumu sniedzējiem tiek prasīts paziņot par incidentiem.

(48) Daudzi uzņēmumi Savienībā pakalpojumu sniegšanā izmanto digitālo pakalpojumu sniedzējus. Tā kā daži digitālie pakalpojumi varētu būt svarīgs resurss to lietotājiem, tostarp pamatpakalpojumu sniedzējiem, un tā kā šādiem lietotājiem ne vienmēr varētu būt pieejamas alternatīvas, šī direktīva būtu jāpiemēro arī šādu pakalpojumu sniedzējiem. Šajā direktīvā minēto digitālo pakalpojumu veidu drošība, nepārtrauktība un uzticamība ir būtiska daudzu uzņēmumu netraucētai darbībai. Šāda digitāla pakalpojuma traucējums varētu liegt citu pakalpojumu sniegšanu, kuros to izmanto, un tādējādi tas varētu ietekmēt būtiskas ekonomiskas un sabiedriskas darbības Savienībā. Šādi digitāli pakalpojumi tādēļ varētu būt īpaši svarīgi to uzņēmumu netraucētai darbībai, kuri ir no tiem atkarīgi, un vēl jo vairāk šādu uzņēmumu dalībai iekšējā tirgū un pārrobežu tirdzniecībai Savienībā. Tie digitālo pakalpojumu sniedzēji, uz kuriem attiecas šī direktīva, ir tie, par kuriem tiek uzskatīts, ka tie piedāvā digitālos pakalpojumus, ko arvien vairāk izmanto daudzi uzņēmumi Savienībā.

(49) Digitālo pakalpojumu sniedzējiem būtu jānodrošina drošības līmenis, kas ir samērīgs ar to riska pakāpi, kāda tiek radīta viņu sniegto digitālo pakalpojumu drošībai, ņemot vērā to, cik viņu pakalpojumi ir svarīgi citu uzņēmumu darbībām Savienībā. Praksē riska pakāpe pamatpakalpojumu sniedzējiem, kuru pakalpojumi bieži ir būtiski īpaši svarīgu sabiedrisku un ekonomisku darbību nodrošināšanai, būs augstāka nekā digitālo pakalpojumu sniedzējiem. Tādēļ drošības prasībām, kuras attiecas uz digitālo pakalpojumu sniedzējiem, vajadzētu būt mazākām. Digitālo pakalpojumu sniedzējiem būtu jāsaglabā rīcības brīvība veikt pasākumus, kurus tie uzskata par piemērotiem, lai pārvaldītu riskus, kas tiek radīti to tīklu un informācijas sistēmu drošībai. Uz digitālo pakalpojumu sniedzējiem to pārrobežu rakstura dēļ būtu jāattiecina saskaņotāka pieeja Savienības līmenī. Ar īstenošanas aktiem būtu jāveicina šādu pasākumu konkretizēšana un īstenošana.

(50) Kaut gan datortehnikas ražotāji un programmatūru izstrādātāji nav ne pamatpakalpojumu, ne digitālo pakalpojumu sniedzēji, to produkti pastiprina tīklu un informācijas sistēmu drošību. Tādējādi tiem ir svarīga loma, palīdzot pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem nodrošināt drošu tīklu un informācijas sistēmas. Uz šādiem datortehnikas un programmatūras produktiem jau attiecas pastāvošie noteikumi par produktu uzticamību.

(51) Tehniskiem un organizatoriskiem pasākumiem, kas noteikti pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, nebūtu jāsatur prasība, ka konkrēta komercinformācija un komunikāciju tehnoloģijas produkts jākonstruē, jāizstrādā vai jāražo kādā konkrētā veidā.

(52) Pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem būtu jānodrošina to izmantoto tīklu un informācijas sistēmu drošība. Tās galvenokārt ir privātas tīklu un informācijas sistēmas, ko pārvalda iekšējais IT personāls vai kuru drošība tiek nodrošināta, izmantojot ārpakalpojumus. Drošības un paziņošanas prasībām būtu jāattiecas uz attiecīgiem pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem neatkarīgi no tā, vai tie veic savu tīklu un informācijas sistēmu uzturēšanu iekšēji vai izmanto ārpakalpojumus.

(53) Lai izvairītos no nesamērīga finansiāla un administratīva sloga radīšanas pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, prasībām vajadzētu būt samērīgām ar risku, ko rada attiecīgā tīklu un informācijas sistēma, ņemot vērā jaunākos sasniegumus saistībā ar šādiem pasākumiem. Digitālo pakalpojumu sniedzēju gadījumā minētās prasības nebūtu jāpiemēro mikrouzņēmumiem un maziem uzņēmumiem.

(54) Ja dalībvalstu valsts pārvaldes iestādes izmanto pakalpojumus, ko piedāvā digitālo pakalpojumu sniedzēji, jo īpaši mākoņdatošanas pakalpojumus, tās varētu vēlēties pieprasīt no šādu pakalpojumu sniedzējiem papildu drošības pasākumus, kas pārsniedz tos, ko digitālo pakalpojumu sniedzēji parasti piedāvātu saskaņā ar šīs direktīvas prasībām. Tām būtu jāspēj to darīt, izmantojot līgumiskas saistības.

(55) Šajā direktīvā tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un mākoņdatošanas pakalpojumu definīcijas tiek lietotas konkrēti šīs direktīvas mērķiem, un tās neskar citus instrumentus.

(56) Šai direktīvai nebūtu jākavē dalībvalstis pieņemt valsts pasākumus, ar kuriem publiskā sektora struktūrām tiktu prasīts garantēt īpašas drošības prasības, kad tās slēdz līgumu par mākoņdatošanas pakalpojumiem. Jebkuri šādi valsts pasākumi būtu jāpiemēro attiecīgajai publiskā sektora struktūrai, nevis mākoņdatošanas pakalpojumu sniedzējam.

(57) Ņemot vērā būtiskās atšķirības starp pamatpakalpojumu sniedzējiem, jo īpaši to tiešo saikni ar fizisko infrastruktūru, un digitālo pakalpojumu sniedzējiem, jo īpaši to pārrobežu raksturu, šajā direktīvā būtu jāizmanto diferencēta pieeja attiecībā uz saskaņošanas līmeni abām minētajām vienību grupām. Attiecībā uz pamatpakalpojumu sniedzējiem dalībvalstīm vajadzētu būt iespējai identificēt attiecīgos pakalpojumu sniedzējus un noteikt stingrākas prasības nekā tās, kuras paredzētas direktīvā. Dalībvalstīm nebūtu jāidentificē digitālo pakalpojumu sniedzēji, jo šo direktīvu būtu jāpiemēro visiem digitālo pakalpojumu sniedzējiem tās darbības jomā. Turklāt ar šo direktīvu un īstenošanas aktiem, ko pieņem saskaņā ar to, attiecībā uz digitālo pakalpojumu sniedzējiem būtu jānodrošina augstāks saskaņošanas līmenis drošības un paziņošanas prasību jomā. Minētajam būtu jādod iespēja digitālo pakalpojumu sniedzējiem saņemt vienādu attieksmi visā Savienībā samērīgi to raksturam un riska pakāpei, ar kādu tie varētu saskarties.

(58) Ar šo direktīvu nebūtu jākavē dalībvalstis šīs direktīvas darbības jomā noteikt drošības un paziņošanas prasības vienībām, kas nav digitālo pakalpojumu sniedzēji, neskarot dalībvalstu saistības saskaņā ar Savienības tiesību aktiem.

(59) Kompetentajām iestādēm būtu jāpievērš pienācīga uzmanība neformālu un uzticamu informācijas apmaiņas kanālu saglabāšanai. Kad incidenti, par kuriem ziņots kompetentajām iestādēm, tiek publiskoti, būtu jāatrod atbilstīgs līdzsvars starp sabiedrības interesēm būt informētai par draudiem un iespējamu kaitējumu reputācijai un komerciālu kaitējumu pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, kuri ziņo par incidentiem. Īstenojot ziņošanas pienākumus, kompetentajām iestādēm un *CSIRT* būtu jāpievērš īpaša uzmanība nepieciešamībai saglabāt stingru konfidencialitāti attiecībā uz informāciju par produktu vājajām vietām, pirms tiek publiskota informācija par atbilstīgiem drošības uzlabojumiem.

(60) Digitālo pakalpojumu sniedzējiem būtu jāpiemēro atturīgas un reaģējošas *ex post* uzraudzības darbības, kuras attaisno to sniegto pakalpojumu un darbību būtība. Tādēļ attiecīgajai kompetentajai iestādei būtu jārīkojas tikai tad, kad tai ir sniegti pierādījumi (piemēram, tos ir sniedzis pats digitālo pakalpojumu sniedzējs, cita kompetentā iestāde, tostarp citas dalībvalsts kompetentā iestāde, vai pakalpojuma lietotājs), ka digitālo pakalpojumu sniedzējs neatbilst šīs direktīvas prasībām, jo īpaši pēc tam, kad ir noticis incidents. Tāpēc kompetentajai iestādei nevajadzētu būt vispārējam pienākumam uzraudzīt digitālo pakalpojumu sniedzējus.

(61) Kompetento iestāžu rīcībā vajadzētu būt nepieciešamajiem līdzekļiem to pienākumu veikšanai, tostarp pilnvarām saņemt pietiekamu informāciju, lai izvērtētu tīklu un informācijas sistēmu drošības līmeni.

(62) Incidenti var notikt noziedzīgu darbību rezultātā, kuru novēršanu, izmeklēšanu un sodīšanu par tām sekmē koordinācija un sadarbība starp pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem, kompetentajām iestādēm un tiesībaizsardzības iestādēm. Ja ir aizdomas, ka incidents ir saistīts ar smagām noziedzīgām darbībām, kas noteiktas Savienības vai valsts tiesību aktos, dalībvalstīm būtu jāmudina pamatpakalpojumu sniedzēji un digitālo pakalpojumu sniedzēji pašiem ziņot attiecīgajām tiesībaizsardzības iestādēm par incidentiem, kam varētu būt smagas noziedzības raksturs. Attiecīgā gadījumā vēlams, lai koordināciju starp dažādu dalībvalstu kompetentajām iestādēm un tiesībaizsardzības iestādēm sekmētu Eiropas Kibernoziedzības apkarošanas centrs (*EC*3) un *ENISA*.

(63) Incidentu dēļ daudzos gadījumos tiek kompromitēti personas dati. Šajā sakarā kompetentajām iestādēm un datu aizsardzības iestādēm būtu jāsadarbojas un jāapmainās ar informāciju visos attiecīgos jautājumos, lai novērstu jebkurus personas datu aizsardzības pārkāpumus, kas rodas incidentu dēļ.

(64) Jurisdikcija attiecībā uz digitālo pakalpojumu sniedzējiem būtu jānosaka dalībvalstij, kurā attiecīgajam digitālo pakalpojumu sniedzējam ir galvenā uzņēmējdarbības vieta Savienībā, kas principā ir turpat, kur ir pakalpojumu sniedzēja galvenā biroja atrašanās vieta Savienībā. Uzņēmējdarbības veikšana nozīmē efektīvu un faktisku darbību, ko veic pastāvīga vienība. Šādas vienības juridiskā forma neatkarīgi no tā, vai tā ir filiāle vai meitasuzņēmums ar juridiskas personas statusu, šajā sakarā nav noteicošais faktors. Šim kritērijam nevajadzētu būt atkarīgam no tā, vai tīklu un informācijas sistēmas fiziski atrodas konkrētajā vietā; šādu sistēmu atrašanās un izmantošana pati par sevi nav galvenā uzņēmējdarbības vieta, un tādēļ tie nav kritēriji galvenās uzņēmējdarbības vietas noteikšanai.

(65) Ja digitālo pakalpojumu sniedzējs, kurš neveic uzņēmējdarbību Savienībā, piedāvā pakalpojumus Savienībā, tam būtu jāieceļ pārstāvis. Lai noteiktu, vai šāds digitālo pakalpojumu sniedzējs piedāvā pakalpojumus Savienībā, būtu jāpārliecinās, vai ir acīmredzami tas, ka digitālo pakalpojumu sniedzējs plāno piedāvāt pakalpojumus personām vienā vai vairākās dalībvalstīs. Lai pārliecinātos par šādu nodomu, nepietiek tikai ar to vien, ka Savienībā ir pieejama digitālo pakalpojumu sniedzēja vai starpnieka tīmekļa vietne vai e-pasta adrese un cita kontaktinformācija, vai ka tiek izmantota valoda, ko parasti izmanto trešā valstī, kurā digitālo pakalpojumu sniedzējs veic uzņēmējdarbību. Tomēr tādi faktori kā, piemēram, valoda, ko izmanto, vai valūta, ko parasti izmanto vienā vai vairākās dalībvalstīs, piedāvājot pasūtīt pakalpojumus šajā citā valodā, vai Savienībā esošu klientu vai lietotāju pieminēšana var liecināt par to, ka digitālo pakalpojumu sniedzējs plāno piedāvāt pakalpojumus Savienībā. Pārstāvim būtu jārīkojas digitālo pakalpojumu sniedzēja vārdā, un kompetentajām iestādēm vai *CSIRT* vajadzētu būt iespējai sazināties ar pārstāvi. Pārstāvis būtu jāieceļ nepārprotami ar digitālo pakalpojumu sniedzēja rakstisku pilnvarojumu rīkoties tā vārdā attiecībā uz tā pienākumiem saskaņā ar šo direktīvu, tostarp attiecībā uz ziņošanu par incidentiem.

(66) Drošības prasību standartizācija ir tirgus virzīts process. Lai nodrošinātu drošības standartu vienveidīgu piemērošanu, dalībvalstīm būtu jāveicina atbilstība konkrētiem standartiem, lai nodrošinātu augstu tīklu un informācijas sistēmu drošības līmeni Savienības līmenī. *ENISA* būtu jāpalīdz dalībvalstīm, sniedzot padomus un pamatnostādnes. Šajā nolūkā varētu būt lietderīgi izstrādāt saskaņotus standartus, kas būtu jādara saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1025/2012[1].

(67) Vienības, uz kurām neattiecas šīs direktīvas darbības joma, var saskarties ar incidentiem, kuriem ir būtiska ietekme uz to sniegtajiem pakalpojumiem. Ja minētās vienības uzskata, ka sabiedrības interesēs ir paziņot par to, ka ir notikuši šādi incidenti, tām vajadzētu būt iespējai to brīvprātīgi darīt. Šādi paziņojumi būtu jāapstrādā kompetentajai iestādei vai *CSIRT*, ja šāda apstrāde nerada nesamērīgu vai nepamatotu slogu attiecīgajām dalībvalstīm.

[1] Eiropas Parlamenta un Padomes Regula (ES) Nr. 1025/2012 (2012. gada 25. oktobris) par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp.).

(68) Lai nodrošinātu vienādus šīs direktīvas īstenošanas nosacījumus, īstenošanas pilnvaras būtu jāuztic Komisijai, lai noteiktu procesuālo kārtību, kas nepieciešama sadarbības grupas darbībai, un drošības un paziņošanas prasības, kas piemērojamas digitālo pakalpojumu sniedzējiem. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011[1]. Pieņemot īstenošanas aktus attiecībā uz procesuālo kārtību, kas nepieciešama sadarbības grupas darbībai, Komisijai būtu vislielākā mērā jāņem vērā *ENISA* atzinums.

(69) Pieņemot īstenošanas aktus par drošības prasībām digitālo pakalpojumu sniedzējiem, Komisijai būtu vislielākā mērā jāņem vērā *ENISA* atzinums un būtu jāapspriežas ar ieinteresētajām personām. Turklāt Komisija tiek mudināta ņemt vērā šādus piemērus: attiecībā uz sistēmu un iekārtu drošību – fiziskā un vides drošība, piegādes drošība, piekļuves kontrole tīklu un informācijas sistēmām un tīklu un informācijas sistēmu integritāte; attiecībā uz incidentu risināšanu – incidentu risināšanas procedūras, incidentu atklāšanas spējas, ziņojumu sniegšana un komunikācija par incidentiem; attiecībā uz darbības nepārtrauktības pārvaldību – pakalpojuma nepārtrauktības stratēģija un ārkārtas rīcības plāni, negadījuma seku novēršanas spējas; un attiecībā uz uzraudzību, revīziju un testēšanu – uzraudzības un reģistrēšanas politika, mācību ārkārtas rīcības plāni, tīklu un informācijas sistēmu testēšana, drošības izvērtējumi un atbilstības uzraudzība.

[1] Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

(70) Īstenojot šo direktīvu, Komisijai būtu attiecīgā gadījumā jāsazinās ar attiecīgām nozaru komitejām un attiecīgām struktūrām, kas izveidotas Savienības līmenī jomās, uz ko attiecas šī direktīva.

(71) Komisijai, apspriežoties ar visām ieinteresētajām personām, būtu periodiski jāpārskata šī direktīva, jo īpaši, lai noteiktu izmaiņu veikšanas nepieciešamību, ņemot vērā izmaiņas sociālajos, politiskajos, tehnoloģiskajos vai tirgus apstākļos.

(72) Lai nodrošinātu informācijas apmaiņu par riskiem un incidentiem sadarbības grupā un *CSIRT* tīklā un atbilstību prasībām paziņot par incidentiem valsts kompetentajām iestādēm vai *CSIRT*, varētu būt nepieciešama personas datu apstrāde. Šādai apstrādei vajadzētu būt saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK [1] un Eiropas Parlamenta un Padomes Regulu (EK) Nr. 45/2001 [2]. Piemērojot šo direktīvu, pēc vajadzības būtu jāpiemēro Eiropas Parlamenta un Padomes Regula (EK) Nr. 1049/2001 [3].

(73) Saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2013. gada 14. jūnijā sniedza atzinumu [4].

---

[1] Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995., 31. lpp.).

[2] Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

[3] Eiropas Parlamenta un Padomes Regula (EK) Nr. 1049/2001 (2001. gada 30. maijs) par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem (OV L 145, 31.5.2001., 43. lpp.).

[4] OV C 32, 4.2.2014., 19. lpp.

(74) Ņemot vērā to, ka šīs direktīvas mērķi, proti, panākt kopēju augsta līmeņa tīklu un informācijas sistēmu drošību Savienībā, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet rīcības ietekmes dēļ to var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā direktīvā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai.

(75) Šajā direktīvā ir respektētas pamattiesības un ievēroti principi, kas atzīti Eiropas Savienības Pamattiesību hartā, jo īpaši tiesības uz privātās dzīves un saziņas neaizskaramību, tiesības uz personas datu aizsardzību, darījumdarbības brīvība, tiesības uz īpašumu, tiesības uz efektīvu tiesību aizsardzību un tiesības tikt uzklausītam. Šī direktīva būtu jāīsteno saskaņā ar minētajām tiesībām un principiem,

IR PIEŅĒMUSI ŠO DIREKTĪVU.

I NODAĻA
VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets un darbības joma

1. Šajā direktīvā ir paredzēti pasākumi ar mērķi panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību Savienībā, lai uzlabotu iekšējā tirgus darbību.

2. Minētajam nolūkam šajā direktīvā:

   a) paredz pienākumus visām dalībvalstīm pieņemt valsts stratēģiju tīklu un informācijas sistēmu drošībai;

   b) izveido sadarbības grupu, lai atbalstītu un sekmētu stratēģisko sadarbību un informācijas apmaiņu starp dalībvalstīm un attīstītu uzticēšanos un paļāvību starp tām;

   c) izveido Datordrošības incidentu reaģēšanas vienību tīklu ("*CSIRT* tīkls"), lai palīdzētu attīstīt uzticēšanos un paļāvību starp dalībvalstīm un veicinātu ātru un efektīvu operatīvo sadarbību;

   d) nosaka drošības un paziņošanas prasības pamatpakalpojumu un digitālo pakalpojumu sniedzējiem;

e) paredz dalībvalstu pienākumus izraudzīties valsts kompetentās iestādes, vienotus kontaktpunktus un *CSIRT*, uzticot tiem uzdevumus saistībā ar tīklu un informācijas sistēmu drošību.

3. Šajā direktīvā paredzētās drošības un paziņošanas prasības neattiecas ne uz uzņēmumiem, kuriem piemēro Direktīvas 2002/21/EK 13.a un 13.b panta prasības, ne uz uzticamības pakalpojumu sniedzējiem, kuriem piemēro Regulas (ES) Nr. 910/2014 19. panta prasības.

4. Šo direktīvu piemēro, neskarot Padomes Direktīvu 2008/114/EK [1], Eiropas Parlamenta un Padomes Direktīvu 2011/93/ES [2] un Eiropas Parlamenta un Padomes Direktīvu 2013/40/ES [3].

5. Neskarot LESD 346. pantu, informācijas – kas ir konfidenciāla, ievērojot Savienības un valsts noteikumus, piemēram, noteikumus par darījumdarbības konfidencialitāti, – apmaiņa notiek ar Komisiju un citām attiecīgajām iestādēm tikai tad, ja šāda apmaiņa ir nepieciešama šīs direktīvas piemērošanai. Apmainās tikai ar to informāciju, kas ir atbilstīga un samērīga šādas apmaiņas nolūkam. Šādā informācijas apmaiņā ievēro minētās informācijas konfidencialitāti un aizsargā pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju drošību un komerciālās intereses.

---

[1] Padomes Direktīva 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību (OV L 345, 23.12.2008., 75. lpp.).

[2] Eiropas Parlamenta un Padomes Direktīva 2011/93/ES (2011. gada 13. decembris) par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, un ar kuru aizstāj Padomes Pamatlēmumu 2004/68/TI (OV L 335, 17.12.2011., 1. lpp.).

[3] Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI (OV L 218, 14.8.2013., 8. lpp.).

6. Šī direktīva neskar pasākumus, kurus dalībvalstis veic, lai nodrošinātu to valsts pamatfunkcijas – jo īpaši, lai garantētu valsts drošību, tostarp pasākumus, ar kuriem aizsargā informāciju, kuras izpaušanu dalībvalstis uzskata par tādu, kas ir pretrunā to drošības pamatinteresēm, – un lai uzturētu likumību un kārtību, jo īpaši, lai ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem.

7. Ja uz konkrētu nozari attiecināmā Savienības tiesību aktā ir paredzēta prasība pamatpakalpojumu sniedzējiem vai digitālo pakalpojumu sniedzējiem nodrošināt vai nu to tīklu un informācijas sistēmu drošību, vai paziņot par incidentiem ar noteikumu, ka šādas prasības iedarbības ziņā ir vismaz līdzvērtīgas šajā direktīvā noteiktajiem pienākumiem, piemēro minētā uz konkrētu nozari attiecināmā Savienības tiesību akta minētos noteikumus.

2. pants

Personas datu apstrāde

1. Personas datu apstrādi, ievērojot šo direktīvu, veic saskaņā ar Direktīvu 95/46/EK.

2. Personas datu apstrāde, ko, ievērojot šo direktīvu, veic Savienības iestādes un struktūras, tiek veikta saskaņā ar Regulu (EK) Nr. 45/2001.

3. pants

Minimālā saskaņošana

Neskarot 16. panta 10. punktu un dalībvalstu pienākumus saskaņā ar Savienības tiesību aktiem, dalībvalstis var pieņemt vai saglabāt spēkā noteikumus nolūkā panākt augstāku tīklu un informācijas sistēmu drošības līmeni.

4. pants

Definīcijas

Šajā direktīvā piemēro šādas definīcijas:

1) "tīklu un informācijas sistēma" ir:

a) elektronisko komunikāciju tīkls Direktīvas 2002/21/EK 2. panta a) punkta nozīmē,

b) jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču kopums, no kurām viena vai vairākas ierīces, ievērojot programmu, veic digitālu datu automātisku apstrādi, vai

c) digitāli dati, ko a) un b) apakšpunktā minētie elementi glabā, apstrādā, iegūst vai sūta to darbības, izmantošanas, aizsardzības un uzturēšanas nolūkos;

2) "tīklu un informācijas sistēmu drošība" ir tīklu un informācijas sistēmu spēja noteiktā uzticamības līmenī pretoties jebkurām darbībām, kas apdraud glabājamo vai pārraidāmo, vai apstrādājamo datu pieejamību, autentiskumu, integritāti vai konfidencialitāti vai minēto tīklu un informācijas sistēmu piedāvātos vai ar to starpniecību pieejamos saistītos pakalpojumus;

3) "valsts stratēģija par tīklu un informācijas sistēmu drošību " ir sistēma, kurā paredz stratēģiskos mērķus un prioritātes attiecībā uz tīklu un informācijas sistēmu drošību valsts līmenī;

4) "pamatpakalpojumu sniedzējs" ir tāda veida publiska vai privāta vienība, kā minēts II pielikumā, un kas atbilst 5. panta 2. punktā noteiktajiem kritērijiem;

5) "digitālais pakalpojums" ir tāda veida pakalpojums Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/1535 [1] 1. panta 1. punkta b) apakšpunkta nozīmē, kā uzskaitīts III pielikumā;

6) "digitālā pakalpojuma sniedzējs" ir jebkura juridiska persona, kas sniedz digitālo pakalpojumu;

7) "incidents" ir jebkāds notikums, kas faktiski nelabvēlīgi ietekmē tīklu un informācijas sistēmu drošību;

8) "incidenta risināšana" ir visas procedūras, kas ļauj atklāt incidentu, veikt tā analīzi, to ierobežot un reaģēt uz to;

[1] Eiropas Parlamenta un Padomes Direktīva (ES) 2015/1535 (2015. gada 9. septembris), ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā (OV L 241, 17.9.2015., 1. lpp.).

9) "risks" ir jebkāds racionāli identificējams apstāklis vai notikums, kas var nelabvēlīgi ietekmēt tīklu un informācijas sistēmu drošību;

10) "pārstāvis" ir jebkura fiziska vai juridiska persona, kura veic uzņēmējdarbību Savienībā un ir nepārprotami izraudzīta rīkoties tāda digitālo pakalpojumu sniedzēja vārdā, kas neveic uzņēmējdarbību Savienībā, un pie kuras digitālo pakalpojumu sniedzēja vietā var vērsties valsts kompetentā iestāde vai *CSIRT*, attiecībā uz minētā digitālo pakalpojumu sniedzēja pienākumiem saskaņā ar šo direktīvu;

11) "standarts" ir standarts Regulas (ES) Nr. 1025/2012 2. panta 1. punkta nozīmē;

12) "specifikācija" ir tehniskā specifikācija Regulas (ES) Nr. 1025/2012 2. panta 4. punkta nozīmē;

13) "interneta plūsmu apmaiņas punkts (IPAP)" ir tīkla iekārta, kas ļauj nodrošināt vairāk nekā divu neatkarīgu autonomu sistēmu starpsavienojumu galvenokārt nolūkā atvieglot interneta datplūsmas apmaiņu; IPAP nodrošina starpsavienojumu tikai autonomām sistēmām; IPAP nav nepieciešams, lai interneta datplūsma starp jebkurām divām iesaistītām autonomām sistēmām izietu cauri jebkurai trešai autonomai sistēmai; tas arī nemaina vai citādi neietekmē šādu datplūsmu;

14) "domēnu nosaukumu sistēma (DNS)" ir hierarhiska sadalīta nosaukumu sistēma tīklā, kura nosūta vaicājumus attiecībā uz domēnu nosaukumiem;

15) "DNS pakalpojumu sniedzējs" ir vienība, kas sniedz DNS pakalpojumus internetā;

16) "augstākā līmeņa domēnu nosaukumu reģistrs" ir vienība, kas pārvalda un veic interneta domēnu nosaukumu reģistrāciju zem konkrēta augstākā līmeņa domēna (*TLD*).

17) "tiešsaistes tirdzniecības vieta" ir digitālais pakalpojums, kas ļauj patērētājiem un/vai tirgotājiem, kuri definēti attiecīgi Eiropas Parlamenta un Padomes Direktīvas 2013/11/ES [1] 4. panta 1. punkta a) un b) apakšpunktā, noslēgt tiešsaistes pirkuma vai pakalpojumu līgumus ar tirgotājiem vai nu tiešsaistes tirdzniecības vietas tīmekļa vietnē, vai tirgotāja tīmekļa vietnē, kurā izmanto datošanas pakalpojumus, ko sniedz tiešsaistes tirdzniecības vieta;

18) "tiešsaistes meklētājprogramma" ir digitālais pakalpojums, kas ļauj lietotājiem veikt meklējumus principā visās tīmekļa vietnēs vai tīmekļa vietnēs konkrētā valodā, pamatojoties uz vaicājumu par jebkādu tematu atslēgvārda, frāzes vai citu ievaddatu veidā, un sniedz saites, kurās var atrast informāciju saistībā ar prasīto saturu;

19) "mākoņdatošanas pakalpojums" ir digitāls pakalpojums, kas dod iespēju piekļūt mērogojamam un elastīgam kopīgojamu datošanas resursu pūlam;

5. pants

Pamatpakalpojumu sniedzēju identifikācija

1. Līdz ... [27 mēneši pēc šīs direktīvas spēkā stāšanās dienas] attiecībā uz katru nozari un apakšnozari, kas minētas II pielikumā, dalībvalstis identificē pamatpakalpojumu sniedzējus, kam to teritorijā ir uzņēmējdarbības vieta.

[1] Eiropas Parlamenta un Padomes Direktīva 2013/11/ES (2013. gada 21. maijs) par patērētāju strīdu alternatīvu izšķiršanu un ar ko groza Regulu (EK) Nr. 2006/2004 un Direktīvu 2009/22/EK (Direktīva par patērētāju SAI) (OV L 165, 18.6.2013., 63. lpp.).

2. Direktīvas 4. panta 4. punktā minētie kritēriji pamatpakalpojumu sniedzēju identificēšanai ir šādi:

a) vienība sniedz pakalpojumu, kas ir būtisks īpaši svarīgu sabiedrisku un/vai ekonomisku darbību nodrošināšanai;

b) minētā pakalpojuma sniegšana ir atkarīga no tīklu un informācijas sistēmām; un

c) incidentam būtu būtiska traucējoša ietekme uz minētā pakalpojuma sniegšanu.

3. Piemērojot 1. punktu, katra dalībvalsts izveido 2. punkta a) apakšpunktā minēto pakalpojumu sarakstu.

4. Piemērojot 1. punktu, ja vienība sniedz 2. punkta a) apakšpunktā minēto pakalpojumu divās vai vairāk dalībvalstīs, minētās dalībvalstis savstarpēji apspriežas. Minētā apspriešanās notiek, pirms tiek pieņemts lēmums par identifikāciju.

5. Dalībvalstis regulāri un vismaz reizi divos gados pēc … [21 mēnesis pēc šīs direktīvas stāšanās spēkā] pārskata un attiecīgā gadījumā atjaunina identificēto pamatpakalpojumu sniedzēju sarakstu.

6. Sadarbības grupas funkcija saskaņā ar 11. pantā minētajiem uzdevumiem ir atbalstīt dalībvalstis konsekventas pieejas izmantošanā pamatpakalpojumu sniedzēju identifikācijas procesā.

7. Direktīvas 23. pantā minētās pārskatīšanas nolūkā un līdz … [27 mēneši pēc šīs direktīvas spēkā stāšanās dienas], un pēc tam reizi divos gados dalībvalstis iesniedz Komisijai informāciju, kas vajadzīga, lai Komisija spētu izvērtēt šīs direktīvas īstenošanu, jo īpaši dalībvalstu izmantoto pieeju konsekvenci pamatpakalpojumu sniedzēju identifikācijā. Minētajā informācijā ietver vismaz:

a) valsts pasākumus, kas ļauj identificēt pamatpakalpojumu sniedzējus;

b) pakalpojumu sarakstu, kas minēts 3. punktā;

c) identificēto pamatpakalpojumu sniedzēju skaitu katrai II pielikumā minētajai nozarei un norādi par to nozīmīgumu attiecībā uz minēto nozari;

d) robežvērtības, ja tādas pastāv, lai noteiktu attiecīgo piedāvājuma līmeni, atsaucoties uz to lietotāju skaitu, kuri izmanto minēto pakalpojumu, kā minēts 6. panta 1. panta a) apakšpunktā, vai uz minētā konkrētā pamatpakalpojumu sniedzēja nozīmīgumu, kā minēts 6. panta 1. punktā.

Lai sekmētu salīdzināmas informācijas sniegšanu, Komisija, maksimāli ņemot vērā *ENISA* atzinumu, var pieņemt atbilstīgas tehniskās pamatnostādnes par rādītājiem attiecībā uz šajā punktā minēto informāciju.

6. pants

Būtiska traucējoša ietekme

1. Nosakot 5. panta 2. punkta c) apakšpunktā minētās traucējošās ietekmes būtiskumu, dalībvalstis ņem vērā vismaz šādus starpnozaru faktorus:

   a) to lietotāju skaits, kuri izmanto attiecīgās vienības sniegtos pakalpojumus;

   b) citu II pielikumā minēto nozaru atkarība no minētās vienības sniegtā pakalpojuma;

   c) ietekme, kas incidentiem pakāpes un ilguma ziņā varētu būt uz ekonomiskām un sabiedriskām darbībām vai sabiedrisko drošību;

   d) minētās vienības tirgus daļa;

   e) ģeogrāfiskā izplatība attiecībā uz vidi, ko varētu skart incidents;

   f) vienības nozīmīgums pietiekama pakalpojumu līmeņa uzturēšanai, ņemot vērā alternatīvu līdzekļu pieejamību minētā pakalpojuma sniegšanai.

2. Lai noteiktu, vai incidentam būtu būtiska traucējoša ietekme, dalībvalstis attiecīgā gadījumā ņem vērā arī konkrētai nozarei raksturīgus faktorus.

II NODAĻA
VALSTU SISTĒMAS ATTIECĪBĀ UZ TĪKLU UN INFORMĀCIJAS SISTĒMU DROŠĪBU

7. pants

Valsts tīklu un informācijas sistēmu drošības stratēģija

1. Katra dalībvalsts pieņem valsts tīklu un informācijas sistēmu drošības stratēģiju, kurā definēti stratēģiskie mērķi un atbilstīgi politikas un regulatīvi pasākumi, lai panāktu un saglabātu augsta līmeņa tīklu un informācijas sistēmu drošību, un kas attiecas vismaz uz II pielikumā minētajām nozarēm un III pielikumā minētajiem pakalpojumiem. Valsts tīklu un informācijas sistēmu drošības stratēģijā pievēršas jo īpaši šādiem jautājumiem:

   a) valsts tīklu un informācijas sistēmu drošības stratēģijas mērķi un prioritātes;

   b) pārvaldības sistēma, lai sasniegtu valsts tīklu un informācijas sistēmu drošības stratēģijas mērķus un prioritātes, tostarp valdības struktūru un citu attiecīgo dalībnieku funkcijas un pienākumi;

   c) tādu pasākumu apzināšana, kas attiecas uz sagatavotību, reaģēšanu un atkopi, tostarp sadarbību starp publisko un privāto sektoru;

d) norāde par izglītības, informētības uzlabošanas un apmācības programmām, kas attiecas uz tīklu un informācijas sistēmu drošības stratēģiju;

e) norāde par pētniecības un attīstības plāniem, kas attiecas uz tīklu un informācijas sistēmu drošības stratēģiju;

f) riska izvērtējuma plāns, lai apzinātu riskus;

g) saraksts ar dažādiem dalībniekiem, kas iesaistīti tīklu un informācijas sistēmu drošības stratēģijas īstenošanā.

2. Dalībvalstis var lūgt *ENISA* palīdzību valstu tīklu un informācijas sistēmu drošības stratēģiju izstrādē.

3. Valsts tīklu un informācijas sistēmu drošības stratēģijas dalībvalstis paziņo Komisijai trīs mēnešos pēc to pieņemšanas. To darot, dalībvalstis var izslēgt stratēģijas elementus, kas saistīti ar valsts drošību.

8. pants

Valstu kompetentās iestādes un vienotais kontaktpunkts

1. Katra dalībvalsts izraugās vienu vai vairākas valsts kompetentās iestādes, kuras atbild par tīklu un informācijas sistēmu drošību (turpmāk "kompetentā iestāde") un kuru darbība attiecas vismaz uz II pielikumā minētajām nozarēm un III pielikumā minētajiem pakalpojumiem. Dalībvalstis var uzticēt šo funkciju esošai iestādei vai iestādēm.

2. Kompetentās iestādes uzrauga šīs direktīvas piemērošanu valsts līmenī.

3. Katra dalībvalsts izraugās valsts vienoto kontaktpunktu, kas atbild par tīklu un informācijas sistēmu drošību ("vienotais kontaktpunkts"). Dalībvalstis var uzticēt šo funkciju esošai iestādei. Ja dalībvalsts izraugās tikai vienu kompetento iestādi, minētā kompetentā iestāde ir arī vienotais kontaktpunkts.

4. Vienotais kontaktpunkts veic sadarbības koordinācijas funkcijas, lai nodrošinātu dalībvalsts iestāžu pārrobežu sadarbību un sadarbību ar attiecīgajām iestādēm citās dalībvalstīs un ar 11. pantā minēto sadarbības grupu, un 12. pantā minēto *CSIRT* tīklu.

5. Dalībvalstis nodrošina, ka kompetentajām iestādēm un vienotajiem kontaktpunktiem ir adekvāti resursi, lai efektīvi un rezultatīvi veiktu tiem uzticētos uzdevumus un tādējādi sasniegtu šīs direktīvas mērķus. Dalībvalstis nodrošina efektīvu, rezultatīvu un drošu izraudzīto pārstāvju sadarbību sadarbības grupā.

6. Kompetentās iestādes un vienotais kontaktpunkts attiecīgā gadījumā un saskaņā ar valsts tiesību aktiem apspriežas un sadarbojas ar attiecīgajām valsts tiesībaizsardzības iestādēm un valsts datu aizsardzības iestādēm.

7. Katra dalībvalsts nekavējoties paziņo Komisijai izraudzīto kompetento iestādi un vienotā kontaktpunkta nosaukumu, to uzdevumus un visas turpmākās izmaiņas šajā informācijā. Katra dalībvalsts publisko savas izraudzītās kompetentās iestādes un vienotā kontaktpunkta nosaukumu. Komisija publicē izraudzīto vienoto kontaktpunktu sarakstu.

9. pants

Datordrošības incidentu reaģēšanas vienības (CSIRT)

1. Katra dalībvalsts izraugās vienu vai vairākas *CSIRT*, kuras atbilst I pielikuma 1. punktā izklāstītajām prasībām, kuru darbība attiecas vismaz uz II pielikumā minētajām nozarēm un III pielikumā minētajiem pakalpojumiem un kuras ir atbildīgas par incidentu un risku risināšanu saskaņā ar labi definētu procesu. *CSIRT* var izveidot kompetentajā iestādē.

2. Dalībvalstis nodrošina, ka *CSIRT* ir adekvāti resursi, lai tās efektīvi pildītu uzdevumus, kā izklāstīts I pielikuma 2. punktā.

   Dalībvalstis nodrošina efektīvu, rezultatīvu un drošu *CSIRT* sadarbību 12. pantā minētajā *CSIRT* tīklā.

3. Dalībvalstis nodrošina, ka to *CSIRT* ir piekļuve atbilstīgai, drošai un noturīgai sakaru un informācijas infrastruktūrai valsts līmenī.

4. Dalībvalstis informē Komisiju par to *CSIRT* uzdevumu jomu, kā arī incidentu risināšanas procesa galvenajiem elementiem.

5. Dalībvalstis var lūgt *ENISA* palīdzību valstu *CSIRT* izveidē.

10. pants

Sadarbība valsts līmenī

1. Vienas un tās pašas dalībvalsts kompetentā iestāde, vienotais kontaktpunkts un *CSIRT* – ja tās ir atsevišķas struktūras – sadarbojas attiecībā uz šajā direktīvā noteikto pienākumu izpildi.

2. Dalībvalstis nodrošina, ka vai nu kompetentās iestādes vai *CSIRT* saņem paziņojumus par incidentiem, ko iesniedz, ievērojot šo direktīvu. Ja dalībvalsts nolemj, ka *CSIRT* nesaņem paziņojumus, *CSIRT* – ciktāl tas nepieciešams, lai izpildītu to uzdevumus – piešķir piekļuvi datiem par incidentiem, ko, ievērojot 14. panta 3. un 5. punktu, paziņojuši pamatpakalpojumu sniedzēji vai, ievērojot 16. panta 3. un 6. punktu - digitālo pakalpojumu sniedzēji.

3. Dalībvalstis nodrošina, ka kompetentās iestādes vai CSIRT informē vienotos kontaktpunktus par paziņojumiem par incidentiem, kas iesniegti, ievērojot šo direktīvu.

   Līdz ... [24 mēneši pēc šīs direktīvas spēkā stāšanās dienas] un pēc tam katru gadu vienotais kontaktpunkts iesniedz sadarbības grupai kopsavilkuma ziņojumu par saņemtajiem paziņojumiem, tostarp par paziņojumu skaitu un paziņoto incidentu raksturu, un darbībām, kas veiktas saskaņā ar 14. panta 3. un 5. punktu un 16. panta 3. un 6. punktu.

III NODAĻA
SADARBĪBA

11. pants

Sadarbības grupa

1. Ar šo tiek izveidota sadarbības grupa, lai atbalstītu un atvieglotu stratēģisko sadarbību un apmaiņu ar informāciju starp dalībvalstīm, lai attīstītu uzticēšanos un paļāvību, kā arī nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību Savienībā.

   Sadarbības grupa veic uzdevumus, pamatojoties uz divgadu darba programmām, kā minēts 3. punkta otrajā daļā.

2. Sadarbības grupas sastāvā ir pārstāvji no dalībvalstīm, Komisijas un *ENISA*.

   Attiecīgā gadījumā sadarbības grupa var uzaicināt pārstāvjus no attiecīgajām ieinteresētajām personām piedalīties tās darbā.

   Komisija nodrošina sekretariātu.

3. Sadarbības grupai ir šādi uzdevumi:

   a) sniegt stratēģiskas norādes saskaņā ar 12. pantu izveidotā *CSIRT* tīkla darbībai;

b) apmainīties ar paraugpraksi saistībā ar tās informācijas apmaiņu, kas saistīta ar 14. panta 3. un 5. punktā un 16. panta 3. un 6. punktā minēto paziņojumu par incidentu;

c) veikt paraugprakses apmaiņu starp dalībvalstīm un sadarbībā ar *ENISA* palīdzēt dalībvalstīm spēju veidošanā, lai nodrošinātu tīklu un informācijas sistēmu drošību;

d) apspriest dalībvalstu spējas un sagatavotību un uz brīvprātības pamata izvērtēt valstu tīklu un informācijas sistēmu drošības stratēģijas un *CSIRT* efektivitāti, un apzināt paraugpraksi;

e) apmainīties ar informāciju un paraugpraksi saistībā ar informētības uzlabošanu un apmācību;

f) apmainīties ar informāciju un paraugpraksi saistībā ar pētījumiem par tīklu un informācijas sistēmu drošību un tās pilnveidošanu;

g) attiecīgā gadījumā apmainīties ar pieredzi jautājumos, kas attiecas uz tīklu un informācijas sistēmu drošību, ar attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām;

h) apspriest 19. pantā minētos standartus un specifikācijas ar pārstāvjiem no attiecīgajām Eiropas standartizācijas organizācijām;

i) vākt paraugprakses informāciju par riskiem un incidentiem;

j) reizi gadā izskatīt kopsavilkuma ziņojumus, kas minēti 10. panta 3. punkta otrajā daļā;

k) apspriest veikto darbu attiecībā uz mācībām saistībā ar tīklu un informācijas sistēmu drošību, izglītības programmām un apmācību, tostarp darbu, ko veic *ENISA*;

l) ar *ENISA* palīdzību apmainīties ar paraugpraksi saistībā ar dalībvalstu veikto pamatpakalpojumu sniedzēju identifikāciju, tostarp attiecībā uz pārrobežu atkarību saistībā ar riskiem un incidentiem;

m) apspriest kārtību ziņošanai par paziņojumiem par incidentiem, kā minēts 14. un 16. pantā.

Līdz... [18 mēneši pēc šīs direktīvas stāšanās spēkā] un pēc tam reizi divos gados sadarbības grupa izstrādā darba programmu par pasākumiem, kas jāveic, lai īstenotu tās mērķus un uzdevumus, kura ir saderīga ar šīs direktīvas mērķiem.

4. Pārskatam, kas minēts 23. pantā un līdz …[24 mēneši pēc šīs direktīvas spēkā stāšanās dienas] un pēc tam - ik pēc pusotra gada sadarbības grupa sagatavo ziņojumu, kurā izvērtē pieredzi, kas gūta saistībā ar stratēģisko sadarbību, ko īsteno, ievērojot šo pantu.

5. Komisija pieņem īstenošanas aktus, ar kuriem nosaka procedūras kārtību, kas nepieciešama sadarbības grupas darbībai. Minētos īstenošanas aktus pieņem saskaņā ar 22. panta 2. punktā minēto pārbaudes procedūru.

Piemērojot pirmo daļu, Komisija iesniedz pirmo īstenošanas akta projektu komitejai, kas minēta 22. panta 1.punktā, līdz ... [6 mēneši pēc šīs direktīvas stāšanās spēkā].

12. pants

CSIRT *tīkls*

1. Ar šo tiek izveidots valstu *CSIRT* tīkls, lai palīdzētu attīstīt paļāvību un uzticēšanos starp dalībvalstīm un veicinātu ātru un efektīvu operatīvo sadarbību.

2. *CSIRT* tīkls sastāv no dalībvalstu *CSIRT* un *CERT-EU* pārstāvjiem. Komisija piedalās *CSIRT* tīklā novērotāja statusā. *ENISA* nodrošina sekretariātu un aktīvi atbalsta sadarbību starp *CSIRT*.

3. *CSIRT* tīklam ir šādi uzdevumi:

   a) apmainīties ar informāciju par *CSIRT* pakalpojumiem, operācijām un sadarbības spējām;

   b) pēc tās dalībvalsts *CSIRT* pārstāvja lūguma, kuru, iespējams, skāris incidents, apmainīties ar un apspriest informāciju, kas nav komerciāli sensitīva un kas saistīta ar minēto incidentu, kā arī saistītos riskus; tomēr jebkuras dalībvalsts *CSIRT* var atteikties sniegt informāciju minētajās apspriedēs, ja pastāv risks, ka tas var kaitēt incidenta izmeklēšanai;

c) apmainīties ar un uz brīvprātības pamata darīt pieejamu nekonfidenciālu informāciju attiecībā uz atsevišķiem incidentiem;

d) pēc dalībvalsts *CSIRT* pārstāvja lūguma apspriest un, ja iespējams, apzināt saskaņotu reaģēšanu uz incidentu, kas ir identificēts tās pašas dalībvalsts jurisdikcijā;

e) nodrošināt dalībvalstīm atbalstu pārrobežu incidentu risināšanā, pamatojoties uz to brīvprātīgu savstarpējo palīdzību;

f) apspriest, izpētīt un apzināt operatīvās sadarbības turpmākos veidus, tostarp attiecībā uz:

   i) risku un incidentu kategorijām,

   ii) agrīno brīdināšanu,

   iii) savstarpēju palīdzību,

   iv) koordinēšanas principiem un kārtību, kad dalībvalstis reaģē uz pārrobežu riskiem un incidentiem;

g) informēt sadarbības grupu par savām darbībām un par operatīvās sadarbības turpmākajiem veidiem, kas apspriesti, ievērojot f) apakšpunktu, un lūgt norādījumus attiecībā uz tiem;

h) apspriest pieredzi, kas gūta mācībās saistībā ar tīklu un informācijas sistēmu drošību, tostarp tajās, ko organizējusi *ENISA*;

i) pēc atsevišķas *CSIRT* pieprasījuma apspriest minētās *CSIRT* spējas un sagatavotību;

j) izdot pamatnostādnes, lai atvieglotu operatīvās prakses konverģenci saistībā ar šā panta noteikumu piemērošanu attiecībā uz operatīvo sadarbību.

4. Pārskatam, kas minēts 23. pantā un līdz …[24 mēneši pēc šīs direktīvas spēkā stāšanās dienas], un pēc tam - ik pēc pusotra gada *CSIRT* tīkls sagatavo ziņojumu, kurā izvērtē pieredzi, kas gūta saistībā ar operatīvo sadarbību, kuru īsteno saskaņā ar šo pantu, tostarp secinājumus un ieteikumus. Minēto ziņojumu iesniedz arī sadarbības grupai.

5. *CSIRT* tīkls nosaka savu reglamentu.

13. pants

Starptautiskā sadarbība

Savienība saskaņā ar LESD 218. pantu var slēgt starptautiskus nolīgumus ar trešām valstīm vai starptautiskām organizācijām, ļaujot tām piedalīties un organizējot to dalību atsevišķās sadarbības grupas darbībās. Šādos nolīgumos ņem vērā vajadzību nodrošināt datu adekvātu aizsardzību.

IV NODAĻA
PAMATPAKALPOJUMU SNIEDZĒJU TĪKLU UN INFORMĀCIJAS SISTĒMU DROŠĪBA

14. pants

Drošības prasības un incidentu paziņošana

1. Dalībvalstis nodrošina, ka pamatpakalpojumu sniedzēji veic atbilstīgus un samērīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmu drošībai, ko tie izmanto savās darbībās. Ņemot vērā jaunākos tehniskos sasniegumus, ar minētajiem pasākumiem nodrošina radītajam riskam atbilstīgu tīklu un informācijas sistēmu drošības līmeni.

2. Dalībvalstis nodrošina, ka pamatpakalpojumu sniedzēji veic atbilstīgus pasākumus, lai novērstu un mazinātu tādu incidentu ietekmi, kuri skar to tīklu un informācijas sistēmu drošību, ko izmanto šādu pamatpakalpojumu sniegšanai, nolūkā nodrošināt minēto pakalpojumu nepārtrauktību.

3. Dalībvalstis nodrošina, ka pamatpakalpojumu sniedzēji bez nepamatotas kavēšanās paziņo kompetentajai iestādei vai *CSIRT* par incidentiem, kuriem ir būtiska ietekme uz to sniegto pamatpakalpojumu nepārtrauktību. Paziņojumos ietver informāciju, kas ļauj kompetentajai iestādei vai *CSIRT* noteikt jebkādu incidenta pārrobežu ietekmi. Paziņošana neuzliek paziņojošajai pusei lielāku atbildību.

4. Lai noteiktu incidenta ietekmes būtiskumu, jo īpaši ņem vērā šādus rādītājus:

a) pamatpakalpojuma traucējumu skarto lietotāju skaits;

b) incidenta ilgums;

c) ģeogrāfiskā izplatība attiecībā uz incidenta skarto vidi.

5. Pamatojoties uz informāciju, kas sniegta pamatpakalpojumu sniedzēja paziņojumā, kompetentā iestāde vai *CSIRT* informē citu(-as) skarto(-ās) dalībvalsti(-is), ja incidentam ir būtiska ietekme uz pamatpakalpojumu nepārtrauktību minētajā dalībvalstī. To darot, kompetentā iestāde vai *CSIRT* saskaņā ar Savienības tiesību aktiem vai valsts tiesību aktiem, kas atbilst Savienības tiesību aktiem, nodrošina pamatpakalpojumu sniedzēja drošību un komerciālās intereses, kā arī informācijas konfidencialitāti, kas sniegta tā paziņojumā.

Ja apstākļi to ļauj, kompetentā iestāde vai *CSIRT* paziņojošajam pamatpakalpojumu sniedzējam sniedz atbilstīgu informāciju attiecībā uz pēcpasākumiem saistībā ar paziņojumu, piemēram, informāciju, kas varētu palīdzēt efektīvi atrisināt incidentu.

Pēc kompetentās iestādes vai *CSIRT* pieprasījuma vienotais kontaktpunkts nosūta pirmajā daļā minētos paziņojumus vienotajiem kontaktpunktiem citās skartajās dalībvalstīs.

6. Pēc apspriešanās ar pamatpakalpojumu sniedzēju, kas sniedzis paziņojumu, kompetentā iestāde vai *CSIRT* var informēt sabiedrību par atsevišķiem incidentiem, ja sabiedrības informētība ir nepieciešama, lai novērstu incidentu vai risinātu notiekošo incidentu.

7. Kompetentās iestādes, kas kopā darbojas sadarbības grupā, var izstrādāt un pieņemt pamatnostādnes par apstākļiem, kādos pamatpakalpojumu sniedzējiem ir pienākums paziņot par incidentiem, tostarp par rādītājiem, lai noteiktu incidenta ietekmes būtiskumu, kā minēts 4. punktā.

15. pants

Īstenošana un izpilde

1. Dalībvalstis nodrošina, ka kompetentajām iestādēm ir vajadzīgās pilnvaras un līdzekļi, lai izvērtētu to, kā pamatpakalpojumu sniedzēji pilda savus 14. pantā noteiktos pienākumus, un to ietekmi uz tīklu un informācijas sistēmu drošību.

2. Dalībvalstis nodrošina, ka kompetentajām iestādēm ir pilnvaras un līdzekļi, lai pieprasītu pamatpakalpojumu sniedzējiem sniegt:

   a) informāciju, kas vajadzīga to tīklu un informācijas sistēmu drošības izvērtēšanai, tostarp informēt par dokumentētu drošības politiku;

b) pierādījumus par efektīvu drošības politikas īstenošanu, piemēram, tādas drošības revīzijas rezultātus, ko veic kompetentā iestāde vai kvalificēts revidents, un – kvalificēta revidenta gadījumā – tās rezultātus, tostarp pamatā esošos pierādījumus, darīt pieejamus kompetentajai iestādei.

Pieprasot šādu informāciju vai pierādījumus, kompetentā iestāde norāda pieprasījuma nolūku un konkretizē, kāda informācija tiek prasīta.

3. Pēc informācijas izvērtējuma vai drošības revīziju rezultātiem, kas minēti 2. punktā, kompetentā iestāde pamatpakalpojumu sniedzējiem var izdot saistošus norādījumus par to, kā koriģēt identificētos trūkumus.

4. Pievēršoties incidentiem, kuru rezultātā notiek personas datu aizsardzības pārkāpumi, kompetentā iestāde strādā ciešā sadarbībā ar personas datu aizsardzības iestādēm.

V NODAĻA
DIGITĀLO PAKALPOJUMU SNIEDZĒJU TĪKLU UN INFORMĀCIJAS SISTĒMU DROŠĪBA

16. pants

Drošības prasības un incidentu paziņošana

1. Dalībvalstis nodrošina, ka digitālo pakalpojumu sniedzēji apzina un veic atbilstīgus un samērīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu riskus, kas tiek radīti tādu tīklu un informācijas sistēmu drošībai, ko tie izmanto saistībā ar III pielikumā minēto pakalpojumu piedāvāšanu Savienībā. Ņemot vērā jaunākos tehniskos sasniegumus, ar minētajiem pasākumiem nodrošina radītajam riskam atbilstīgu tīklu un informācijas sistēmu drošības līmeni un ņem vērā šādus elementus:

   a) sistēmu un iekārtu drošība,

   b) incidentu risināšana,

   c) darījumdarbības nepārtrauktības pārvaldība,

   d) uzraudzība, revīzijas un pārbaudes,

   e) atbilstība starptautiskajiem standartiem.

2. Dalībvalstis nodrošina, ka digitālo pakalpojumu sniedzēji veic pasākumus, lai novērstu un mazinātu incidentu, kas skar to tīklu un informācijas sistēmu drošību, ietekmi uz III pielikumā minētajiem pakalpojumiem, kurus piedāvā Savienībā, nolūkā nodrošināt minēto pakalpojumu nepārtrauktību.

3. Dalībvalstis nodrošina, ka digitālo pakalpojumu sniedzēji bez nepamatotas kavēšanās paziņo kompetentajai iestādei vai *CSIRT* par jebkuru incidentu, kam ir būtiska ietekme uz tā pakalpojuma sniegšanu, kas minēts III pielikumā un ko tie piedāvā Savienībā. Paziņojumos ietver informāciju, kas ļauj kompetentajai iestādei vai *CSIRT* noteikt jebkādas pārrobežu ietekmes būtiskumu. Paziņošana neuzliek paziņojošajai pusei lielāku atbildību.

4. Lai noteiktu, vai incidenta ietekme ir būtiska, jo īpaši ņem vērā šādus rādītājus:

   a) incidenta skarto lietotāju – jo īpaši to, kuri attiecīgo pakalpojumu izmanto paši savu pakalpojumu sniegšanai, – skaitu;

   b) incidenta ilgumu;

   c) ģeogrāfisko izplatību attiecībā uz incidenta skarto vidi;

   d) to, cik lielā mērā tiek traucēta pakalpojuma darbība;

   e) to, cik lielā mērā tiek ietekmētas ekonomiskās un sabiedriskās darbības.

Pienākumu paziņot par incidentu piemēro tikai tad, ja digitālo pakalpojumu sniedzējam ir piekļuve informācijai, kura ir nepieciešama, lai izvērtētu incidentu attiecībā uz pirmajā daļā minētajiem rādītājiem.

5. Ja pamatpakalpojumu sniedzējs paļaujas uz trešo personu digitālo pakalpojumu sniedzēju attiecībā uz tāda pakalpojuma sniegšanu, kas ir būtisks īpaši svarīgu sabiedrisko un ekonomisko darbību nodrošināšanai, minētais sniedzējs paziņo par jebkādu būtisku ietekmi uz pamatpakalpojumu nepārtrauktību sakarā ar incidentu, kas skar digitālo pakalpojumu sniedzēju.

6. Attiecīgā gadījumā un jo īpaši tad, ja 3. punktā minētais incidents skar divas vai vairāk dalībvalstis, kompetentā iestāde vai *CSIRT* informē citas skartās dalībvalstis. To darot, kompetentās iestādes, *CSIRT* un vienotie kontaktpunkti saskaņā ar Savienības tiesību aktiem vai valsts tiesību aktiem, kas atbilst Savienības tiesību aktiem, nodrošina digitālo pakalpojumu sniedzēja drošību un komerciālās intereses, kā arī sniegtās informācijas konfidencialitāti.

7. Pēc apspriešanās ar attiecīgo digitālo pakalpojumu sniedzēju kompetentā iestāde vai *CSIRT* un – attiecīgā gadījumā – citu attiecīgo dalībvalstu iestādes vai *CSIRT* var informēt sabiedrību par atsevišķiem incidentiem vai pieprasīt to darīt digitālo pakalpojumu sniedzējam, ja sabiedrības informētība ir nepieciešama, lai novērstu incidentu vai risinātu notiekošo incidentu, vai arī ja incidenta publiskošana kādā citādā ziņā ir sabiedrības interesēs.

8. Komisija pieņem īstenošanas aktus, lai vēl sīkāk precizētu šā panta 1. punktā minētos elementus un 4. punktā minētos parametrus. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 22. panta 2. punktā līdz ... [1 gads pēc šīs direktīvas stāšanās spēkā].

9. Komisija var pieņemt īstenošanas aktus, nosakot formātus un procedūras, kas piemērojamas paziņošanas prasībām. Minētos īstenošanas aktus pieņem saskaņā ar 22. panta 2. punktā minēto pārbaudes procedūru.

10. Neskarot 1. panta 6.b punktu, dalībvalstis digitālo pakalpojumu sniedzējiem nenosaka nekādas papildu drošības vai paziņošanas prasības.

11. V nodaļu nepiemēro mikrouzņēmumiem un mazajiem uzņēmumiem, kā definēts Komisijas Ieteikumā 2003/361/EK [1].

17. pants

Īstenošana un izpilde

1. Dalībvalstis nodrošina, ka kompetentās iestādes rīkojas, ja nepieciešams, izmantojot *ex post* uzraudzības pasākumus, kad tām sniegti pierādījumi, ka digitālo pakalpojumu sniedzējs neatbilst 16. pantā noteiktajām prasībām. Šādus pierādījumus var iesniegt tādas citas dalībvalsts kompetentā iestāde, kurā tiek sniegts pakalpojums.

[1] Komisijas Ieteikums 2003/361/EK (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

2. Piemērojot 1. punktu, kompetentajām iestādēm ir nepieciešamās pilnvaras un līdzekļi, lai pieprasītu digitālo pakalpojumu sniedzējiem:

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

b) labot jebkādu 16. pantā noteikto prasību neizpildi.

3. Ja digitālo pakalpojumu sniedzēja galvenā uzņēmējdarbības vieta vai pārstāvis ir vienā dalībvalstī, bet tā tīkli un informācijas sistēmas atrodas vienā vai vairākās citās dalībvalstīs, tās dalībvalsts kompetentā iestāde, kurā ir galvenā uzņēmējdarbības vieta vai pārstāvis, un minēto citu dalībvalstu kompetentās iestādes sadarbojas un pēc vajadzības cita citai palīdz. Šāda palīdzība un sadarbība var attiekties uz informācijas apmaiņu starp attiecīgajām kompetentajām iestādēm un lūgumiem veikt uzraudzības pasākumus, kas minēti 2. punktā.

18. pants

Jurisdikcija un teritorialitāte

1. Piemērojot šo direktīvu, uzskata, ka digitālo pakalpojumu sniedzējs ir tās dalībvalsts jurisdikcijā, kurā ir tā galvenā uzņēmējdarbības vieta. Tiek uzskatīts, ka digitālo pakalpojumu sniedzēja galvenā uzņēmējdarbības vieta ir kādā dalībvalstī, ja tā galvenais birojs atrodas minētajā dalībvalstī.

2. Digitālo pakalpojumu sniedzējs, kas neveic uzņēmējdarbību Savienībā, bet, kā minēts III pielikumā, piedāvā pakalpojumus Savienībā, ieceļ pārstāvi Savienībā. Minētais pārstāvis veic uzņēmējdarbību vienā no tām dalībvalstīm, kurās tiek piedāvāti attiecīgie pakalpojumi. Uzskata, ka digitālo pakalpojumu sniedzējs ir tās dalībvalsts jurisdikcijā, kurā pārstāvis veic uzņēmējdarbību.

3. Pārstāvja iecelšana, ko veic digitālo pakalpojumu sniedzējs, neskar juridiskus procesus, kurus varētu ierosināt pret pašu digitālo pakalpojumu sniedzēju.

VI NODAĻA
STANDARTIZĀCIJA UN BRĪVPRĀTĪGA PAZIŅOŠANA

19. pants

Standartizācija

1. Lai sekmētu 14. panta 1. un 2. punkta un 16. panta 1. un 2. punkta konverģentu īstenošanu, dalībvalstis, neliekot izmantot konkrētu tehnoloģijas veidu vai nediskriminējot par labu tā izmantošanai, veicina tādu Eiropas vai starptautiski atzītu standartu un specifikāciju izmantošanu, kas ir atbilstīgi tīklu un informācijas sistēmu drošībai.

2. *ENISA* sadarbībā ar dalībvalstīm izstrādā konsultatīvus ieteikumus un pamatnostādnes par tehniskajām jomām, kas jāapsver saistībā ar 1. punktu, kā arī par jau esošajiem standartiem, tostarp dalībvalstu standartiem, kas ļautu aptvert minētās jomas.

20. pants

Brīvprātīga paziņošana

1. Neskarot 3. pantu, vienības, kuras nav identificētas kā pamatpakalpojumu sniedzēji un nav digitālo pakalpojumu sniedzēji, brīvprātīgi var paziņot par incidentiem, kuriem ir būtiska ietekme uz to sniegto pakalpojumu nepārtrauktību.

2. Apstrādājot paziņojumus, dalībvalstis rīkojas saskaņā ar 14. pantā izklāstīto procedūru. Dalībvalstis obligātos paziņojumus var apstrādāt, nosakot tiem prioritāti pār brīvprātīgajiem paziņojumiem. Brīvprātīgos paziņojumus apstrādā tikai tad, ja šāda apstrāde nerada nesamērīgu vai nepamatotu slogu attiecīgajām dalībvalstīm.

   Brīvprātīgas paziņošanas rezultātā paziņojošajai vienībai netiek uzlikti nekādi pienākumi, kas uz to neattiektos, ja tā nebūtu sniegusi minēto paziņojumu.

VII NODAĻA
NOBEIGUMA NOTEIKUMI

21. pants

Sankcijas

Dalībvalstis paredz noteikumus par sankcijām, ko piemēro par to valsts noteikumu pārkāpumiem, kuri pieņemti, ievērojot šo direktīvu, un veic visus vajadzīgos pasākumus, lai nodrošinātu to piemērošanu. Paredzētās sankcijas ir iedarbīgas, samērīgas un atturošas. Dalībvalstis līdz … [21 mēnesis pēc šīs direktīvas spēkā stāšanās dienas.] dara zināmus minētos noteikumus un pasākumus Komisijai un nekavējoties paziņo tai par jebkādiem turpmākiem grozījumiem, kas tos ietekmē.

22. pants

Komiteju procedūra

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

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

23. pants

Pārskatīšana

1. Līdz … [33 mēneši pēc šīs direktīvas spēkā stāšanās dienas] Komisija iesniedz ziņojumu Eiropas Parlamentam un Padomei, izvērtējot tās pieejas konsekvenci, ko dalībvalstis izmanto pamatpakalpojumu sniedzēju identifikācijā.

2. Komisija periodiski pārskata šīs direktīvas darbību un iesniedz ziņojumu Eiropas Parlamentam un Padomei. Šim nolūkam un lai turpinātu attīstīt stratēģisko un operatīvo sadarbību, Komisija ņem vērā sadarbības grupas un *CSIRT* tīkla ziņojumus par stratēģiskā un operatīvā līmenī gūto pieredzi. Veicot pārskatīšanu, Komisija izvērtē arī II un III pielikumā ietverto sarakstu un konsekvenci pamatpakalpojumu un II pielikumā minēto nozaru pakalpojumu sniedzēju identifikācijā. Pirmo ziņojumu iesniedz līdz …[57 mēneši pēc šīs direktīvas spēkā stāšanās dienas].

24. pants

Pārejas pasākumi

1. Neskarot 25. pantu un lai dalībvalstīm sniegtu papildu iespējas atbilstīgai sadarbībai transponēšanas laikposmā, sadarbības grupa un *CSIRT* tīkls sāk pildīt uzdevumus, kas izklāstīti attiecīgi 11. panta 3. punktā un 12. panta 3. punktā, līdz … [6 mēneši pēc šīs direktīvas spēkā stāšanās dienas].

2. Laikposmā no ... [6 mēneši pēc šīs direktīvas spēkā stāšanās dienas] līdz…[27 mēneši pēc šīs direktīvas spēkā stāšanās dienas] un nolūkā atbalstīt dalībvalstis konsekventas pieejas izmantošanā pamatpakalpojumu sniedzēju identifikācijas procesā sadarbības grupa apspriež to valsts pasākumu procesu, būtību un veidu, kas ļauj identificēt pamatpakalpojumu sniedzējus konkrētā nozarē saskaņā ar 5. un 6. pantā izklāstītajiem kritērijiem. Sadarbības grupa pēc dalībvalsts lūguma apspriež arī konkrētus minētās dalībvalsts pasākumu projektus, ar kuriem ļauj identificēt pamatpakalpojumu sniedzējus konkrētā nozarē saskaņā ar 5. un 6. pantā izklāstītajiem kritērijiem.

3. Līdz… [6 mēneši pēc šīs direktīvas spēkā stāšanās dienas], un piemērojot šo pantu, dalībvalstis nodrošina atbilstīgu pārstāvību sadarbības grupā un *CSIRT* tīklā.

25. pants

Transponēšana

1. Dalībvalstis līdz ... [21 mēnesis pēc šīs direktīvas stāšanās spēkā] pieņem un publicē normatīvos un administratīvos aktus, kas vajadzīgi, lai izpildītu šīs direktīvas prasības. Dalībvalstis tūlīt dara zināmu Komisijai minēto noteikumu tekstu.

   Tās minētos aktus piemēro no … [viena diena pēc pirmajā daļā minētās dienas].

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

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

26. pants

Stāšanās spēkā

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

27. pants

Adresāti

Šī direktīva ir adresēta dalībvalstīm.

…, … gada ….

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*

I PIELIKUMS

Datordrošības incidentu reaģēšanas vienību (*CSIRT*) prasības un uzdevumi

CSIRT prasības un uzdevumus adekvāti un skaidri nosaka un atbalsta valstu politika un/vai regulējums. Tie ietver turpmāk norādīto:

1) prasības attiecībā uz *CSIRT*:

   a) *CSIRT* nodrošina to komunikāciju pakalpojumu plašu pieejamības līmeni, izvairoties no atsevišķu informācijas ķēdes punktu kļūdainas darbības, un tai ir vairāki saziņas līdzekļi, kas jebkurā laikā ļauj ar to sazināties un nodrošina saziņu ar citiem. Turklāt saziņas kanāli ir skaidri norādīti un labi zināmi attiecīgām personām un sadarbības partneriem;

   b) *CSIRT* telpas un izmantotās informācijas sistēmas atrodas drošās vietās;

   c) darījumdarbības nepārtrauktība:

      i) *CSIRT* ir aprīkota ar atbilstīgu sistēmu pieprasījumu pārvaldībai un novirzīšanai, lai atvieglotu nodošanu,

      ii) *CSIRT* ir adekvāts darbinieku skaits, lai nodrošinātu pieejamību jebkurā brīdī,

      iii) *CSIRT* izmanto infrastruktūru, kurai ir nodrošināta nepārtrauktība. Minētajā nolūkā ir pieejamas dublējošās sistēmas un rezerves darba telpa;

d) *CSIRT* ir iespēja, jā tās to vēlas, piedalīties starptautiskos sadarbības tīklos;

2) *CSIRT* uzdevumi:

a) *CSIRT* uzdevumos ietilpst vismaz šādi uzdevumi:

i) incidentu uzraudzība valsts līmenī,

ii) agrīnās brīdināšanas, brīdināšanas, paziņojumu un informācijas izplatīšanas nodrošināšana attiecīgajām ieinteresētajām personām par riskiem un incidentiem,

iii) reaģēšana uz incidentiem,

iv) dinamiskas risku un incidentu analīzes un situācijas apzināšanas nodrošināšana,

v) dalība *CSIRT* tīklā;

b) *CSIRT* izveido sadarbības attiecības ar privāto sektoru;

c) lai atvieglotu sadarbību, *CSIRT* veicina kopīgas vai standartizētas prakses ieviešanu un izmantošanu attiecībā uz:

i) incidentu un risku risināšanas procedūrām,

ii) incidentu, risku un informācijas klasifikācijas shēmām.

II PIELIKUMS

Vienību veidi, piemērojot 4. panta 4. punktu

Nozare	Apakšnozare	Vienības veids
1. Enerģētika:	a) elektroenerģija:	– elektroenerģijas uzņēmums, kas definēts Eiropas Parlamenta un Padomes Direktīvas 2009/72/EK [1] 2. panta 35. punktā un kas veic "piegādes" funkciju, kā definēts minētās direktīvas 2. panta 19. punktā,
		– sadales sistēmas operatori, kā definēts Direktīvas 2009/72/EK 2. panta 6. punktā;
		– pārvades sistēmas operatori, kā definēts Direktīvas 2009/72/EK 2. panta 4. punktā;
	b) nafta:	– naftas pārvades cauruļvadu operatori,
		– naftas ražošanas operatori, pārstrādes un attīrīšanas iekārtas, uzglabāšana un pārvade;

[1] Eiropas Parlamenta un Padomes Direktīva 2009/72/EK (2009. gada 13. jūlijs) par kopīgiem noteikumiem attiecībā uz elektroenerģijas iekšējo tirgu un par Direktīvas 2003/54/EK atcelšanu (OV L 211, 14.8.2009., 55. lpp.).

Nozare	Apakšnozare	Vienības veids
	c) gāze:	– piegādes uzņēmumi, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2009/73/EK [1] 2. panta 8. punktā,
		– sadales sistēmas operatori, kā definēts Direktīvas 2009/73/EK 2. panta 6. punktā,
		– pārvades sistēmas operatori, kā definēts Direktīvas 2009/73/EK 2. panta 4. punktā,
		– uzglabāšanas sistēmas operatori, kā definēts Direktīvas 2009/73/EK 2. panta 10. punktā,
		– SDG sistēmas operatori, kā definēts Direktīvas 2009/73/EK 2. panta 12. punktā,
		– dabasgāzes uzņēmumi, kā definēts Direktīvas 2009/73/EK 2. panta 1. punktā,
		– dabasgāzes pārstrādes un attīrīšanas iekārtu operatori.

[1] Eiropas Parlamenta un Padomes Direktīva 2009/73/EK (2009. gada 13. jūlijs) par kopīgiem noteikumiem attiecībā uz dabasgāzes iekšējo tirgu un par Direktīvas 2003/55/EK atcelšanu (OV L 211, 14.8.2009., 94. lpp.).

Nozare	Apakšnozare	Vienības veids
2. Transports:	a) gaisa transports:	– gaisa pārvadātāji, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 300/2008 [1] 3. panta 4. punktā,
		– lidostu pārvaldības struktūras, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2009/12/EK [2] 2. panta 2. punktā, lidostas, kā definēts minētās direktīvas 2. panta 1. punktā, tostarp galvenās lidostas, kas uzskaitītas Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1315/2013 [3] II pielikuma 2. iedaļā; un vienības, kuras nodarbojas ar tādu palīgiekārtu ekspluatāciju, kuras atrodas lidostās,
		– satiksmes vadības kontroles operatori, kas sniedz gaisa satiksmes vadības (*ATC*) pakalpojumu, kā definēts Eiropas Parlamenta un Padomes Regulas (EK) Nr. 549/2004 [4] 2. panta 1. punktā;

[1] Eiropas Parlamenta un Padomes Regula (EK) Nr. 300/2008 (2008. gada 11. marts) par kopīgiem noteikumiem civilās aviācijas drošības jomā un ar ko atceļ Regulu (EK) Nr. 2320/2002 (OV L 97, 9.4.2008., 72. lpp.).

[2] Eiropas Parlamenta un Padomes Direktīva 2009/12/EK (2009. gada 11. marts) par lidostas maksām (OV L 70, 14.3.2009., 11. lpp.).

[3] Eiropas Parlamenta un Padomes Regula (ES) Nr. 1315/2013 (2013. gada 11. decembris) par Savienības pamatnostādnēm Eiropas transporta tīkla attīstībai un ar ko atceļ Lēmumu Nr. 661/2010/ES (OV L 348, 20.12.2013., 1. lpp.).

[4] Eiropas Parlamenta un Padomes Regula (EK) Nr. 549/2004 (2004. gada 10. marts), ar ko nosaka pamatu Eiropas vienotās gaisa telpas izveidošanai (Pamatregula) (OV L 96, 31.3.2004., 1. lpp.).

Nozare	Apakšnozare	Vienības veids
	b) dzelzceļa transports:	– infrastruktūras pārvaldītāji, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2012/34/ES [1] 3. panta 2. punktā,
		– dzelzceļa pārvadājumu uzņēmumi, kā definēts Direktīvas 2012/34/ES 3. panta 1. punktā, tostarp apkalpes vietas operatori, kā definēts Direktīvas 2012/34/ES 3. panta 12. punktā;
	c) ūdens transports:	– iekšējo, jūras un piekrastes ūdens transporta pasažieru un kravu pārvadājumu uzņēmumi, kā attiecībā uz jūras transportu definēts Eiropas Parlamenta un Padomes Regulas (EK) Nr. 725/2004 [2] I pielikumā, neietverot atsevišķus kuģus, kurus ekspluatē minētie uzņēmumi,
		– ostu pārvaldības struktūras, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2005/65/EK [3] 3. panta 1. punktā, tostarp to ostas iekārtas, kā definēts Regulas (EK) Nr. 725/2004 2. panta 11. punktā; un vienības, kas ekspluatē rūpnīcas un iekārtas, kuras atrodas ostās,

[1] Eiropas Parlamenta un Padomes Direktīva 2012/34/ES (2012. gada 21. novembris), ar ko izveido vienotu Eiropas dzelzceļa telpu (OV L 343, 14.12.2012., 32. lpp.).

[2] Eiropas Parlamenta un Padomes Regula (EK) Nr. 725/2004 (2004. gada 31. marts) par kuģu un ostas iekārtu drošības pastiprināšanu (OV L 129, 29.4.2004., 6. lpp.).

[3] Eiropas Parlamenta un Padomes Direktīva 2005/65/EK (2005. gada 26. oktobris) par ostu aizsardzības pastiprināšanu (OV L 310, 25.11.2005., 28. lpp.).

Nozare	Apakšnozare	Vienības veids
		– kuģu satiksmes dienestu operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2002/59/EK [1] 3. panta o) punktā;
	d) autotransports:	– par autoceļiem atbildīgās iestādes, kā definēts Komisijas Deleģētās regulas (ES) 2015/962 [2] 2. panta 12. punktā, kuras ir atbildīgas par satiksmes pārvaldības kontroli,
		– inteliģentu transporta sistēmu operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2010/40/ES [3] 4. panta 1. punktā;
3. Banku nozare:		kredītiestādes, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 575/2013 [4] 4. panta 1. punktā,

[1] Eiropas Parlamenta un Padomes Direktīva 2002/59/EK (2002. gada 27. jūnijs), ar ko izveido Kopienas kuģu satiksmes uzraudzības un informācijas sistēmu un atceļ Padomes Direktīvu 93/75/EEK (OV L 208, 5.8.2002., 10. lpp.).

[2] Komisijas Deleģētā regula (ES) 2015/962 (2014. gada 18. decembris), ar ko papildina Eiropas Parlamenta un Padomes Direktīvu 2010/40/ES attiecībā uz reāllaika satiksmes informācijas pakalpojumu nodrošināšanu visā ES (OV L 157, 23.6.2015., 21. lpp.).

[3] Eiropas Parlamenta un Padomes Direktīva 2010/40/ES (2010. gada 7. jūlijs) par pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomā un saskarnēm ar citiem transporta veidiem (OV L 207, 6.8.2010., 1. lpp.).

[4] Eiropas Parlamenta un Padomes Regula (ES) Nr. 575/2013 (2013. gada 26. jūnijs) par prudenciālajām prasībām attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām, un ar ko groza Regulu (ES) Nr. 648/2012 (OV L 176, 27.6.2013., 1. lpp.).

Nozare	Apakšnozare	Vienības veids
4. Finanšu tirgus infrastruktūras:		– tirdzniecības vietu operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2014/65/ES [1] 4. panta 24) punktā,
		– centrālie darījumu partneri (CDP), kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 648/2012 [2] 2. panta 1. punktā;
5. Veselības nozare:	Veselības aprūpes iestādes (tostarp slimnīcas un privātas klīnikas):	veselības aprūpes sniedzēji, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2011/24/ES [3] 3. panta g) punktā;
6. Dzeramā ūdens piegāde un izplatīšana:		ūdens, kas domāts dzeršanai piegādātāji un izplatītāji, kā definēts Padomes Direktīvas 98/83/EK [4] 2. panta 1. punkta a) apakšpunktā, taču izslēdzot izplatītājus, kuriem dzeramā ūdens izplatīšana ir tikai daļa no to veiktās patēriņa preču un pārējo preču izplatīšanas vispārējās darbības, ko neuzskata par pamatpakalpojumu sniegšanu.
7. Digitālā infrastruktūra:		– IPAP
		– DNS
		– *TLD*

---

[1] Eiropas Parlamenta un Padomes Direktīva 2014/65/ES (2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar ko groza Direktīvu 2002/92/EK un Direktīvu 2011/61/ES (OV L 173, 12.6.2014., 349. lpp.).

[2] Eiropas Parlamenta un Padomes Regula (ES) Nr. 648/2012 (2012. gada 4. jūlijs) par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem (OV L 201, 27.7.2012., 1. lpp.).

[3] Eiropas Parlamenta un Padomes Direktīva 2011/24/ES (2011. gada 9. marts) par pacientu tiesību piemērošanu pārrobežu veselības aprūpē (OV L 88, 4.4.2011., 45. lpp.).

[4] Padomes Direktīva 98/83/EK (1998. gada 3. novembris) par dzeramā ūdens kvalitāti (OV L 330, 5.12.1998., 32. lpp.).

III PIELIKUMS

Digitālo pakalpojumu veidi, piemērojot 4. panta 5.) punktu

1. Tiešsaistes tirdzniecības vieta

2. Tiešsaistes meklētājprogramma

3. Mākoņdatošanas pakalpojums