EIROPAS
KOMISIJA

Briselē, 4.10.2017.
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

PIELIKUMS

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

TID direktīvas potenciāla maksimāla izmantošana - kā efektīvi īstenot Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā

SATURS

PIELIKUMS

1. Ievads.

Šī pielikuma mērķis ir veicināt Direktīvas (ES) 2016/1148 par tīklu un informācijas sistēmu drošību visā Savienībā[1] (turpmāk "TID direktīva" vai "direktīva") efektīvu piemērošanu, ieviešanu un izpildi un palīdzēt dalībvalstīm nodrošināt ES tiesību aktu efektīvu piemērošanu. Konkrētāk, tam ir trīs specifiski mērķi: a) nodrošināt lielāku skaidrību valstu iestādēm par direktīvā iekļautajiem pienākumiem, kas skar šīs iestādes, b) nodrošināt to direktīvā noteikto pienākumu efektīvu izpildi, kas piemērojami vienībām, kurām ir pienākumi, kas skar drošības prasības un incidentu paziņošanu, un c) kopumā veicināt juridisko noteiktību visiem iesaistītajiem dalībniekiem.

Tālab šajā pielikumā sniegtas norādes par šādiem aspektiem, kas ir būtiski, lai sasniegtu TID direktīvas mērķi, t.i., nodrošinātu vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā ES, kas ir mūsu sabiedrisko un ekonomisko norišu pamatā:

- dalībvalstu pienākums pieņemt valsts stratēģiju par tīklu un informācijas sistēmu drošību (2. iedaļa);
- valstu kompetento iestāžu, vienotu kontaktpunktu un datordrošības incidentu reaģēšanas vienību izveide (3. iedaļa);
- drošības un incidentu paziņošanas prasības, kas piemērojamas pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem (4. iedaļa); kā arī
- saikne starp TID direktīvu un citiem tiesību aktiem (5. iedaļa).

Norāžu sagatavošanā Komisija ir izmantojusi direktīvas sagatavošanas gaitā apkopoto informāciju un analīzi, Eiropas Savienības Tīklu un informācijas drošības aģentūras ("*ENISA*") un sadarbības grupas informāciju. Tā ir arī izmantojusi atsevišķu dalībvalstu pieredzi. Kad nepieciešams, Komisija ir ievērojusi ES tiesību aktu interpretācijas pamatprincipus: TID direktīvas formulējumi, konteksts un mērķi. Tā kā direktīva vēl nav transponēta, Eiropas Savienības Tiesa (EST) vai valstu tiesas nav pieņēmušas nolēmumus. Tāpēc nav iespējams vadīties pēc judikatūras.

Šīs informācijas apkopošana vienā dokumentā var sniegt dalībvalstīm labu pārskatu par direktīvu un ņemt šo informāciju vērā savu nacionālo normatīvo aktu izstrādē. Vienlaikus Komisija uzsver, ka šis Pielikums nav saistošs un ar to nav paredzēts izveidot jaunus noteikumus. Galīgā kompetence interpretēt ES tiesību aktus ir EST.

[1] Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. Direktīva stājās spēkā 2016. gada 8. augustā.

2. Valsts tīklu un informācijas sistēmu drošības stratēģija.
Saskaņā ar TID direktīvas 7. pantu dalībvalstīm ir pienākums pieņemt valsts tīklu un informācijas sistēmu drošības stratēģiju, kuru var uzskatīt par ekvivalentu terminam Valsts kiberdrošības stratēģija ("VKDS") Valsts stratēģijas funkcija ir noteikt stratēģiskos mērķus un atbilstīgu politiku un regulatīvos pasākumus attiecībā uz kiberdrošību. VKDS jēdziens tiek plaši lietots starptautiskā un Eiropas mērogā, it īpaši kontekstā ar *ENISA* darbu ar dalībvalstīm pie valstu stratēģijām, kā rezultātā nesen sagatavots atjaunots VKDS labas prakses ceļvedis[2].

Šajā iedaļā Komisija skaidro, kā TID direktīva veicina dalībvalstu gatavību, jo tajā prasīts ieviest pamatīgas valstu tīklu un informācijas sistēmu drošības stratēģijas (7. pants). Šajā iedaļā aprakstīti šādi aspekti: (a) stratēģijas darbības joma un (b) saturs un pieņemšanas kārtība.

Kā turpmāk aprakstīts, TID direktīvas 7. panta pareiza transponēšana ir svarīga direktīvas mērķu sasniegšanai, un tas paredz, ka šīm mērķim jāpiešķir pietiekami finansiālie resursi un cilvēkresursi.

2.1. Valsts stratēģijas darbības joma.
Saskaņā ar 7. panta formulējumu, pienākums pieņemt VKDS attiecas tikai uz "II pielikumā minētajām nozarēm (t.i., enerģētika, transports, banku nozare, finanšu tirgus infrastruktūras, veselības nozare, dzeramā ūdens piegāde un izplatīšana un digitālā infrastruktūra) un III pielikumā minētajiem pakalpojumiem" (tiešsaistes tirdzniecības vieta, tiešsaistes meklētājprogramma, mākoņdatošanas pakalpojums).

Direktīvas 3. pants nosaka minimālās saskaņošanas principu, saskaņā ar kuru dalībvalstis var pieņemt vai saglabāt spēkā noteikumus nolūkā panākt augstāku tīklu un informācijas sistēmu drošības līmeni. Šī principa piemērošana pienākumam pieņemt VKDS ļauj dalībvalstīm aptvert vairāk nozaru un pakalpojumu, nekā noteikts direktīvas II un III pielikumā.

Pēc Komisijas uzskatiem un ņemot vērā TID direktīvas mērķi, t.i., panākt vienādi augstu līmeni tīklu un informācijas sistēmu drošībā visā Savienībā[3], būtu ieteicams izstrādāt valsts stratēģiju, kas aptvertu visas attiecīgās sabiedriskās un ekonomiskās sfēras, nevis tikai tās nozares un digitālos pakalpojumus, ko aptver TID direktīvas attiecīgi II un III pielikums. Tas ir saskaņā ar labāko starptautisko praksi (skatīt ITU vadlīnijas un OECD analīzi, kas minēta vēlāk) un TID direktīvu.

Kā turpmāk skaidrots, tas īpaši attiecas uz publiskās pārvaldes iestādēm, kas atbild par nozarēm un pakalpojumiem, kas nav minēti direktīvas II un III pielikumā. Publiskās pārvaldes iestādes var apstrādāt sensitīvu informāciju, tāpēc tās būtu jāiekļauj VKDS un pārvaldības plānos, kas novērš informācijas noplūdi un nodrošina pietiekamu šīs informācijas aizsardzību.

[2] *ENISA, Valstu kiberdrošības stratēģijas labā prakse* (2016.). Skatīt https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[3] Skatīt 1. panta 1. punktu

2.2. Saturs un valstu stratēģiju pieņemšanas kārtība.

Saskaņā ar TID direktīvas 7. pantu, VKDS jāiekļauj vismaz:

i) valsts tīklu un informācijas sistēmu drošības stratēģijas mērķi un prioritātes;
ii) pārvaldības sistēma, lai sasniegtu valsts tīklu un informācijas sistēmu drošības stratēģijas mērķus un prioritātes
iii) tādu pasākumu apzināšana, kas attiecas uz sagatavotību, reaģēšanu un atkopi, tostarp sadarbību starp publisko un privāto sektoru;
iv) norāde par izglītības, izpratnes veidošanas un apmācības programmām;
v) norāde par pētniecības un attīstības plāniem;
vi) riska izvērtējuma plāns, lai apzinātu riskus; kā arī
vii) dažādu dalībnieku saraksts, kas iesaistīti stratēģijas īstenošanā.

Ne 7. pants, ne atbilstīgais 29. apsvērums nenorāda prasības VKDS pieņemšanai un neraksturo precīzāk VKDS saturu. Attiecībā uz procesu un VKDS satura papildu elementiem Komisija uzskata turpmāk aprakstīto pieeju par vienu no veidiem, kas būtu piemērots VKDS pieņemšanai. Tā pamatā ir analīze par dalībvalstu un trešo valstu pieredzi savu stratēģiju pieņemšanā. Resurss sīkākas informācijas saņemšanai ir *ENISA* VKDS apmācību rīks, kas pieejams kā video klipi un lejupielādējams multivides fails tās tīmekļvietnē[4].

2.3. Process un risināmie jautājumi.

Valsts stratēģijas sagatavošanas un pēcākās pieņemšanas process ir sarežģīts un daudzšķautņains; lai tas būtu efektīvs un veiksmīgs, tam nepieciešama ilgstoša sadarbība ar kiberdrošības ekspertiem, pilsonisko sabiedrību un valsts politisko procesu. Pamatu pamats ir augstākā līmeņa administratīvs atbalsts vismaz valsts sekretāra vai līdzvērtīgā līmenī vadošajā ministrijā, kā arī politiskais atbalsts. Lai veiksmīgi pieņemtu VKDS, var apsvērt šādus piecus procesa soļus (skatīt 1. tabulu):

Pirmais solis — **no stratēģijas izrietošo pamatprincipu un stratēģisko mērķu noteikšana.**

Vispirms valstu kompetentajām iestādēm būtu jānosaka galvenie elementi, kas jāiekļauj VKDS, proti, kādi ir sasniedzamie rezultāti direktīvas izpratnē (7. panta 1. punkta a) apakšpunkts) "*mērķi un prioritātes*", kā šādi rezultāti papildina valstu sociālās un ekonomikas politikas un kā tie atbilst privilēģijai un pienākumam būt par Eiropas Savienības dalībvalsti. Mērķiem ir jābūt specifiskiem, izmērāmiem, sasniedzamiem, reāliem un ar noteiktu termiņu (*SMART*). Ilustratīvs piemērs: "*Mēs nodrošināsim, lai šīs [noteikta perioda] stratēģijas pamatā būtu precīzi un visaptveroši izmērāmi kritēriji, pēc kuriem mēs mērīsim virzību uz sasniedzamajiem rezultātiem*"[5]

Iepriekš minētais ietver arī politisko novērtējumu, vai ir iespējams saņemt pietiekami daudz budžeta līdzekļu, lai finansētu stratēģijas ieviešanu. Tas arī ietver stratēģijas iecerētās darbības

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool
[5] Fragments no AK Nacionālās kiberdrošības stratēģijas, 2016.–2021., 67. lpp.

jomas aprakstu un dažādas ieinteresēto pušu kategorijas no publiskā un privātā sektora, kam būtu jāiesaistās dažādu mērķu un pasākumu sagatavošanā.

Šo pirmo soli var izpildīt tematiskās darba grupās, kur piedalās augstākie ministrijas ierēdņi un politiķi un ko vada kiberspeciālisti ar profesionālām komunikācijas prasmēm, kuri var izskaidrot, kādas sekas mūsdienīgai digitālai ekonomikai un sabiedrībai rada kiberdrošības trūkums vai vāja kiberdrošība.

Otrais solis — **stratēģijas satura izstrāde.**

Stratēģijā būtu jāiekļauj veicinoši pasākumi, darbības ar izpildes termiņiem un galvenie darbības rādītāji rezultātu novērtējumam, pilnveidei un uzlabojumiem pēc noteiktā ieviešanas perioda. Šiem pasākumiem būtu jāatbalsta mērķis, prioritātes un rezultāti, pēc kuriem jāvadās kā pēc pamatprincipiem. Nepieciešamību iekļaut veicinošus pasākumus nosaka TID direktīvas 7. panta 1. punkta c) apakšpunkts.

Ieteicams izveidot vadošās ministrijas vadītu darba grupu, kas organizētu stratēģijas izstrādes procesu un atvieglotu informācijas saņemšanu. Šo varētu sasniegt, izveidojot vairākas izstrādes grupas, kurās piedalās attiecīgās amatpersonas un eksperti, kas katra nodarbotos ar kādu būtisku vispārīgo tematu, piemēram, riska novērtējums, ārkārtas rīcības plāns, incidentu pārvaldība, prasmju pilnveide, jautājuma svarīguma apziņas veicināšana, izpēte un rūpnieciskā attīstība u.c. Atsevišķi būtu jāuzaicina katra nozare (piemēram, enerģētika, transports u.c.), lai novērtētu, kāda būs ietekme, tostarp uz resursiem, ja tās tiks iekļautas, un izraudzītie pamatpakalpojumu sniedzēji un galvenie digitālo pakalpojumu sniedzēji, lai noteiktu prioritātes un iesniegtu priekšlikumus izstrādes procesam. Nozaru ieinteresēto dalībnieku iesaiste ir svarīga, ņemot vērā arī vajadzību nodrošināt saskaņotu direktīvas ieviešanu dažādās nozarēs, vienlaikus ievērojot nozaru specifiku.

Trešais solis — **pārvaldības sistēmas izveide.**

Lai pārvaldes sistēma būtu efektīva un produktīva, tai vajadzētu balstīties uz šādiem elementiem: galvenās ieinteresētās personas, izstrādes procesā noteiktās prioritātes un ierobežojumi un nacionālās administratīvās un politiskās struktūras. Būtu vēlama tieša pakļautība politiskajam līmenim, un pārvaldības sistēmai vajadzētu piešķirt lēmumu pieņemšanas un resursu sadales funkcijas, kā arī tā saņemtu informāciju no kiberdrošības ekspertiem un nozares ieinteresētajām personām. TID direktīvas 7. panta 1. punkta b) apakšpunkts norāda uz pārvaldības sistēmu un precīzi paredz, ka jānosaka "*valdības struktūru un citu attiecīgo dalībnieku funkcijas*".

Ceturtais solis — **stratēģijas uzmetuma sagatavošana un izskatīšana.**

Šajā posmā būtu jāsagatavo un jāizskata stratēģijas uzmetums, izmantojot stipro pušu, trūkumu, iespēju un draudu (SVID) analīzi, un tā varētu konstatēt, vai ir nepieciešams pārskatīt saturu. Pēc iekšējas izskatīšanas būtu jānotiek konsultācijām ar ieinteresētajām personām. Būtu svarīgi arī organizēt sabiedrisku apspriešanu, lai izskaidrotu, cik nozīmīgs ir

stratēģijas priekšlikums sabiedrībai, saņemtu informāciju no visiem iespējamiem avotiem un rastu atbalstu stratēģijas ieviešanai nepieciešamo resursu ieguvei.

Piektais solis — **oficiāla pieņemšana.**

Pēdējais solis ietver oficiālu pieņemšanu politiskajā līmenī un budžeta līdzekļu piešķiršanu, kas atspoguļo, cik lielu nozīmi attiecīgā dalībvalsts piešķir kiberdrošībai. Komisija aicina dalībvalstis, kad tās paziņo valsts stratēģijas dokumentu Komisijai saskaņā ar 7. panta 3. punktu, sniegt informāciju par budžetu, lai sasniegtu TID direktīvas mērķus. Budžeta un nepieciešamo cilvēkresursu piešķiršana ir izšķiroši svarīga efektīvai stratēģijas un direktīvas ieviešanai. Tā kā kiberdrošība joprojām ir samērā jauna un strauji augoša sabiedriskās kārtības joma, vairumā gadījumu nepieciešamas jaunas investīcijas, pat ja kopējā situācija valsts budžetā liek samazināt izdevumus un taupīt.

Konsultācijas par valstu stratēģiju izstrādes procesu un saturu var sniegt dažādas publiskas un akadēmiskas struktūras, piemēram, *ENISA*[6], Starptautiskā telekomunikāciju savienība (ITU)[7], OECD[8], Globālais kiberekspertīzes forums un Oksfordas Universitāte[9].

2.4. Konkrēti soļi, kas dalībvalstīm veicami līdz transponēšanas termiņam.

Pirms direktīvas pieņemšanas gandrīz visas dalībvalstis[10] jau ir publicējušas dokumentus, kas norādīti kā VKDS. Šī pielikuma 6. iedaļā minētas stratēģijas, kas šobrīd ieviestas katrā dalībvalstī[11]. Tajās parasti ietverti stratēģiski principi, vadlīnijas un mērķi, dažkārt — specifiski pasākumi, ar ko mazina ar kiberdrošību saistītus riskus.

Ņemot vērā, ka dažas no šīm stratēģijām tika pieņemtas pirms TID direktīvas pieņemšanas, tajās varētu nebūt visi 7. panta elementi. Lai nodrošinātu korektu transponēšanu, dalībvalstīm būs jāizanalizē trūkstošie elementi, salīdzinot savu VKDS saturu ar septiņām 7. pantā skaidri norādītajām prasībām attiecībā uz direktīvas II pielikumā minētajām nozarēm un III pielikumā minētajiem pakalpojumiem. Identificētos trūkumus pēc tam var novērst, pārskatot esošo VKDS vai lemjot par pilnīgu savas valsts TID stratēģijas principu pārstrādi no nulles. Iepriekš

---

[6] *ENISA, Valstu kiberdrošības stratēģijas labā prakse* (2016). Skatīt https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] ITU, *Nacionālās kiberdrošības stratēģijas ceļvedis* (2011). Skatīt http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
ITU 2017. gadā izlaidīs arī Valstu kiberdrošības stratēģijas rīkkopu (skatīt prezentācijuhttp://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

[8] OECD, *Kiberdrošības politikas izveide pagrieziena punktā: jaunas paaudzes nacionālo kiberdrošības stratēģiju analīze* (2012). Skatīt: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

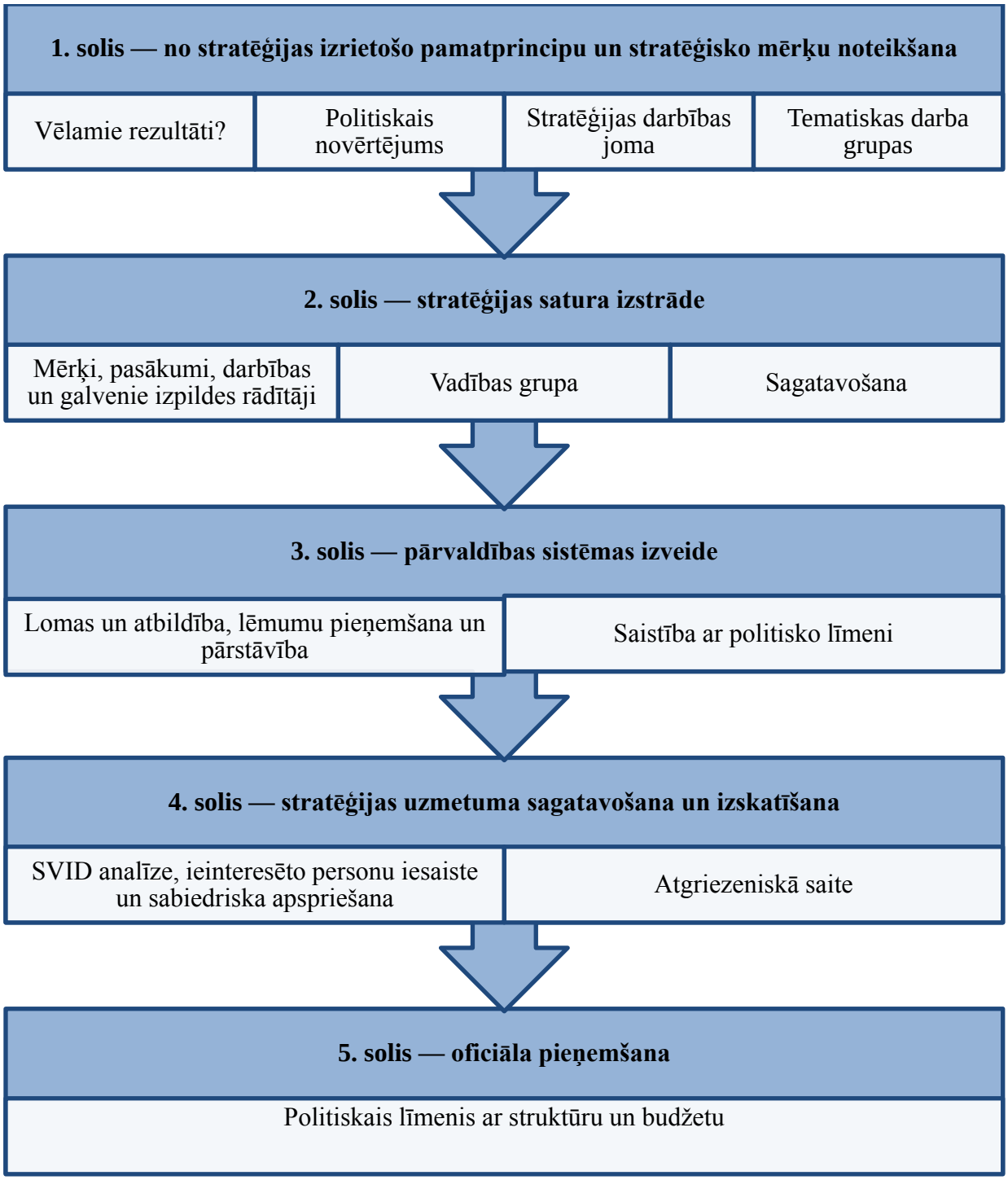
[9] Globālais kiberdrošības kapacitātes centrs un Oksfordas Universitāte, *Kiberdrošības kapacitātes brieduma modelis valstīm (KBM) - Pārstrādātais izdevums* (2016). Skatīt: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Izņemot Grieķiju, kur valsts kiberdrošības stratēģija tiek gatavota kopš 2014. gada (skatīthttps://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] Šī informācija ir sagatavota, balstoties uz VKDS pārskatu, ko sniegusi *ENISA* tīmekļvietnēhttps://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

minētās vadlīnijas par VKDS pieņemšanas procesu ir attiecināmas arī uz esošas VKDS pārskatīšanu un atjaunināšanu.

1. attēls. 5 soļu process VKDS pieņemšanai



3. TID direktīva: valstu kompetentās iestādes, vienots kontaktpunkts un datordrošības incidentu reaģēšanas vienības (*CSIRT*).

Saskaņā ar 8. panta 1. punktu dalībvalstīm ir pienākums izraudzīties vienu vai vairākas valsts kompetentās iestādes, kuru darbība attiecas vismaz uz direktīvas II pielikumā minētajām nozarēm un III pielikumā minētajiem pakalpojumiem un kuru uzdevums ir uzraudzīt direktīvas piemērošanu. Dalībvalstis var uzticēt šo funkciju esošai iestādei vai iestādēm.

Šajā iedaļā aprakstīts, kā TID direktīva vairo dalībvalstu gatavību, jo tajā paredzēts, ka ir nepieciešamas efektīvas valstu kompetentās iestādes un datordrošības incidentu reaģēšanas vienības (*CSIRT*). Precīzāk, šajā iedaļā iztirzāts pienākums izraudzīties valstu kompetentās iestādes, tostarp tās, kas pildīs vienota kontaktpunkta lomu. Tajā apskatītas trīs tēmas: (a) iespējamās valstu pārvaldības struktūras (piemēram, centralizēti, decentralizēti modeļi u.c.) un citas prasības; (b) vienota kontaktpunkta loma un (c) datordrošības incidentu reaģēšanas vienības.

3.1. Iestāžu veidi.

TID direktīvas 8. punkts nosaka dalībvalstīm pienākumu izraudzīties valsts kompetentās iestādes, kuras atbild par tīklu un informācijas sistēmu drošību, skaidri pieļaujot iespēju izraudzīties "*vienu vai vairākas valsts kompetentās iestādes*". Direktīvas 30. apsvērums paskaidro šādas pieejas izvēli: *"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".*

Tādējādi dalībvalstis var izvēlēties — izraudzīties vienu centrālo iestādi, kas atbild par visām direktīvas aptvertajām nozarēm un pakalpojumiem, vai vairākas iestādes atkarībā, piemēram, no nozares veida.

Lemjot par pieeju, dalībvalstis var vadīties no savas pieredzes saistībā ar esošo tiesisko regulējumu par informācijas kritiskās infrastruktūras aizsardzību (*CIIP*). Kā aprakstīts 1. tabulā, izstrādājot *CIIP* regulējumu, dalībvalstis kompetenču noteikšanā valsts līmenī nolēmušas izmantot centralizētu vai decentralizētu pieeju. Šeit valstu piemēri tiek izmantoti tikai ilustratīvā nolūkā un ar mērķi vērst dalībvalstu uzmanību uz esošajiem organizatoriskajiem ietvariem. Tādējādi Komisija neuzskata, ka attiecīgo valstu izmantotie *CIIP* regulējuma modeļi obligāti jāizmanto TID direktīvas transponēšanai.

Dalībvalstis var izvēlēties arī dažādus kombinētus pasākumus, kuros ietverti gan centralizētas, gan decentralizētas pieejas elementi. Izvēli var izdarīt saskanīgi ar iepriekšējiem nacionālajiem pārvaldības pasākumiem attiecībā uz direktīvas aptvertajām dažādajām nozarēm un pakalpojumiem vai no jauna pieņemtajiem pasākumiem, kurus pieņēmušas attiecīgās iestādes un attiecīgās ieinteresētās personas, kas identificētas kā pamatpakalpojumu sniedzēji un digitālo pakalpojumu sniedzēji. Svarīgi faktori, kas nosaka dalībvalstu izvēli, var būt arī speciālistu pieredze kiberdrošībā, finansēšanas apsvērumi, saikne starp ieinteresētajām personām un valsts interesēm (piemēram, ekonomikas attīstība, sabiedrības drošība utt.).

3.2 Publiskošana un citi nozīmīgi aspekti.

Saskaņā ar 8. panta 7. punktu dalībvalstīm ir jāinformē Komisija par izraudzīto valsts kompetento iestādi un tās uzdevumiem. Tas ir jāizdara līdz transponēšanas termiņa beigām.

Direktīvas 15. un 17. pants nosaka dalībvalstīm pienākumu nodrošināt, lai kompetentajām iestādēm būtu vajadzīgās pilnvaras un līdzekļi šajos pantos noteikto uzdevumu izpildei.

Turklāt noteiktu subjektu izraudzīšanās par valsts kompetento iestādi ir jāpublisko. Direktīva nenosaka, kādā veidā informācija ir jāpublisko. Tā kā šīs prasības mērķis ir nodrošināt TID aptverto subjektu un sabiedrības lielāku izpratni šajā jautājumā un ņemot vērā pieredzi citās nozarēs (telekomunikācijas, banku sektors, zāles), Komisija uzskata, ka to varētu darīt, piemēram, pietiekami plaši zināmā portālā.

TID direktīvas 8. panta 5. punkts nosaka, ka šādām iestādēm ir jābūt "adekvātiem resursiem", lai veiktu direktīvā noteiktos uzdevumus.

1. tabula. Valstu pieejas informācijas kritiskās infrastruktūras aizsardzībai (*CIIP*).

2016. gadā *ENISA* publicēja pētījumu[12] par dalībvalstu atšķirīgajām pieejām, ko tās izmanto, lai aizsargātu savu informācijas kritisko infrastruktūru. Tajā aprakstīti divi *CIIP* pārvaldības profili dalībvalstīs, kurus var izmantot saistībā ar TID direktīvas transponēšanu.

1. profils. Decentralizēta pieeja — vairākas dažādu nozaru iestādes, kas ir kompetentas par noteiktām nozarēm un pakalpojumiem, kas minēti direktīvas II un III pielikumā.

Decentralizētajai pieejai raksturīgi:

(i) subsidiaritātes princips;
(ii) spēcīga sadarbība starp publiskā sektora aģentūrām;
(iii)nozarspecifiski tiesību akti.

Subsidiaritātes princips.

Tā vietā, lai veidotu vai izraudzītos vienu aģentūru ar vispārēju atbildību, decentralizācijas pieejas pamatā ir subsidiaritātes princips. Tas nozīmē, ka atbildība par ieviešanu ir noteiktas nozares iestādes ziņā, kas vislabāk izprot attiecīgo nozari valstī un kurai jau ir izveidotas attiecības ar ieinteresētajām personām. Saskaņā ar šo principu lēmumus pieņem tā iestāde, kas atrodas vistuvāk jomai, ko lēmums skar.

Spēcīga sadarbība starp publiskā sektora aģentūrām.

Tā kā *CIIP* ir piesaistītas dažādas publiskā sektora aģentūras, daudzas dalībvalstis izveidojušas sadarbības shēmas, lai koordinētu dažādo iestāžu darbu un centienus. Šīs sadarbības shēmas var būt neformāli tīkli vai institucionalizētāki forumi vai pasākumi. Taču šīs sadarbības shēmas kalpo tikai informācijas apmaiņas nolūkā un dažādu publiskā sektora aģentūru darba koordinēšanai, taču tām nav noteicošas ietekmes pār tām.

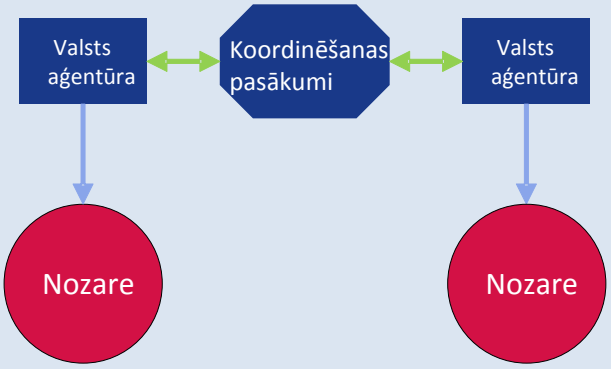
Nozarspecifiski tiesību akti.

Valstis, kas izvēlējušās decentralizētu pieeju kritisko nozaru jomā, bieži atturas no tiesiskā regulējuma par *CIIP*. Tā vietā likumus un noteikumus pieņem noteiktu nozaru ietvaros, un tādējādi tie var ievērojami atšķirties dažādās nozarēs. Šīs pieejas priekšrocība būtu ar TID saistītu pasākumu saskaņošana ar esošajiem nozarēm specifiskajiem noteikumiem, kas uzlabotu gan to pieņemšanu nozarē, gan ieviešanas efektivitāti, ko veiktu attiecīgā iestāde.

Pastāv būtisks risks, ka tiks mazināta direktīvas ieviešanas konsekvence dažādās nozarēs un dažādu pakalpojumu jomā, ja tiek izmantota tikai decentralizēta pieeja. Šādā gadījumā direktīva paredz vienotu valsts kontaktpunktu pārrobežu jautājumu risināšanai, un šai struktūrai attiecīgā dalībvalsts varētu uzdot koordinēt un organizēt iekšējo sadarbību daudzo valsts kompetento iestāžu starpā saskaņā ar direktīvas 10. pantu.

[12] *ENISA, Informācijas kritiskās infrastruktūras aizsardzības novērtēšana, analīze un ieteikumi* (2016). Skatīt: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

2. attēls. Decentralizēta pieeja.



Decentralizētas pieejas piemēri.

Zviedrija ir labs piemērs decentralizācijas principa ieviešanai *CIIP* jomā. Valsts izmanto "sistēmas perspektīvu", kas nozīmē, ka galvenie *CIIP* uzdevumi, piemēram, vitāli svarīgo pakalpojumu un kritiskās infrastruktūras identificēšana, uzturētāju koordinēšana un atbalstīšana, regulatīvie uzdevumi, kā arī pasākumi gatavībai ārkārtas situācijās, ir dažādu aģentūru un pašvaldību atbildībā. Šīs aģentūras ir Zviedrijas Civilās aizsardzības aģentūra (*MSB*), Zviedrijas Pasta un telekomunikāciju aģentūra (*PTS*) un vairākas Zviedrijas aizsardzības, militārās un tiesībaizsardzības aģentūras.

Lai koordinētu dažādo aģentūru un publisko struktūru darbību, Zviedrijas valdība ir izveidojusi sadarbības tīklu, kuru veido iestādes "ar tiešu atbildību par sabiedrības informācijas drošību". Šo Sadarbības grupu informācijas drošībai (*SAMFI*) veido dažādu iestāžu pārstāvji, tās dalībnieki tiekas vairākas reizes gadā, lai pārrunātu ar valsts informācijas drošību saistītus jautājumus. SAMFI darbojas galvenokārt politiski stratēģiskās jomās un aptver tādas tēmas kā tehniskie jautājumi un standartizācija, informācijas drošības attīstība valsts un starptautiskā mērogā vai IT incidentu pārvaldība un novēršana. (Zviedrijas Civilās aizsardzības aģentūra (MSB) 2015).

Zviedrija nav publicējusi centrālo likumu par *CIIP* informācijas kritiskās infrastruktūras (IKI) uzturētājiem dažādās nozarēs. Tā vietā attiecīgās publiskās pārvaldes iestādes ir atbildīgas par tāda regulējuma sagatavošanu, kas nosaka pienākumus konkrētu nozaru uzņēmumiem. Piemēram, MSB ir tiesīga izdot noteikumus valdības iestādēm informācijas drošības jomā, bet PTS var pieprasīt no uzņēmumiem, lai tie ievieš noteiktus tehniskus vai organizatoriskus drošības pasākumus, pamatojoties uz sekundāro regulējumu.

Īrija ir vēl viena valsts, kurā novērojamas šī profila iezīmes. Īrija ievēro "subsidiaritātes doktrīnu", kas nozīmē, ka katra ministrija atbild par IKI identificēšanu un riska novērtējumu savā nozarē. Turklāt valsts līmenī nav pieņemti konkrēti noteikumi par *CIIP*. Tiesiskais regulējums tiek īstenots pa nozarēm un pastāv galvenokārt enerģētikas un telekomunikāciju

nozarē (2015). Citi piemēri ir Austrija, Kipra un Somija.

2. profils. Centralizēta pieeja — viena centrāla iestāde, kas ir kompetenta par visām nozarēm un pakalpojumiem, kas minēti direktīvas II un III pielikumā.

Centralizētajai pieejai raksturīgi:

i) centrāla iestāde visām nozarēm;
ii) visaptverošs regulējums.

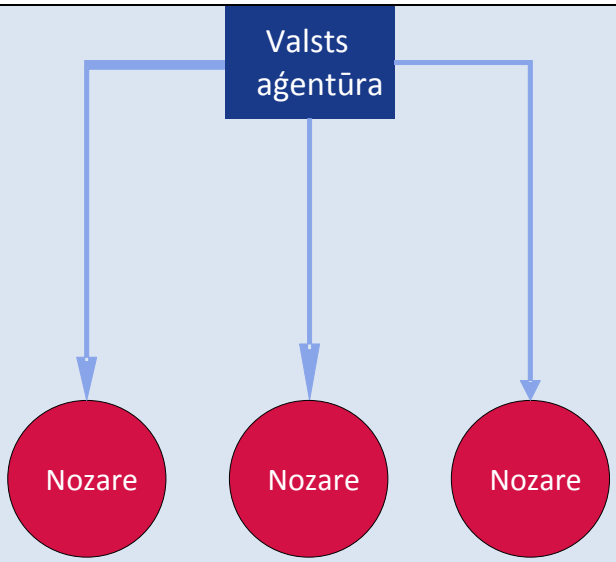
Centrāla iestāde visām nozarēm.

Dalībvalstis, kas ievēro centralizētu pieeju, ir izveidojušas iestādes ar pienākumiem un plašu kompetenci vairākās vai visās kritiski svarīgajās nozarēs vai ir paplašinājušas esošo iestāžu pilnvaras. Šīs galvenās *CIIP* iestādes risina vairākus uzdevumus, piemēram, plāni ārkārtas situācijām, ārkārtas situāciju pārvaldība, regulatīvie uzdevumi un privātu pakalpojumu sniedzēju atbalsts. Daudzkārt valsts vai valdības *CSIRT* ir daļa no galvenās *CIIP* iestādes. Centrālajā iestādē visdrīzāk būs vairāk augstāka līmeņa kiberdrošības speciālistu nekā vairākās nozaru iestādēs, ņemot vērā vispārējo kiberprasmju trūkumu.

Visaptverošs regulējums.

Visaptverošs regulējums nosaka pienākumus un prasības visiem IKI pakalpojumu sniedzējiem visās nozarēs. To panāk ar jauniem visaptverošiem likumiem vai esošā nozarspecifiskā regulējuma papildināšanu. Šāda pieeja veicinātu konsekventu TID direktīvas piemērošanu attiecībā uz visām tās aptvertajām nozarēm un pakalpojumiem. Tas ļautu izvairīties no nepilnīgas ieviešanas riska, kas varētu rasties, ja darbojas vairākas iestādes atsevišķās jomās.

3. attēls. Centralizēta pieeja.



Centralizētas pieejas piemēri

Francija ir labs piemērs ES dalībvalstij, kas izmanto centralizētu pieeju. 2011. gadā Francijas Informācijas sistēmu drošības nacionālā aģentūra (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) tika atzīta par galveno valsts iestādi, kas nodarbojas ar informācijas sistēmu aizsardzību. ANSSI stingri uzrauga "būtiski svarīgu pakalpojumu sniedzējus" (BSPS): aģentūra var norīkot BSPS ievērot drošības pasākumus, un tā ir pilnvarota veikt drošības auditus to uzņēmumos; Turklāt tā ir galvenais vienotais kontaktpunkts BSPS, kuriem ir pienākums ziņot par drošības incidentiem aģentūrai.

Drošības incidentu gadījumos ANSSI rīkojas kā *CIIP* ārkārtas situāciju aģentūra un lemj par pasākumiem, kas jāveic pakalpojumu sniedzējiem, lai reaģētu krīzes situācijā. Valdības rīcību koordinē ANSSI operatīvajā centrā. Draudu konstatēšanu un reaģēšanu incidentu gadījumā operatīvā līmenī veic CERT-FR, kas ir daļa no ANSSI.

Francija ir izstrādājusi visaptverošu *CIIP* tiesisko regulējumu. 2006. gadā premjers uzdeva izveidot kritiskās infrastruktūras nozaru sarakstu. Pamatojoties uz šo sarakstu, kurā identificētas divpadsmit svarīgākās nozares, valdība ir noteikusi aptuveni 250 BSPS. 2013. gadā tika izsludināts Militārās programmēšanas likums (MPL).[13] Tas nosaka dažādus pienākumus BSPS, piemēram, ziņošanu par incidentiem vai drošības pasākumu ieviešanu. Šīs prasības ir obligātas visiem BSPS visās nozarēs (Francijas Senāts 2013).

[13] La loi de programmation militaire

3.3. TID direktīvas 9. pants Datordrošības incidentu reaģēšanas vienības (*CSIRT*).

Saskaņā ar 9. pantu dalībvalstīm ir pienākums izraudzīties vienu vai vairākas *CSIRT*, kuras ir atbildīgas par incidentu un risku risināšanu TID direktīvas II pielikumā minētajās nozarēs un III pielikumā minētajiem pakalpojumiem. Ņemot vērā direktīvas 3. pantā noteikto prasību par minimālo saskaņošanu, dalībvalstis var izmantot *CSIRT* arī citās nozarēs, kuras direktīva neaptver, piemēram, publiskajā pārvaldē.

Dalībvalstis var izveidot *CSIRT* valsts kompetentajā iestādē[14].

3.4. Uzdevumi un prasības.

CSIRT uzdevumi, kas noteikti TID direktīvas I pielikumā:

- incidentu uzraudzība valsts līmenī;
- agrīnās brīdināšanas, brīdināšanas, paziņojumu un informācijas izplatīšanas nodrošināšana attiecīgajām ieinteresētajām personām par riskiem un incidentiem;
- reaģēšana uz incidentiem,
- dinamiskas risku un incidentu analīzes un situācijas apzināšanas nodrošināšana; kā arī
- dalība valsts *CSIRT* tīklā (*CSIRT* tīkls), kas izveidots saskaņā ar 12. pantu.

14. panta 3. punktā, 14. panta 5. punktā, 14. panta 6. punktā, 16. panta 3. punktā, 16. panta 6. punktā un 16. panta 7. punktā ir noteikti papildu uzdevumi attiecībā tieši uz incidentu paziņošanu, ja dalībvalsts nolemj, ka *CSIRT* papildus valsts kompetentajām iestādēm vai to vietā var uzņemties šādus pienākumus.

Transponējot direktīvu, dalībvalstīm ir dažādi varianti, kāda ir *CSIRT* loma incidentu paziņošanas prasību izpildē. Ir iespējama tieša obligāta ziņošana *CSIRT*, kuras priekšrocība ir administratīvā efektivitāte, bet dalībvalstis var izvēlēties arī tiešu pakļautību valsts kompetentajām iestādēm, kad *CSIRT* ir tiesības uz piekļuvi paziņotajai informācijai. *CSIRT* galu galā ir ieinteresētas problēmu risināšanā — kā nepieļaut kiberincidentus, kā tos atklāt, kā uz tiem reaģēt un kā mazināt to ietekmi (tostarp to, par kuriem nav kritiski svarīgi ziņot obligāti) — kopā ar ieinteresētajām personām, bet atbilstība regulējumam ir valsts kompetentās iestādes jautājums.

Saskaņā ar direktīvas 9. panta 3. punktu dalībvalstīm jānodrošina, ka *CSIRT* ir piekļuve drošai un noturīgai IKT infrastruktūrai.

Direktīvas 9. panta 4. punkts nosaka dalībvalstīm pienākumu informēt Komisiju par *CSIRT* uzdevumu jomu, kā arī incidentu risināšanas procesa galvenajiem elementiem.

Prasības dalībvalstu izraudzītajām *CSIRT* ir minētas TID direktīvas I pielikumā. *CSIRT* nodrošina savu komunikāciju pakalpojumu plašu pieejamības līmeni. To telpas un izmantotās

[14] Skatīt 9. panta 1. punkta pēdējo teikumu.

informācijas sistēmas atrodas drošās vietās un spēj nodrošināt darījumdarbības nepārtrauktību. Turklāt *CSIRT* ir jābūt iespējai piedalīties starptautiskos sadarbības tīklos.

3.5. Palīdzība *CSIRT* izveidē.

Eiropas infrastruktūras savienošanas (EISI) Kiberdrošības digitālo pakalpojumu infrastruktūras (DSI) programma var nodrošināt ievērojamu ES finansējumu, ar ko dalībvalstu *CSIRT* tiek palīdzēts uzlabot spējas un savstarpēju sadarbību informācijas apmaiņas un sadarbības mehānismā. Sadarbības mehānisms, kas tiek izstrādāts SMART 2015/1089 projektā, ir paredzēts, lai veicinātu ātru un efektīvu operatīvo sadarbību pēc brīvprātības principa starp dalībvalstu *CSIRT*, proti, tā tiek atbalstīta to *CSIRT* tīklam uzdoto uzdevumu izpilde, kas tam uzdota saskaņā ar direktīvas 12. pantu.

Sīkāka informācija par uzaicinājumiem iesniegt priekšlikumus par dalībvalstu *CSIRT* spēju pilnveidošanu ir pieejama Eiropas Komisijas Inovācijas un tīklu izpildaģentūras (*INEA*) tīmekļvietnē[15].

EISI Kiberdrošības DSI pārvaldības padome ir neformāla struktūra, ka sniedz norādes par rīcībpolitiku un palīdzību dalībvalstu *CSIRT* nolūkā stiprināt to spējas un ieviest brīvprātīgu sadarbības mehānismu.

No jauna izveidotas *CSIRT* vai *CSIRT*, kam uzdots izpildīt TID direktīvas I pielikumā minētos uzdevumus, var paļauties uz *ENISA* konsultācijām un pieredzi, lai uzlabotu savu darbību un efektīvi veiktu savu darbu[16]. Šajā sakarā ir jānorāda, ka dalībvalstu *CSIRT* var vadīties pēc *ENISA* pēdējā laikā paveiktā. Konkrētāk, kā norādīts šī pielikuma 7. iedaļā, aģentūra ir izdevusi vairākus dokumentus un pētījumus, kas raksturo labo praksi, un tehniskus ieteikumus, tostarp *CSIRT* brieduma līmeņa novērtējumus, attiecībā uz dažādām *CSIRT* spējām un pakalpojumiem. Turklāt *CSIRT* tīkli ir dalījušies ar vadlīnijām un labo praksi gan vispasaules (*FIRST*[17]), gan Eiropas mērogā (*Trusted Introducer, TI*[18]).

3.6. Vienota kontaktpunkta loma.

Saskaņā ar TID direktīvas 8. panta 3. punktu katrai dalībvalstij jāizraugās valsts vienotais kontaktpunkts, kurš koordinē sadarbību, lai nodrošinātu pārrobežu sadarbību ar attiecīgajām iestādēm citās dalībvalstīs, ar sadarbības grupu un *CSIRT* tīklu[19], kas izveidoti ar direktīvu. 31. apsvērums un 8. panta 4. punkts skaidro šīs prasības pamatojumu, t.i., veicināt pārrobežu sadarbību un saziņu. Tas jo īpaši nepieciešams tāpēc, ka dalībvalstis var izlemt izveidot vairākas valsts iestādes. Tādējādi vienots kontaktpunkts veicinātu dažādu dalībvalstu iestāžu identificēšanu un sadarbību.

Vienotā kontaktpunkta sadarbības koordinācijas funkcija, visticamāk, ietvers saziņu ar sadarbības grupas un *CSIRT* tīkla sekretariātiem tādos gadījumos, ja valsts vienotais kontaktpunkts nav ne *CSIRT*, ne sadarbības grupas dalībnieks. Turklāt dalībvalstīm

[15] Skatīt: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Skatīt TID direktīvas 9. panta 5. punktu.
[17] Incidentu risināšanas un drošības grupu forums (https://www.first.org/)
[18] https://www.trusted-introducer.org/
[19] Valstu CSIRT tīkls operatīvai sadarbībai dalībvalstu starpā saskaņā ar 12. pantu

jānodrošina, ka vienotais kontaktpunkts tiek informēts par pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju paziņojumiem[20].

Direktīvas 8. panta 3. punkts norāda, ka, ja dalībvalsts izvēlas centralizētu pieeju, t.i., izraugās tikai vienu kompetento iestādi, šī iestāde ir arī vienotais kontaktpunkts. Ja dalībvalsts izvēlas decentralizētu pieeju, tā varētu par vienoto kontaktpunktu iecelt vienu no vairākām kompetentajām iestādēm. Neatkarīgi no izvēlētā institucionālā modeļa, ja kompetentā iestāde, *CSIRT* un vienotais kontaktpunkts ir dažādi subjekti, dalībvalstīm ir pienākums nodrošināt efektīvu sadarbību to starpā, lai izpildītu direktīvā noteiktos pienākumus[21].

Informācija par vienoto kontaktpunktu ir jāiesniedz līdz 2018. gada 9. augustam, un pēc tam katru gadu ir jāiesniedz kopsavilkuma ziņojums sadarbības grupai par saņemtajiem paziņojumiem, kurā norādīts paziņojumu skaits, paziņojumu raksturs un iestāžu veiktie pasākumi, piemēram, citu skarto dalībvalstu informēšana par incidentu vai attiecīgas informācijas sniegšana paziņojošajam uzņēmumam incidenta novēršanai[22]. Pēc kompetentās iestādes vai *CSIRT* pieprasījuma vienotajam kontaktpunktam ir jāpārsūta pamatpakalpojumu sniedzēju paziņojumi vienotajiem kontaktpunktiem citās incidentu skartajās dalībvalstīs[23].

Dalībvalstīm līdz transponēšanas termiņa beigām ir jāinformē Komisija par vienota kontaktpunkta izraudzīšanos un tā uzdevumiem. Vienotā kontaktpunkta izraudzīšanās ir jāpublisko tāpat, kā tiek publiskotas valstu kompetentās iestādes. Komisija publicē izraudzīto vienoto kontaktpunktu sarakstu.

3.7. Sankcijas

21. pants dalībvalstīm ļauj lemt par piemērojamo sankciju veidu un raksturu, ar nosacījumu, ka tās būs iedarbīgas, samērīgas un atturošas. Citiem vārdiem sakot, dalībvalstis principā var brīvi lemt par maksimālo sankciju apmēru, kas tiek noteikts to tiesību aktos, bet noteiktajai summai vai procentuālajam apmēram jābūt tādām, lai valsts iestādēm katrā atsevišķā gadījumā varētu piemērot iedarbīgas, samērīgas un atturošas sankcijas, ņemot vērā dažādus faktorus, piemēram, pārkāpuma nopietnību vai biežumu.

4. Vienības, kurām ir pienākumi saistībā ar drošības prasībām un incidentu paziņošanu.

Vienībām, kam ir svarīga loma sabiedrībā un ekonomikā un kas minētas direktīvas 4. panta 4. punktā un 4. panta 5. punktā kā pamatpakalpojumu sniedzēji (PS) un digitālo pakalpojumu sniedzēji (DPS), ir pienākums veikt piemērotus drošības pasākumus un paziņot par nopietniem incidentiem attiecīgām valstu iestādēm. *Pamatojums* — drošības incidentu ietekme var radīt būtiskus draudus tādu pakalpojumu darbībai, un tas var radīt būtiskus

[20] Skatīt 10. panta 3. punktu
[21] Skatīt 10. panta 1. punktu
[22] Turpat.
[23] Skatīt 14. panta 5. punktu

traucējumus saimnieciskajai darbībai un sabiedrībai kopumā, potenciāli apdraudēt lietotāju uzticēšanos un radīt lielu kaitējumu Savienības ekonomikai[24].

Šajā iedaļā sniegts pārskats par vienībām, kas ietilpst direktīvas II un III pielikumu darbības jomā, un uzskaitīti to pienākumi. Plaši skaidrota pamatpakalpojumu sniedzēju identificēšana, ņemot vērā šī procesa nozīmi saskaņotas TID direktīvas ieviešanā visā ES. Sniegti arī plaši skaidrojumi digitālās infrastruktūras un digitālo pakalpojumu sniedzēju definīcijām. Izvērtēta vēl citu nozaru iespējamā iekļaušana un arī sīkāk izskaidrota specifiskā pieeja attiecībā uz DPS.

4.1. Pamatpakalpojumu sniedzēji (PS).

TID direktīva tieši nenosaka, kādas tieši vienības tiks uzskatītas par PS tās izpratnē. Tā vietā tā norāda kritērijus, kas dalībvalstīm būs jāpiemēro, lai veiktu identifikācijas procesu, kas galu galā noteiks, tieši kuri atsevišķie uzņēmumi, kas atbilst II pielikumā uzskaitītajiem vienību veidiem, tiks uzskatīti par pamatpakalpojumu sniedzējiem un uz kuriem tā rezultātā attieksies direktīvā noteiktie pienākumi.

4.1.1. TID direktīvas II pielikumā minētie vienību veidi.

4. panta 4. punkts definē PS kā direktīvas II pielikumā minēto veidu publiskas vai privātas vienības, kas atbilst 5. panta 2. punkta prasībām. II pielikumā minētas nozares, apakšnozares un vienību veidi, par kurām katrai dalībvalstij jāveic identifikācijas process saskaņā ar 5. panta 2. punktu[25]. Minētās nozares ir enerģētika, transports, banku nozare, finanšu tirgus infrastruktūra, veselības nozare, dzeramā ūdens piegāde un digitālā infrastruktūra.

Vairumam vienību, kas pieder "tradicionālajām nozarēm", ES tiesību aktos ir labi izstrādātas definīcijas, uz kurām ir atsauces II pielikumā. Taču tādu nav digitālās infrastruktūras nozarē, kura minēta II pielikuma 7. punktā un kurā ietilpst interneta plūsmu apmaiņas punkti, domēnu nosaukumu sistēmas un augstākā līmeņa domēnu nosaukumu reģistri. Tādējādi nolūkā precizēt šīs definīcijas turpmāk dots šo definīciju sīks skaidrojums.

1) Interneta plūsmu apmaiņas punkti (IPAP).

Termins "interneta plūsmu apmaiņas punkti" definēts 4. panta 13. punktā un sīkāk skaidrots 18. apsvērumā; to var raksturot kā tīkla iekārtu, kas ļauj savienot vairāk nekā divas neatkarīgas un tehniski autonomas sistēmas un kā primārais mērķis ir nodrošināt interneta plūsmu apmaiņu. Interneta plūsmu apmaiņas punktu var arī raksturot kā fizisku vietu, kurā notiek interneta plūsmu apmaiņa vairāku tīklu starpā ar komutatora palīdzību. IPAP galvenokārt dod iespēju tieši starpsavienot tīklus, nodrošinot datplūsmu apmaiņu starp tiem, nevis izmantojot vienu vai vairākus trešo personu tīklus. IPAP nodrošinātājs parasti neatbild par interneta plūsmu maršrutēšanu. Plūsmu maršrutēšanu nodrošina tīkla nodrošinātāji. Tiešu

[24] Sk. 2. apsvērumu.
[25] Sīkāku informāciju par identifikācijas procesu skatīt 4.1.6. iedaļā

starpsavienojumu priekšrocību ir daudz, bet galvenie to izmantošanas iemesli ir izmaksas, latentums un joslas platums. Par datplūsmām, kas iziet caur apmaiņas punktu, parasti apmaksa netiek prasīta, turpretī par augšupstraumes datu plūsmām uz interneta pakalpojumu sniedzēja (IPS) tīklu tiek. Tiešs starpsavienojums, kas bieži atrodas tajā pašā pilsētā, kur abi tīkli, nodrošina, ka dati nav jāpārsūta lielā attālumā, lai tie nonāktu no viena tīkla citā, tādējādi tiek mazināts latentums.

Ir jāatzīmē, ka IPAP definīcija neaptver fiziskus punktus, kur tiek starpsavienoti tikai divi fiziski tīkli (t.i., tīkla nodrošinātāji, piemēram BASE un PROXIMUS). Tādējādi, transponējot direktīvu, dalībvalstīm būtu jādiferencē tie operatori, kas nodrošina agregētu interneta datu plūsmu apmaiņu vairāku tīkla nodrošinātāju starpā, un tie, kas ir atsevišķa tīkla nodrošinātāji un fiziski starpsavieno savus tīklus saskaņā ar starpsavienojuma līgumu. Pēdējā gadījumā uz tīkla nodrošinātājiem neattiecas 4. panta 13. punkta definīcija. Skaidrojumu šajā jautājumā var atrast 18. apsvērumā, kas nosaka, ka IPAP nesniedz piekļuvi tīklam, nedz arī darbojas kā tranzīta nodrošinātājs vai nesējs. Pēdējā pakalpojumu sniedzēju kategorija ir uzņēmumi, kas nodrošina publiskos komunikāciju tīklus un/vai pakalpojumus un kam piemērojami Direktīvas 2002/21/EK 13.a un 13.b pantā minētie drošības un paziņošanas pienākumi, un kas tādējādi ir izslēgti no TID direktīvas darbības jomas[26].

2) Domēnu nosaukumu sistēma (DNS).

Jēdziens "domēnu nosaukumu sistēma" ir definēts 4. panta 14. punktā kā *"hierarhiska sadalīta nosaukumu sistēma tīklā, kura nosūta vaicājumus attiecībā uz domēnu nosaukumiem"*. Precīzāk, DNS var raksturot kā hierarhiski sadalītu nosaukumu sistēmu internetam pieslēgtiem datoriem, pakalpojumiem un jebkuriem citiem resursiem, kas ļauj kodēt domēnu nosaukumus par IP (interneta protokola) adresēm. Sistēmas galvenais uzdevums ir pārveidot piešķirtos domēna nosaukumus par IP adresēm. Šādā nolūkā DNS izmanto datu bāzi un lieto nosaukumu serverus un atrisinātāju, kas nodrošina domēnu nosaukumu "pārvēršanu" par IP adresēm. Lai arī domēna nosaukumu kodēšana nav vienīgais DNS uzdevums, tas ir šīs sistēmas pamatuzdevums. Juridiskā definīcija 4. panta 14. punktā apraksta sistēmas galveno uzdevumu no lietotāju skatpunkta, neiedziļinoties tehniskākā informācijā, kā, piemēram, domēnu nosaukumvietas darbība, domēnu nosaukumu serveri, atrisinātāji u.c. Visbeidzot, 4. panta 15. punkts skaidro, kas būtu jāuzskata par DNS pakalpojumu sniedzēju.

3) Augstākā līmeņa domēnu nosaukumu reģistri (TLD nosaukumu reģistrs).

Augstākā līmeņa domēnu nosaukums reģistrs ir definēts 4. panta 16. punktā kā vienība, kas pārvalda un veic interneta domēnu nosaukumu reģistrāciju zem konkrēta augstākā līmeņa domēna. Šāda domēna nosaukumu pārvaldība un pārraudzība ietver TLD nosaukumu kodēšanu par IP adresēm.

[26] Sīkāku informāciju par saikni starp TID direktīvu un Direktīvu 2002/21/EK skatīt 5.2. iedaļā.

IANA (Interneta numurpiešķires institūcija) atbild par DNS saknes, interneta protokolu adrešu un citu interneta protokolu resursu koordinēšanu visā pasaulē. Konkrētāk, *IANA* atbild par vispārīgo augstākā līmeņa domēna nosaukumu (gTLD), piemēram, ".com", un valsts koda augstākā līmeņa domēnu nosaukumu (ccTLD), piemēram ".be", piešķiršanu operatoriem (reģistriem) un to tehniskās un administratīvās informācijas uzturēšanu. *IANA* uztur piešķirto TLD vispasaules reģistru un piešķir tos interneta lietotājiem visā pasaulē, kā arī ievieš jaunus TLD.

Svarīgs reģistru uzdevums ir piešķirt otrā līmeņa nosaukumus tā dēvētajiem reģistrētājiem zem to attiecīgā TLD. Šie reģistrētāji var arī paši piešķirt trešā līmeņa domēna nosaukumus, ja vēlas to darīt. ccTLD ir paredzēti, lai apzīmētu valsti vai teritoriju saskaņā ar ISO 3166-1 standartu. "Vispārīgajiem" TLD parasti nav ģeogrāfiskas vai valsts piesaistes.

Ir jāatzīmē, ka TLD nosaukumu reģistra uzturēšana var ietvert DNS nodrošināšanu. Piemēram, saskaņā ar *IANA* deleģēšanas noteikumiem izraudzītajai vienībai, kas darbojas ar ccTLD cita starpā ir jāpārrauga domēna nosaukumi un jāuztur attiecīgās valsts DNS[27]. Šie apstākļi ir jāņem vērā dalībvalstij, veicot pamatpakalpojumu sniedzēju identificēšanu saskaņā ar 5. panta 2. punktu.

4.1.2. Pamatpakalpojumu sniedzēju identificēšana.

Saskaņā ar direktīvas 5. panta prasībām katrai dalībvalstij ir pienākums attiecībā uz katru II pielikumā minēto nozari un apakšnozari identificēt pamatpakalpojumu sniedzējus, kam attiecīgās dalībvalsts teritorijā ir likumīga uzņēmējdarbības vieta. Šī novērtējuma rezultātā visas vienības, kas atbilst 5. panta 2. punktā noteiktajiem kritērijiem, ir jāidentificē kā PS un tām jāpiemēro 14. panta drošības prasību un incidentu paziņošanas pienākumi.

Dalībvalstīm līdz 2018. gada 9. novembrim ir jāidentificē pakalpojumu sniedzēji katrā nozarē un apakšnozarē. Lai atbalstītu dalībvalstis šajā procesā, sadarbības grupa šobrīd izstrādā vadlīniju dokumentu ar attiecīgu informāciju par nepieciešamajām darbībām un labo praksi saistībā ar PS identificēšanu.

Turklāt saskaņā ar 24. panta 2. punktu sadarbības grupai ir jāapspriež to valsts pasākumu process, būtība un veids, kas ļauj identificēt pamatpakalpojumu sniedzējus konkrētā nozarē. Dalībvalsts pirms 2018. gada 9. novembra var lūgt iespēju apspriest sadarbības grupā plānotos valsts pasākumus, kas ļauj identificēt pamatpakalpojumu sniedzējus.

4.1.3. Papildu nozaru iekļaušana.

Ņemot vērā 3. pantā paredzēto minimālās saskaņošanas prasību, dalībvalstis var pieņemt vai saglabāt tiesību aktus, kas nodrošina augstāku tīklu un informācijas sistēmu drošības līmeni. Šajā sakarā dalībvalstis visumā ir tiesīgas attiecināt 14. pantā noteiktos drošības un incidentu paziņošanas pienākumus uz vienībām, kas pieskaitāmas citām nozarēm un apakšnozarēm, kas nav minētas TID direktīvas II pielikumā. Vairākās dalībvalstīs ir nolemts vai pašlaik tiek apsvērts ietvert kādu no šādām nozarēm:

i) Publiskās pārvaldes iestādes

[27] Informācija pieejama tīmekļa vietnē: https://www.icann.org/resources/pages/delegation-2012-02-25-en

Publiskās pārvaldes iestādes var piedāvāt direktīvas II pielikumā noteiktos pamatpakalpojumus, kas atbilst 5. panta 2. punkta prasībām. Šādos gadījumos uz publiskās pārvaldes iestādēm, kas piedāvā šādus pakalpojumus, attiecas attiecīgie drošības prasību un incidentu paziņošanas pienākumi. *A contrario*, kad publiskās pārvaldes iestādes piedāvā pakalpojumus, kas neietilpst iepriekš minētajā jomā, šādu pakalpojumu sniegšanai nav piemērojami attiecīgie pienākumi.

Publiskās pārvaldes iestādes atbild par valdības struktūru, reģionālo un vietējo pašvaldības institūciju, aģentūru un saistīto uzņēmumu sniegto publisko pakalpojumu pienācīgu nodrošināšanu. Tālab bieži nepieciešams radīt un pārvaldīt personas un korporatīvos datus par personām un organizācijām, kuri var tikt izplatīti un darīti pieejami vairākām publiskām organizācijām. Plašākā izpratnē augsta drošības līmeņa tīklu un informācijas sistēmu lietošana publiskajā pārvaldē ir nozīmīga sabiedrības un ekonomikas interesēm kopumā. Tādējādi Komisija uzskata, ka dalībvalstīm, transponējot direktīvu, būtu ieteicams apsvērt publiskās pārvaldes iestāžu iekļaušanu valstu tiesību aktu darbības jomā, neaprobežojoties tikai ar pamatpakalpojumu sniegšanu, atbilstīgi II pielikumam un 5. panta 2. punktam.

ii) Pasta pakalpojumu nozare

Pasta pakalpojumu nozare aptver pasta pakalpojumu nodrošināšanu, piemēram, pasta sūtījumu savākšanu, šķirošanu, transportēšanu un nogādāšanu adresātam.

iii) Pārtikas nozare

Pārtikas nozare skar lauksaimniecisko un citu pārtikas produktu ražošanu, un tā varētu ietvert tādus pamatpakalpojumus kā nodrošinātība ar pārtiku un pārtikas kvalitātes un drošuma kontrole.

iv) Ķīmiskā un kodolrūpniecība

Ķīmiskā un kodolrūpniecība it īpaši risina jautājumus par ķīmisko un naftas ķīmisko produktu vai kodolmateriālu glabāšanu, ražošanu un apstrādi.

v) Vides nozare

Vides nozare aptver tādu preču un pakalpojumu sniegšanu, kas nepieciešami vides aizsardzībai un resursu pārvaldībai. Tādējādi darbības tiek vērstas uz to, lai novērstu, samazinātu un likvidētu piesārņojumu un saglabātu pieejamo dabas resursu krājumus. Šajā nozarē pamatpakalpojumi varētu būt piesārņojuma (piemēram, gaisa un ūdens) un meteoroloģisko parādību novērošana un kontrole.

vi) Civilā aizsardzība

Civilās aizsardzības nozares mērķis ir nepieļaut dabas un cilvēku izraisītas katastrofas, sagatavoties un reaģēt uz tām. Šādā nolūkā sniegtie pakalpojumi var būt neatliekamās palīdzības dienestu numuru aktivizēšanu un darbības, kas saistītas ar informēšanu par ārkārtas situācijām, ārkārtas situāciju ierobežošanu un reaģēšanu uz tām.

4.1.4. Jurisdikcija.

Saskaņā ar 5. panta 1. punktu katrai dalībvalstij ir jāidentificē PS, kuram tās teritorijā ir uzņēmējdarbības vieta. Noteikums neprecizē uzņēmējdarbības veidu, bet 21. apsvērums

skaidro, ka šāda uzņēmējdarbība nozīmē efektīvu un faktisku darbību, ko veic pastāvīga vienība, turpretim pastāvīgo vienību juridiskais statuss nav noteicošais faktors. Tas nozīmē, ka pamatpakalpojumu sniedzējs var būt dalībvalsts jurisdikcijā ne tikai gadījumos, ja dalībvalsts teritorijā atrodas pakalpojuma sniedzēja galvenais birojs, bet arī gadījumos, kad pakalpojuma sniedzējam dalībvalsts teritorijā ir, piemēram, filiāle vai citas juridiskas formas vienība.

Tas nozīmē, ka viena vienība vienlaikus var būt vairāku dalībvalstu jurisdikcijā.

4.1.5. Komisijai iesniedzamā informācija.

Pārskatīšanas nolūkā, kas Komisijai jāveic saskaņā ar TID direktīvas 23. panta 1. punktu, dalībvalstīm ir pienākums iesniegt Komisijai līdz 2018. gada 9. novembrim un pēc tam ik pēc diviem gadiem šādu informāciju:

- valstu pasākumus, kas ļauj identificēt PS;
- pamatpakalpojumu sarakstu;
- identificēto pamatpakalpojumu sniedzēju skaitu katrai II pielikumā minētajai nozarei un norādi par to nozīmīgumu attiecībā uz minēto nozari; kā arī
- robežvērtības, ja tādas pastāv, lai noteiktu attiecīgo piedāvājuma līmeni, atsaucoties uz to lietotāju skaitu, kuri izmanto minēto pakalpojumu, kā minēts 6. panta 1. punkta a) apakšpunktā, vai uz minētā konkrētā pamatpakalpojumu sniedzēja nozīmīgumu, kā minēts 6. panta 1. punkta f) apakšpunktā.

23. panta 1. punktā paredzētā pārskatīšana, kas veicama pirms visaptverošas direktīvas pārskatīšanas, atspoguļo to, cik lielu nozīmi likumdevēji piešķir pareizai direktīvas transponēšanai attiecībā uz pamatpakalpojumu sniedzēju identificēšanu, lai izvairītos no tirgus sadrumstalošanās.

Lai veiktu šo procesu vislabākajā iespējamā veidā, Komisija mudina dalībvalstis sadarbības grupā pārrunāt šo tēmu un dalīties attiecīgajā pieredzē. Komisija arī mudina dalībvalstis iesniegt Komisijai, ja nepieciešams, konfidenciāli, identificēto (galu galā izraudzīto) pamatpakalpojumu sniedzēju sarakstus papildus visai informācijai, kura dalībvalstīm jāsniedz Komisijai saskaņā ar direktīvu. Šādu sarakstu pieejamība palīdzētu Komisijai sagatavot kvalitatīvāku vērtējumu par identifikācijas procesa konsekvenci, kā arī ļautu salīdzināt dažādās dalībvalstu pieejas, tādējādi nodrošinot labāku rezultātu direktīvas mērķu sasniegšanā.

4.1.6. Kā veikt identifikācijas procesu?

Kā redzams 4. att., ir seši galvenie jautājumi, kas valsts iestādei jāuzdod konkrētas vienības identifikācijas procesā. Turpmākajā rindkopā katrs jautājums atbilst solim, kas jāveic saskaņā ar 5. pantu kopā ar 6. pantu un arī ņemot vērā 1. panta 7. punkta piemērojamību.

1. solis — **vai vienība pieder pie direktīvas II pielikumā norādītas nozares/apakšnozares un atbilst vienības veidam?**

Valsts iestādei būtu jānovērtē, vai tās teritorijā izveidotā vienība pieder pie nozarēm un apakšnozarēm, kas minētas direktīvas II pielikumā. II pielikums aptver vairākas ekonomikas nozares, kas tiek uzskatītas par būtiski svarīgām, lai nodrošinātu iekšējā tirgus pareizu darbību. Konkrētāk, II pielikumā minētas šādas nozares un apakšnozares:

- enerģētika — elektroenerģija, nafta un gāze;
- transports — gaisa transports, dzelzceļa transports, ūdens transports un autotransports;
- banku nozare — kredītiestādes;
- finanšu tirgus infrastruktūras — tirdzniecības vietas, centrālie darījumu partneri;
- veselības aprūpe — veselības aprūpes iestādes (tostarp slimnīcas un privātas klīnikas);
- ūdens — dzeramā ūdens piegāde un izplatīšana;
- digitālā infrastruktūra — interneta plūsmu apmaiņas punkti, domēnu nosaukumu sistēmu pakalpojumu sniedzēji, augstākā līmeņa domēnu nosaukumu reģistri[28].

2. solis — **vai ir piemērojams *lex specialis*?**

Nākamajā solī valsts iestādei jānovērtē, vai ir piemērojams 1. panta 7. punktā ietvertais noteikums par *lex specialis*. Konkrētāk: ja pastāv ES tiesību akts, ar ko uzliek drošības prasību un/vai incidentu paziņošanas pienākumu pamatpakalpojumu sniedzējiem vai digitālo pakalpojumu sniedzējiem un kas ir vismaz līdzvērtīgs TID direktīvā noteiktajām prasībām, piemērojami speciālajā tiesību aktā noteiktie pienākumi. Turklāt 9. apsvērums skaidro, ka, ja ir izpildītas 1. panta 7. punkta prasības, dalībvalstīm jāpiemēro nozarspecifisko ES tiesību akta noteikumi, tostarp tie, kas attiecas uz jurisdikciju. A *contrario* attiecīgie TID direktīvas noteikumi nav piemērojami. Šādā gadījumā kompetentajai iestādei nav jāturpina identifikācijas process saskaņā ar 5. panta 2. punktu[29].

3. solis — **vai pakalpojumu sniedzējs sniedz pamatpakalpojumu direktīvas izpratnē?**

Saskaņā ar 5. panta 2. punkta a) apakšpunktu identificējamajai vienībai ir jāsniedz pakalpojums, kas ir būtisks īpaši svarīgu sabiedrisku un/vai ekonomisku darbību nodrošināšanai. Veicot šo novērtējumu, dalībvalstīm vajadzētu ņemt vērā, ka viena vienība var sniegt gan pamatpakalpojumus, gan pakalpojumus, kas nav pamatpakalpojumi. Tas nozīmē, ka TID direktīvas drošības un incidentu paziņošanas prasības būs attiecināmas uz noteiktu pakalpojumu sniedzēju tikai tiktāl, cik tas sniedz pamatpakalpojumus.

Saskaņā ar 5. panta 3. punktu dalībvalstij ir jāizveido visu pamatpakalpojumu saraksts, ko pamatpakalpojumu sniedzēji sniedz tās teritorijā. Šis saraksts jāiesniedz Komisijai līdz 2018. gada 9. novembrim un pēc tam ik pēc diviem gadiem[30].

4. solis — **vai pakalpojuma sniegšana ir atkarīga no tīkla un informācijas sistēmām?**

[28] Šīs vienības plašāk aprakstītas 4.1.1. iedaļā.

[29] Sīkāka informācija par *lex specialis* piemērošanu sniegta 5.1. iedaļā

[30] Skatīt 5. panta 7. punkta b) apakšpunktu

Turklāt būtu jānoskaidro, vai šis pakalpojums atbilst 5. panta 2. punkta b) apakšpunkta kritērijam un it īpaši, vai pamatpakalpojuma sniegšana ir atkarīga no tīklu un informācijas sistēmām, kā noteikts 4. panta 1. punktā.

5. solis — **vai drošības incidentam būtu būtiska traucējoša ietekme?**

5. panta 2. punkta c) apakšpunkts nosaka, ka valsts iestāde novērtē, vai incidentam būtu būtiska traucējoša ietekme uz pakalpojuma sniegšanu. Šajā kontekstā 6. panta 1. punkts nosaka vairākus starpnozaru faktorus, kas jāņem vērā novērtējumā. Turklāt 6. panta 2. punkts nosaka, ka attiecīgā gadījumā novērtējumā jāņem vērā arī nozarspecifiski faktori.

Starpnozaru faktori, kas minēti 6. panta 1. punktā:

- to lietotāju skaits, kuri izmanto attiecīgās vienības sniegtos pakalpojumus;
- citu II pielikumā minēto nozaru atkarība no minētās vienības sniegtā pakalpojuma;
- ietekme, kas incidentiem pakāpes un ilguma ziņā varētu būt uz ekonomiskām un sabiedriskām darbībām vai sabiedrisko drošību;
- minētās vienības tirgus daļa;
- ģeogrāfiskā izplatība attiecībā uz vidi, ko varētu skart incidents;
- vienības nozīmīgums pietiekama pakalpojumu līmeņa uzturēšanai, ņemot vērā alternatīvu līdzekļu pieejamību minētā pakalpojuma sniegšanai.

Attiecībā uz **nozarspecifiskiem faktoriem** 28. apsvērums sniedz dažus piemērus (skatīt 4. tabulu), kas varētu sniegt noderīgas vadlīnijas valstu iestādēm.

4. tabula. Nozarspecifiski faktori, kas jāizvērtē, nosakot, vai incidentam būtu būtiska traucējoša ietekme.

Nozare	Konkrētai nozarei specifisku faktoru piemēri
Enerģijas piegādātāji	apjoms vai daļa no valstī saražotās enerģijas
Naftas piegādātāji	piegādātais naftas apjoms dienā
Gaisa transports (tostarp lidostas un gaisa pārvadātāji) **Dzelzceļa transports** **Jūras ostas**	daļa valsts satiksmes apjomā; pasažieru vai kravas pārvadājumu operāciju skaits gadā.
Banku vai finanšu tirgu infrastruktūras	to sistēmiskais nozīmīgums, balstoties uz aktīvu kopsummu; aktīvu kopsummas attiecība pret IKP.
Veselības aprūpes nozare	pacientu skaits, ko pakalpojumu sniedzējs aprūpē gadā.
Ūdens ieguve, attīrīšana un apgāde	apjoms un apgādāto lietotāju skaits un veidi (tostarp, piemēram, slimnīcas, organizācijas, kas sniedz publiskos pakalpojumus, vai privātpersonas); vai tajā pašā ģeogrāfiskajā apvidū pastāv alternatīvi ūdens avoti.

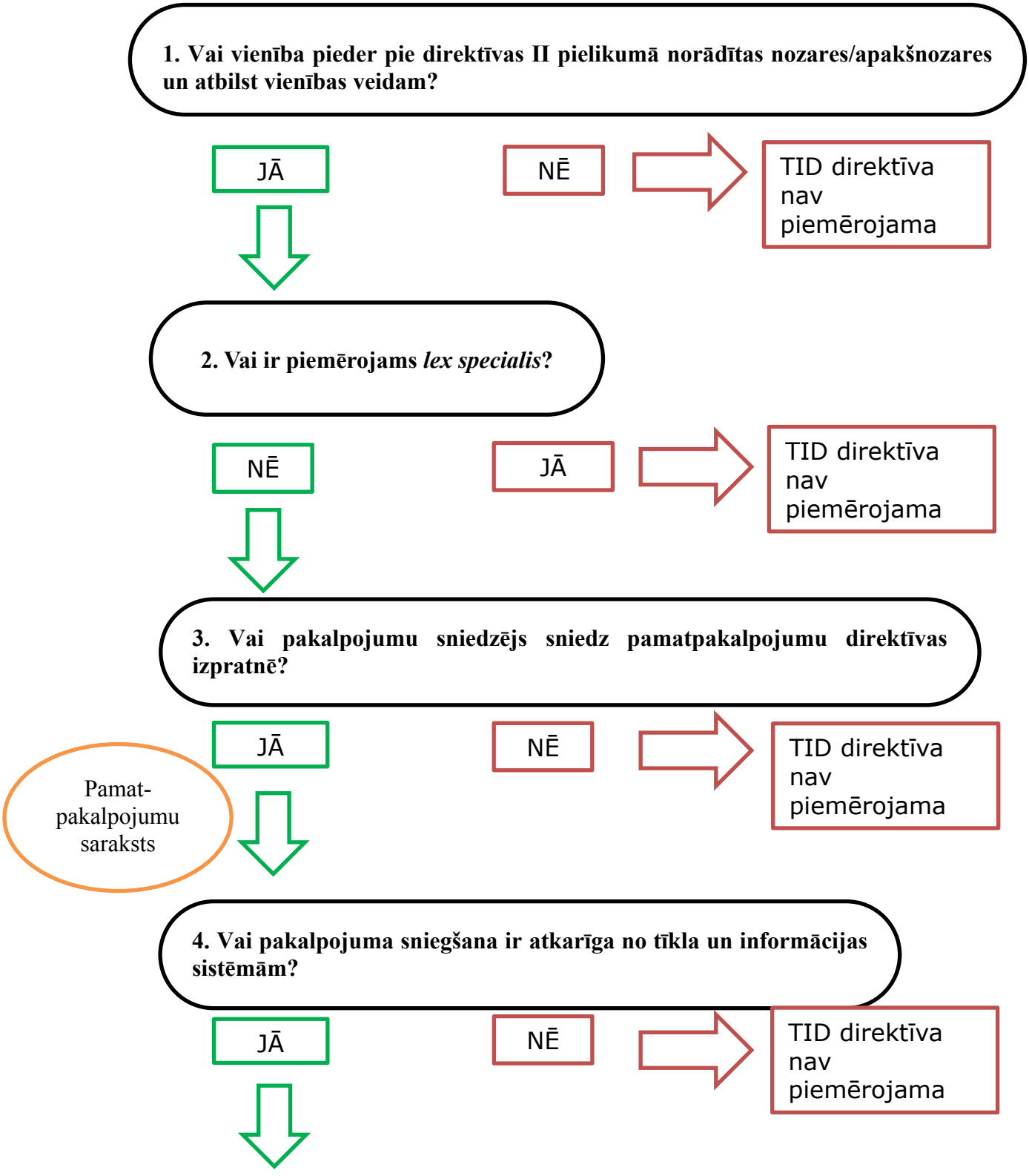
Ir jānorāda, ka, veicot novērtējumu saskaņā ar 5. panta 2. punktu, dalībvalstīm nevajadzētu pievienot kritērijus papildus šajā punktā uzskaitītajiem, jo tas varētu sašaurināt identificēto PS skaitu un apdraudēt minimālo saskaņošanu attiecībā uz PS, ko paredz direktīvas 3. pants.

6. solis — **vai attiecīgais pakalpojumu sniedzējs sniedz pamatpakalpojumus citās dalībvalstīs?**

6. solis attiecināms uz gadījumiem, kad pakalpojumu sniedzējs sniedz savus pamatpakalpojumus divās vai vairākās dalībvalstīs. 5. panta 4. punkts nosaka, ka attiecīgajām dalībvalstīm ir jāapspriežas pirms identifikācijas procesa pabeigšanas[31].

[31] Sīkāku informāciju par apspriešanās procesu skatīt 4.1.7. iedaļā.

4. attēls. Identifikācijas process 6 soļos.



5. Vai drošības incidentam būtu būtiska traucējoša ietekme?

Starpnozaru faktori (6. panta 1. punkts)

- **Lietotāju skaits**, kuri izmanto pakalpojumus
- Citu pamatpakalpojuma nozaru **atkarība** no pakalpojuma
- Ietekme, kas incidentiem varētu būt uz **ekonomiskām un sabiedriskām darbībām** vai **sabiedrisko drošību**
- Iespējamā **ģeogrāfiskā izplatība**
- Vienības nozīmīgums **pietiekama pakalpojumu līmeņa** uzturēšanai

Nozarspecifiski faktori (piemēri minēti 28. apsvērumā)

- **Enerģētika:** apjoms vai daļa no valstī saražotās enerģijas
- **Transports**: daļa valsts satiksmes apjoma un kravas pārvadājumu operācijām gadā
- **Veselības aprūpe:** pacientu skaits, ko pakalpojumu sniedzējs aprūpē gadā

JĀ

NĒ → TID direktīva nav piemērojama

6. Vai attiecīgais pakalpojumu sniedzējs sniedz pamatpakalpojumus citās dalībvalstīs?

JĀ

NĒ → TID direktīva nav piemērojama

Obligāta apspriešanās ar attiecīgo dalībvalsti vai

Valsts pasākumu pieņemšana (piemēram, pamatpakalpojumu sniedzēju saraksts, rīcībpolitika un juridiski pasākumi).

4.1.7. Pārrobežu konsultāciju process.

Ja pakalpojumu sniedzējs sniedz pamatpakalpojumus divās vai vairākās dalībvalstīs, 5. panta 4. punkts nosaka, ka dalībvalstis savstarpēji apspriežas, pirms tiek pieņemts lēmums par identifikāciju. Šīs apspriešanās mērķis ir palīdzēt izvērtēt pakalpojumu sniedzēja būtiskumu, ņemot vērā pārrobežu ietekmi.

Vēlamais apspriešanās mērķis ir dot iespēju iesaistītajām valstu iestādēm paust savus argumentus un uzskatus un ideālā gadījumā nonākt pie kopsaucēja par attiecīgā pakalpojumu sniedzēja identifikāciju. Tomēr TID direktīva neizslēdz iespēju, ka dalībvalstis nonāk pie atšķirīgiem secinājumiem par to, vai konkrētā vienība tiek vai netiek identificēta kā PS. 24. apsvērums norāda uz iespēju dalībvalstīm lūgt sadarbības grupas palīdzību šajos jautājumos.

Komisijas ieskatā dalībvalstīm jācenšas panākt vienošanos šajos jautājumos, lai izvairītos no situācijas, ka vienam uzņēmumam ir atšķirīgs juridiskais statuss dažādās dalībvalstīs. Atšķirībām būtu jābūt patiešām izņēmuma gadījumiem, piemēram, kad vienība, kas noteikta par PS vienā dalībvalstī, veic mazsvarīgu un nenozīmīgu darbību citā.

4.2. Drošības prasības.

Saskaņā ar 14. panta 1. punktu dalībvalstīm ir pienākums nodrošināt, ka pamatpakalpojumu sniedzēji, ņemot vērā jaunākos tehniskos sasniegumus, veic atbilstīgus un samērīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmu drošībai, ko organizācijas izmanto savu pakalpojumu sniegšanai. Saskaņā ar 14. panta 2. punktu piemērotajiem pasākumiem ir jānovērš un jāmazina incidentu ietekme.

Tālab specializēta vienība sadarbības grupā šobrīd izstrādā nesaistošas vadlīnijas par drošības pasākumiem PS[32]. Vadlīniju dokumentu grupa pabeigs 2017. gada 4. ceturksnī. Komisija aicina dalībvalstis rūpīgi ievērot vadlīniju dokumentu, kuru izstrādās sadarbības grupa, lai valstu noteikumi par drošības prasībām būtu tik saskaņoti, cik vien iespējams. Šādu prasību saskaņošana PS ievērojami atvieglotu to ievērošanu, jo PS bieži sniedz pamatpakalpojumus vairākās dalībvalstīs, bet valstu kompetentajām iestādēm un *CSIRT* — uzraudzības uzdevumu veikšanu.

4.3 Paziņošanas prasības.

Saskaņā ar 14. panta 3. punktu dalībvalstīm ir jānodrošina, ka pamatpakalpojumu sniedzēji paziņo "*par incidentiem, kuriem ir būtiska ietekme uz pamatpakalpojumu nepārtrauktību*". Tādējādi PS nav jāpaziņo par maznozīmīgiem incidentiem, bet tikai par nopietniem incidentiem, kas ietekmē pamatpakalpojuma nepārtrauktību. Incidents 4. panta 7. punktā definēts kā "*jebkāds notikums, kas faktiski nelabvēlīgi ietekmē tīklu un informācijas sistēmu drošību*". Jēdziens "tīklu un informācijas sistēmu drošība" sīkāk precizēts 4. panta 2. punktā

[32] Šī specializētā vienība iepazinās ar starptautisko standartu sarakstiem, labo praksi un riska novērtēšanas/pārvaldības metodikām attiecībā uz visām TID direktīvā ietvertajām nozarēm, un šo informāciju izmantoja darbā pie ierosinātajām drošības jomām un pasākumiem.

kā "*tīklu 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 pakalpojumu".* Tādējādi ikviens notikums, kam ir negatīva ietekme ne tikai uz datu vai saistīto pakalpojumu pieejamību, bet arī autentiskumu, integritāti vai konfidencialitāti, varētu potenciāli radīt paziņošanas pienākumu. Faktiski 14. panta 3. punktā norādītā pakalpojuma nepārtrauktība var tikt apdraudēta ne tikai gadījumos, kas skar fizisku pieejamību, bet arī jebkura cita incidenta gadījumā, kas ietekmē pienācīgu pakalpojuma sniegšanu[33].

Specializēta vienība sadarbības grupā šobrīd izstrādā nesaistošas paziņošanas vadlīnijas par apstākļiem, kuros pamatpakalpojumu sniedzējiem ir pienākums paziņot par incidentiem saskaņā ar 14. panta 7. punktu un par valstu paziņojumu formātu un kārtību. Vadlīnijas plānots pabeigt 2017. gada 4. ceturksnī.

Dažādas valstu prasības var novest pie tiesiskas nenoteiktības, sarežģītākām un apgrūtinošām procedūrām un ievērojamām administratīvām izmaksām tiem pakalpojumu sniedzējiem, kas darbojas pārrobežu režīmā. Tāpēc Komisija atbalsta sadarbības grupas darbu. Tāpat kā drošības prasību jautājumā, Komisija aicina dalībvalstis vērīgi sekot vadlīniju dokumentam, kuru izstrādās sadarbības grupa, lai valstu noteikumi par incidentu paziņošanu būtu tik saskaņoti, cik vien iespējams.

4.4. TID direktīva, III pielikums: digitālo pakalpojumu sniedzēji.

Digitālo pakalpojumu sniedzēji (DPS) ir otra vienību kategorija, kas ietverta TID direktīvas darbības jomā. Šīs vienības uzskatāmas par nozīmīgiem ekonomikas dalībniekiem tāpēc, ka to pakalpojumus izmanto daudzi uzņēmumi paši savu pakalpojumu sniegšanā, un digitālā pakalpojuma traucējums varētu ietekmēt svarīgas saimnieciskas un sabiedriskas norises.

4.4.1. DPS kategorijas.

4. panta 5. punktā, kur definēts digitālais pakalpojums, ir atsauce uz juridisku definīciju Direktīvas (ES) 2015/1535 1. panta 1. punkta b) apakšpunktā, kas sašaurina darbības jomu līdz III pielikumā minētajiem pakalpojumu veidiem. Direktīvas (ES) 2015/1535 1. panta 1. punkta b) apakšpunktā šie pakalpojumi definēti kā "*jebkāds pakalpojums, ko parasti sniedz par atlīdzību no attāluma, ar elektroniskiem līdzekļiem un pēc pakalpojumu saņēmēja individuāla pieprasījuma*", un direktīvas III pielikumā uzskaitīti trīs konkrēti pakalpojumu veidi: tiešsaistes tirdzniecības vieta, tiešsaistes meklētājprogramma un mākoņdatošanas pakalpojums. Atšķirībā no pamatpakalpojumu sniedzējiem direktīva nepieprasa dalībvalstīm identificēt digitālo pakalpojumu sniedzējus, kuriem tad tiktu noteikti attiecīgi pienākumi. Tādējādi attiecīgie direktīvā paredzētie pienākumi, proti, 16. pantā noteiktās drošības prasības un incidentu paziņošanas pienākumi, attieksies uz visiem DPS tās darbības jomā.

[33] Tas pats attiecas uz DPS.

Turpmākajās iedaļās sniegti papildu skaidrojumi par trim digitālo pakalpojumu veidiem, kas ietverti direktīvas darbības jomā.

1. Tiešsaistes tirdzniecības vieta.
Tiešsaistes tirdzniecības vieta ļauj daudziem un dažādiem uzņēmumiem veikt tiešus tirdznieciskus darījumus ar patērētājiem un iesaistīties attiecībās ar citiem uzņēmumiem. Tā nodrošina uzņēmumiem pamata infrastruktūru tirdzniecībai tiešsaistē un citās valstīs. Ekonomikā tās ieņem nozīmīgu lomu, proti, nodrošina MVU piekļuvi plašākam ES digitālajam vienotajam tirgum. Tiešsaistes tirdzniecības vietas nodrošinātājs var sniegt arī attālinātus datorpakalpojumus, kas veicina to klientu saimniecisko darbību, tostarp apstrādāt darījumus un apkopot informāciju par pircējiem, piegādātājiem un precēm, tāpat arī atvieglot atbilstošu preču meklējumus, nodrošināt ar produktiem, sniegt profesionālas zināšanas par darījumiem un palīdzēt pircējiem atrast pārdevējus un otrādi.

Termins "tiešsaistes tirdzniecības vieta" definēts 4. panta 17. punktā un sīkāk skaidrots 15. apsvērumā. Tā raksturota kā pakalpojums, kas ļauj patērētājiem un tirgotājiem slēgt tiešsaistes tirdzniecības vai pakalpojumu līgumus ar tirgotājiem, un tā ir vieta, kur tiek galīgi noslēgti minētie līgumi. Piemēram, tādu pakalpojumu sniedzēju kā *E-bay* var uzskatīt par tiešsaistes tirdzniecības vietu, jo tas ļauj citiem izveidot veikalus savā platformā, lai tiešsaistē piedāvātu savas preces un pakalpojumus patērētājiem vai uzņēmumiem. Tāpat tiešsaistes lietotņu veikali, kur izplata lietotnes un programmas, tiek uzskatīti par vienu no tiešsaistes tirdzniecības vietas veidiem, jo tajos lietotņu izstrādātāji var pārdot vai izplatīt savus pakalpojumus patērētājiem vai citiem uzņēmumiem. Turpretim starpniecība kādas trešās personas pakalpojumiem, piemēram, *Skyscanner*, un cenu salīdzināšanas pakalpojumi, kas novirza lietotāju uz izvēlētā tirgotāja tīmekļa vietni, kur tiek slēgts faktiskais līgums par pakalpojumu vai preci, neatbilst 4. panta 17. punkta definīcijai.

2. Tiešsaistes meklētājprogrammu pakalpojumu sniedzēji.
Termins "tiešsaistes meklētājprogramma" definēts 4. panta 18. punktā un sīkāk skaidrots 16. apsvērumā. Tā tiek raksturota kā digitāls pakalpojums, kas ļauj lietotājam veikt meklējumus principā visās tīmekļa vietnēs vai vietnēs konkrētā valodā, pamatojoties uz vaicājumu par jebkādu tematu. Te neietilpst ne meklēšana tikai vienā konkrētā tīmekļa vietnē, ne cenu salīdzināšanas tīmekļa vietnes. Piemēram, tāda veida meklētājprogrammu, kas darbojas vietnē EUR LEX[34], nevar uzskatīt par meklētāju direktīvas izpratnē, jo meklēšanas funkcija attiecas vienīgi uz konkrētas tīmekļa vietnes saturu.

3. Mākoņdatošanas pakalpojumu sniedzēji.
4. panta 19. punkts definē mākoņdatošanas pakalpojumu kā "digitālu pakalpojumu, kas dod iespēju piekļūt mērogojamam un elastīgam kopīgojamu datošanas resursu pūlam", un 17. apsvērums sīkāk skaidro terminus "datošanas resursi", "mērogojams" un "elastīgs pūls".

Īsumā — mākoņdatošanu var raksturot kā īpašu datošanas pakalpojuma veidu, kas izmanto kopīgotus resursus, lai pēc pieprasījuma apstrādātu datus, un kopīgoti resursi ir jebkādas

[34] Skatīt: http://eur-lex.europa.eu/homepage.html

iekārtas vai programmatūras komponentes (piemēram, tīkli, serveri vai cita infrastruktūra, glabāšana, lietotnes un pakalpojumi), kas pēc pieprasījuma tiek piešķirti lietotājiem datu apstrādei. Termins "kopīgojami" definē datošanas resursus kā resursus, kurus izmanto daudzi lietotāji, kuriem ir kopīga fiziskā infrastruktūra datu apstrādei. Datošanas resursu var definēt kā kopīgojamu, ja nodrošinātāja izmantoto resursu pūlu var palielināt un samazināt jebkurā laikā atkarībā no lietotāju prasībām. Tātad, ja kopējā datošanas jauda vai glabāšanas ietilpība ir jāaktualizē, tad datu centrus vai atsevišķas datu centra komponentes varētu pievienot vai noņemt. Terminu "elastīgs pūls" var skaidrot kā noslodzes izmaiņas, kas notiek, nodrošinot un pārtraucot nodrošināt resursus automātiskā veidā tā, lai katrā laika brīdī pieejamie resursi pēc iespējas precīzāk atbilstu faktiskajam pieprasījumam"[35].

Šobrīd ir trīs galvenie mākoņdatošanas pakalpojumu modeļi, kādus pakalpojuma sniedzējs var piedāvāt:

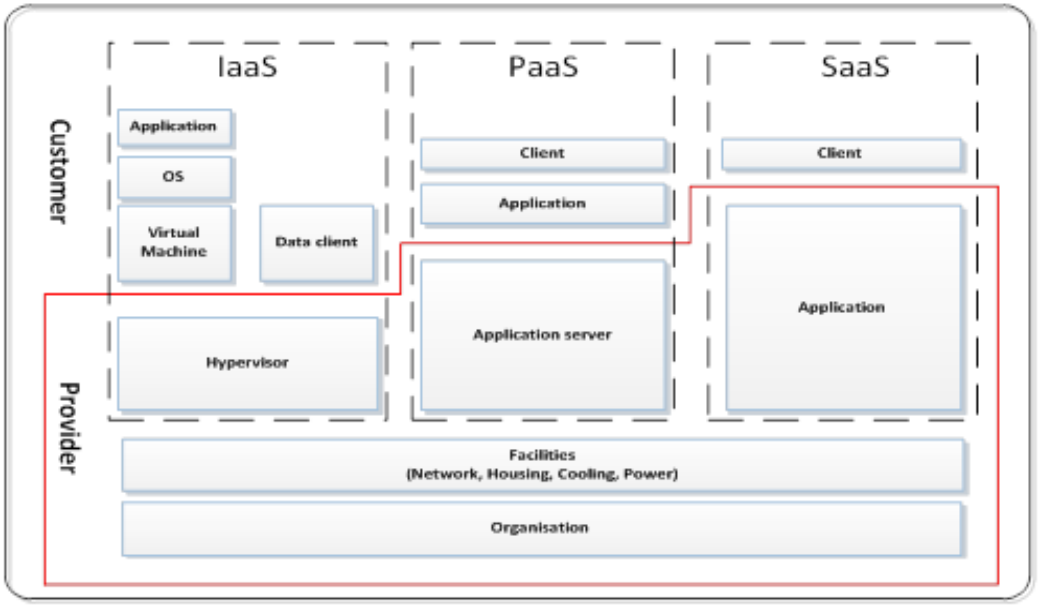
- Infrastruktūras pakalpojums (*IaaS*): mākoņdatošanas pakalpojuma kategorija, kuras ietvaros klientam piedāvātais mākoņa iespēju tips ir infrastruktūra. Tas ietver datošanas resursu — iekārtu, tīklu un krātuvju pakalpojumu— virtuālu nodrošināšanu. IaaS darbina serverus, krātuves, tīklus un operētājsistēmas. Tas nodrošina uzņēmuma infrastruktūru, kurā uzņēmums var glabāt savus datus un darbināt lietotnes, kas nepieciešamas tā ikdienas darbībai.

- Platformas pakalpojums (*PaaS*): mākoņdatošanas pakalpojuma kategorija, kuras ietvaros klientam piedāvātais mākoņa iespēju tips ir platforma. Tā ietver tiešsaistes datošanas platformas, kas ļauj uzņēmumiem darbināt esošas lietotnes vai izstrādāt un testēt jaunas.

- Programmatūras pakalpojums (*SaaS*): mākoņdatošanas pakalpojuma kategorija, kuras ietvaros klientam piedāvātais mākoņa iespēju tips ir lietotne vai programmatūra, kas izvietota internetā. Šis mākoņdatošanas pakalpojumu veids ļauj gala lietotājiem nepirkt, neinstalēt un nepārvaldīt programmatūru, un tā priekšrocība ir programmatūras pieejamība no jebkuras vietas, kur ir interneta pieslēgums.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, "Elasticity in Cloud Computing: What It Is, and What It Is Not", skatīt: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Skatīt arī COM(2012) 529, 2.-5. lappuse.

5. attēls. Pakalpojumu modeļi un aktīvi mākoņdatošanā



ENISA ir sagatavojusi visaptverošas vadlīnijas par specifiskiem tematiem, kas skar mākoņdatošanu[36], un norāžu dokumentu par mākoņdatošanas pamatiem[37].

4.4.2. Drošības prasības.

Saskaņā ar 16. panta 1. punktu dalībvalstīm ir pienākums nodrošināt, ka DPS veic atbilstīgus un samērīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmu drošībai, ko uzņēmumi izmanto savu pakalpojumu sniegšanai. Šie drošības pasākumi būtu jāveic, ņemot vērā jaunākos tehniskos sasniegumus un šādus piecus elementus: i) sistēmu un iekārtu drošība; ii) incidentu risināšana; iii) darījumdarbības nepārtrauktības pārvaldība; iv) uzraudzība, revīzijas un pārbaudes; v) atbilstība starptautiskajiem standartiem.

Šajā sakarā saskaņā ar 16. panta 8. punktu Komisija ir pilnvarota pieņemt īstenošanas aktus, lai vēl sīkāk precizētu šos elementus un nodrošinātu augstu saskaņotības līmeni šiem pakalpojumu sniedzējiem. Sagaidāms, ka Komisija īstenošanas aktu pieņems 2017. gada rudenī. Turklāt dalībvalstīm ir pienākums nodrošināt, lai digitālo pakalpojumu sniedzēji veiktu nepieciešamos pasākumus, lai novērstu un mazinātu incidentu ietekmi nolūkā nodrošināt to pakalpojumu nepārtrauktību.

4.4.3. Paziņošanas prasības.

DPS jābūt pienākumam par nopietniem incidentiem paziņot kompetentajām iestādēm vai *CSIRT*. Saskaņā ar TID direktīvas 16. panta 3. punktu paziņošanas pienākums digitālo pakalpojumu sniedzējiem iestājas gadījumos, kad drošības incidentam ir būtiska ietekme uz pakalpojuma

[36] Skatīt: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] *ENISA, Mākoņdrošības ceļvedis MVU* (2015). Skatīt: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

sniegšanu. 16. panta 4. punktā īpaši norādīti pieci ietekmes novērtēšanas parametri, kas digitālo pakalpojumu sniedzējiem jāņem vērā. Šajā sakarā saskaņā ar 16. panta 8. punktu Komisija ir pilnvarota pieņemt īstenošanas aktus, kas nodrošinātu detalizētākus parametru aprakstus. Precīzāks šo parametru apraksts, norādot 4.4.2. punktā minētos drošības elementus, tiks ietverts īstenošanas aktā, kuru Komisija plāno pieņemt rudenī.

4.4.4. Uz risku balstīta regulatīvā pieeja.

17. pants nosaka, ka DPS piemērojama *ex post* uzraudzība, kuru veic valstu kompetentās iestādes. Dalībvalstīm jānodrošina, ka kompetentās iestādes rīkojas, kad tām sniegti pierādījumi, ka DPS nepilda direktīvas 16. pantā noteiktās prasības.

Turklāt saskaņā ar 16. panta 8. punktu un 9. punktu Komisija ir pilnvarota pieņemt īstenošanas aktus par paziņošanas un drošības prasībām, kas veicinās saskaņotības līmeni DPS. Bez tam saskaņā ar 16. panta 10. punktu dalībvalstīm nav atļauts DPS noteikt papildu drošības un paziņošanas prasības, kas atšķiras no tām, kas paredzētas direktīvā, izņemot gadījumus, kad šādi pasākumi ir nepieciešami, lai aizsargātu būtiskas valsts funkcijas, īpaši valsts drošību, un ļautu izmeklēt un atklāt noziedzīgus nodarījumus un saukt pie atbildības par to nodarīšanu.

Un visbeidzot, ņemot vērā DPS pārrobežu darbību, direktīvā ievērots nevis vairāku paralēlu jurisdikciju modelis, bet pieeja, kuras pamatā ir kritērijs par pakalpojuma sniedzēja galvenās uzņēmējdarbības atrašanās vietu ES.[38] Šī pieeja ļauj piemērot vienu noteikumu kopumu DPS, un par uzraudzību atbild viena kompetentā iestāde, un tas ir īpaši svarīgi, jo daudzi DPS piedāvā savus pakalpojumus vairākas dalībvalstīs vienlaikus. Šīs pieejas piemērošana mazina noteikumu slogu DPS un nodrošina pienācīgu digitālā vienotā tirgus darbību.

4.4.5. Jurisdikcija.

Kā skaidrots iepriekš, saskaņā ar TID direktīvas 18. panta 1. punktu DPS ir tās dalībvalsts jurisdikcijā, kurā ir tā galvenā uzņēmējdarbības vieta. Ja konkrēts DPS piedāvā pakalpojumus ES, bet neveic uzņēmējdarbību ES teritorijā, 18. panta 2. punkts nosaka pienākumu DPS iecelt pārstāvi Savienībā. Šādā gadījumā uzņēmums būs tās dalībvalsts jurisdikcijā, kurā iecelts pārstāvis. Gadījumos, kad DPS sniedz pakalpojumus dalībvalstī, bet nav iecēlis pārstāvi ES, dalībvalsts var principā vērsties pret DPS, jo pakalpojumu sniedzējs nepilda savus pienākumus, kas izriet no direktīvas.

4.4.6. Nelielu digitālo pakalpojumu sniedzēju atbrīvojums no drošības prasību un paziņošanas pienākumu izpildes.

Saskaņā ar 16. panta 11. punktu uz digitālo pakalpojumu sniedzējiem, kas ir mikrouzņēmumi vai mazie uzņēmumi Komisijas Ieteikuma 2003/361/EK39 izpratnē, neattiecas 16. pantā noteiktās drošības prasības un paziņošanas pienākums. Tas nozīmē, ka tiem uzņēmumiem, kas nodarbina mazāk nekā 50 personas un kuru gada apgrozījums un/vai gada bilance nepārsniedz 10 miljonus euro, šī prasība nav saistoša. Nosakot vienības lielumu, nav svarīgi, vai attiecīgais

[38] Skatīt īpaši direktīvas 18. pantu.
[39] OV L 24, 20.5.2003., 36. lpp.

uzņēmums sniedz tikai digitālos pakalpojumus TID direktīvas izpratnē vai arī citus pakalpojumus.

5. Saikne starp TID direktīvu un citiem tiesību aktiem.

Šīs iedaļas uzmanības centrā ir TID direktīvas 1. panta 7. punktā ietvertie *lex specialis* noteikumi; te iztirzāti trīs Komisijas līdz šim izvērtētie *lex specialis* piemēri, un skaidrotas drošības un paziņošanas prasības, kas piemērojamas telekomunikāciju un uzticamības pakalpojumu sniedzējiem.

5.1. TID direktīvas 1. panta 7. punkts: *lex specialis* noteikums.

Saskaņā ar TID direktīvas 1. panta 7. punktu noteikumus par drošības nodrošināšanu un/vai incidentu paziņošanu digitālo pakalpojumu sniedzējiem vai pamatpakalpojumu sniedzējiem saskaņā ar direktīvu nepiemēro, ja nozarspecifiskā ES tiesību aktā paredzētas drošības un/vai paziņošanas prasības, kas ir vismaz līdzvērtīgas TID direktīvā noteiktajiem pienākumiem. Dalībvalstīm, transponējot direktīvu kopumā, ir jāapsver 1. panta 7. punkts un jāsniedz informācija Komisijai par *lex specialis* noteikumu piemērošanu.

Metodika.

Izvērtējot kāda nozarspecifiska ES tiesība akta līdzvērtību attiecīgajiem TID direktīvas noteikumiem, īpaša nozīmē būtu jāpiešķir jautājumam, vai drošības prasības nozarspecifiskajā tiesību aktā ietver pasākumus, ar ko nodrošina tīklu un informācijas sistēmu drošību, kas definēta direktīvas 4. panta 2. punktā.

Tiktāl, ciktāl tas attiecas uz paziņošanas prasībām, TID direktīvas 14. panta 3. punkts un 16. panta 3. punkts nosaka, ka pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem bez nepamatotas kavēšanās jāpaziņo kompetentajām iestādēm vai *CSIRT* par ikvienu incidentu, kam ir nozīmīga/būtiska ietekme uz pakalpojuma sniegšanu. Šeit īpaša uzmanība jāpievērš pakalpojuma sniedzēja/digitālā pakalpojumu sniedzēja pienākumiem paziņojumā ietvert informāciju, kas ļauj kompetentajai iestādei vai *CSIRT* noteikt drošības incidenta pārrobežu ietekmes būtiskumu.

Šobrīd nav digitālo pakalpojumu sniedzējiem piemērojamu nozarspecifisku tiesību aktu, kas noteiktu drošības un paziņošanas prasības, kuras būtu salīdzināmas ar TID direktīvas 16. pantā noteiktajām un kuras varētu apsvērt, piemērojot TID direktīvas 1. panta 7. punktu[40].

Tiktāl, ciktāl tiek skarti pamatpakalpojumu sniedzēji, uz finanšu nozari un īpaši uz II pielikuma 3. un 4. punktā minēto banku un tirgus infrastruktūru nozari, šobrīd tiek attiecinātas drošības un/vai paziņošanas prasības, kas izriet no nozarspecifiskiem ES tiesību aktiem. Tas ir tāpēc, ka finanšu iestādēs lietoto IT un tīkla un informācijas sistēmu drošība un stabilitāte ir

[40] Tas neskar paziņojumu par personas datu aizsardzības pārkāpumu uzraudzības iestādei, kas minēta Vispārīgās datu aizsardzības regulas 33. pantā.

būtiska daļa no prasībām, kuras saskaņā ar ES tiesību aktiem ir izvirzītas finanšu iestādēm attiecībā uz operacionālajiem riskiem.

Piemēri.

i) Otrā Maksājumu pakalpojumu direktīva.

Attiecībā uz banku nozari un it īpaši, ciktāl tiek skarti maksājumu pakalpojumi, ko sniedz kredītiestādes, kuras definētas Regulas (ES) 575/2013 4. panta 1. punktā, tā sauktās Otrās Maksājumu pakalpojumu direktīvas (MPD 2)[41] 95. un 96. pantā ir noteiktas nosaka drošības un paziņošanas prasības.

Precīzāk, 95. panta 1. punkts nosaka pienākumu maksājumu pakalpojumu sniedzējiem ieviest atbilstošus riska mazināšanas pasākumus un kontroles mehānismus tādu operacionālo un drošības risku pārvaldībai, kas saistīti ar to sniegtajiem maksājumu pakalpojumiem. Ar šiem pasākumiem nosaka un uztur efektīvas incidentu pārvaldības procedūras, tostarp būtisku operacionālo un drošības incidentu atklāšanai un klasifikācijai. MPD 2 95. un 96. apsvērums sīkāk skaidro šādu drošības pasākumu raksturu. No šiem noteikumiem acīmredzami izriet, ka noteikto pasākumu mērķis ir pārvaldīt tādus drošības riskus, kas saistīti ar tīkliem un informācijas sistēmām, kas tiek izmantotas maksājumu pakalpojumu sniegšanai. Tādējādi šīs drošības prasības var uzskatīt par vismaz iedarbības ziņā līdzvērtīgām tām prasībām, kas noteiktas TID direktīvas 14. panta 1. un 2. punktā.

Attiecībā uz paziņošanas prasībām MPD 2 96. panta 1. punkts paredz pienākumu maksājumu pakalpojumu sniedzējiem bez nepamatotas kavēšanās paziņot par nopietniem incidentiem kompetentajai iestādei. Turklāt līdzīgi kā TID direktīvas 14. panta 5. punkts arī MPD 2 direktīvas 96. panta 2. punkts nosaka kompetentajām iestādēm pienākumu informēt citu dalībvalstu kompetentās iestādes, ja incidents tām ir būtisks. Šis pienākums tai pat laikā nozīmē, ka drošības incidenta paziņojumā jāietver informācija, kas ļauj iestādēm novērtēt incidenta pārrobežu ietekmes nozīmīgumu. MPD 2 direktīvas 96. panta 3. punkts šādā nolūkā pilnvaro EBI sadarbībā ar ECB izdot pamatnostādnes par paziņojuma precīzu saturu un formātu.

Tādējādi var secināt, ka saskaņā ar TID direktīvas 1. panta 7. punktu gan drošības, gan paziņošanas prasības, kas noteiktas MPD 2 direktīvas 95. un 96. pantā, būtu jāpiemēro TID direktīvas 14. panta attiecīgo noteikumu vietā, ciktāl tās attiecas uz kredītiestāžu sniegtajiem maksājumu pakalpojumiem.

ii) Eiropas Parlamenta un Padomes 2012. gada 4. jūlija Regula (ES) Nr. 648/2012 par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem.

Attiecībā uz finanšu tirgus infrastruktūru Regula (ES) 648/2012 kopā ar Komisijas Deleģēto regulu (ES) 153/2013 ietver noteikumus par drošības prasībām centrālajiem darījumu

[41] Direktīva (ES) 2015/2366, OV L 337, 23.12.2015., 35. lpp.

partneriem (CDP), kurus var uzskatīt par *lex specialis*. Konkrētāk, šie tiesību akti nosaka tehniskus un organizatoriskus pasākumus, kas saistīti ar tīklu un informācijas sistēmu drošību, kuri detalizācijas ziņā ir pat stingrāki nekā TID direktīvas 14. panta 1. punkta un 2. punkta prasības, un tādējādi var uzskatīt, ka tie izpilda TID direktīvas 1. panta 7. punkta prasības, ciktāl tas skar drošības prasības.

Precīzāk, Regulas (ES) 648/2012 26. panta 1. punkts nosaka, ka vienībai vajadzētu "*stingrus pārvaldības mehānismus, kas ietvertu skaidras organizatoriskās struktūras ar precīzi definētu, pārredzamu un konsekventu atbildības sadalījumu, efektīvām procedūrām esošo vai varbūtējo risku identificēšanai, pārvaldībai, uzraudzībai un ziņošanai un atbilstīgu iekšējās kontroles mehānismu, tostarp pareizas administratīvās un grāmatvedības procedūras*". 26. panta 3. punkts nosaka, ka organizatoriskajai struktūrai jānodrošina pakalpojumu un darbību veikšanas nepārtrauktība un pareiza funkcionēšana, izmantojot piemērotas un samērīgas sistēmas, resursus un procedūras.

Turklāt 26. panta 6. punkts skaidro, ka CDP ir jāuztur "*informācijas tehnoloģijas sistēmas, kas būtu piemērotas tam, lai tiktu galā ar dažādiem sarežģītiem un daudzveidīgiem pakalpojumiem un darbībām, ko veic, lai nodrošinātu augstus drošības standartus un uzturētās informācijas neskartību un slepenumu*". Turklāt 34. panta 1. punkts paredz, ka jāiedibina, jāīsteno un jāuztur piemērota uzņēmējdarbības nepārtrauktības politika un negadījuma seku novēršanas plāns, kas nodrošinātu darbību laicīgu atjaunošanu.

Šie pienākumi sīkāk precizēti Komisijas 2012. gada 19. decembra Deleģētajā regulā (ES) Nr. 153/2013, ar ko papildina Eiropas Parlamenta un Padomes Regulu (ES) Nr. 648/2012 attiecībā uz regulatīvajiem tehniskajiem standartiem par prasībām centrālajiem darījumu partneriem[42]. Jo īpaši tās 4. pants uzliek pienākumu CCP izveidot atbilstīgus riska pārvaldības rīkus, lai spētu pārvaldīt visus būtiskos riskus un ziņot par tiem, un norādīt arī pasākumu veidus (piemēram: stabilas informācijas un riska kontroles sistēmas, resursu, speciālistu pieejamība un piekļuve visai attiecīgajai informācijai, lai veiktu riska pārvaldības funkciju, piemēroti iekšējās kontroles mehānismi, kā piemēram, stabilas administratīvās un grāmatvedības procedūras, lai palīdzētu valdei uzraudzīt un novērtēt riska pārvaldības politikas piemērotību un efektivitāti, procedūru un sistēmas).

Pie tam 9. pants nepārprotami attiecas uz informācijas tehnoloģiju sistēmām un nosaka konkrētus tehniskus un organizatoriskus pasākumus, kas saistīti ar stabilas informācijas drošības sistēmas uzturēšanu pienācīgai IT drošības risku pārvaldīšanai. Šiem pasākumiem būtu jāietver mehānismi un procedūras, kas nodrošina pakalpojumu pieejamību un datu autentiskuma, integritātes un konfidencialitātes aizsardzību.

(iii) Eiropas Parlamenta un Padomes 2014. gada 15. maija Direktīva 2014/65/ES par finanšu instrumentu tirgiem un ar ko groza Direktīvu 2002/92/EK un Direktīvu 2011/61/ES[43].

[42] OV L 52, 23.2.2013., 41. lpp.
[43] OV L 173, 12.6.2014., 349. lpp.

Attiecībā uz tirdzniecības vietām Direktīvas 2014/65/ES 48. panta 1. punkts nosaka pienākumu pakalpojumu sniedzējiem nodrošināt savu pakalpojumu nepārtrauktību, ja to tirdzniecības sistēmā rodas jebkāda kļūme. Šo vispārīgo pienākumu tālāk precizējusi un papildinājusi 2016. gada 14. jūlija Komisijas Deleģētā regula (ES) 2017/584[44], ar ko Eiropas Parlamenta un Padomes Direktīvu 2014/65/ES papildina ar regulatīvajiem tehniskajiem standartiem par prasībām attiecībā uz tirdzniecības vietu organizāciju[45]. It īpaši minētās regulas 23. panta 1. punkts paredz, ka tirdzniecības vietas ievieš procedūras un mehānismus attiecībā uz fizisko un elektronisko drošību, ar kuriem paredzēts aizsargāt to sistēmas no ļaunprātīgas izmantošanas vai neatļautas piekļuves un nodrošināt datu integritāti. Šie pasākumi dotu iespēju novērst vai mazināt pret informācijas sistēmām vērstu uzbrukumu riskus.

23. panta 2. punkts nosaka arī, ka tirdzniecības vietu veiktajiem pasākumiem un mehānismiem jābūt tādiem, kas dod iespēju nekavējoties identificēt un pārvaldīt riskus, kas saistīti ar neatļautu piekļuvi, sistēmas traucējumiem, kas ievērojami apgrūtina vai pārtrauc informācijas sistēmas darbību, datu traucējumiem, kas apdraud to pieejamību, integritāti vai autentiskumu. Turklāt minētās regulas 15. pants nosaka pienākumu tirdzniecības vietām ieviest efektīvus uzņēmējdarbības nepārtrauktības nodrošināšanas mehānismus, kas nodrošina, ka tās sistēmas ir pietiekami stabilas un var risināt traucējumus radošus incidentus. Šādiem mehānismiem jo īpaši jānodrošina tirdzniecības vietām iespēja atsākt tirdzniecību divās stundās vai apmēram tādā laikā un vienlaikus jānodrošina, ka zaudēto datu apjoms ir tuvu nullei.

16. pants nosaka, ka identificētie mehānismi traucējumus radošu incidentu risināšanai un pārvaldībai jāietver tirdzniecības vietu darbības nepārtrauktības plānā, un nosaka īpašus elementus, kas tirdzniecības vietai jāapsver, pieņemot darbības nepārtrauktības plānu (piemēram, speciālas drošības pasākumu vienības izveide, ietekmes novērtējums, kura ietvaros apzina riskus un kurš regulāri tiek pārskatīts).

Ņemot vērā šo drošības pasākumu saturu, konstatējams, ka tie paredzēti, lai pārvaldītu un risinātus riskus, kas saistīti ar datu vai sniegto pakalpojumu pieejamību, autentiskumu, integritāti un konfidencialitāti, un līdz ar to var secināt, ka iepriekšminētie nozarspecifiskie ES tiesību akti ietver drošības pienākumus, kas iedarbības ziņā ir vismaz ekvivalenti TID direktīvas 14. panta 1. un 2. punktā minētajiem attiecīgajiem pienākumiem.

5.2. TID direktīvas 1. panta 3. punkts: Telekomunikāciju un uzticamības pakalpojumu sniedzēji.

Saskaņā ar 1. panta 3. punktu direktīvā noteiktās drošības un paziņošanas prasības neattiecas uz pakalpojumu sniedzējiem, kam piemēro Direktīvas 2002/21/EK 13.a panta un 13.b panta prasības. Direktīvas 2002/21/EK 13.a pants un 13.b pants piemērojami uzņēmumiem, kas nodrošina publiskus komunikāciju tīklus un publiski pieejamus elektronisko komunikāciju

[44] OV L 87, 31.3.2017., 350. lpp.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

pakalpojumus Tādējādi uzņēmumam jāievēro Direktīvas 2002/21/EK drošības un paziņošanas prasības, ciktāl tas skar publisku komunikāciju tīklu un publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu.

Taču, ja tas pats uzņēmums sniedz arī citus TID direktīvas III pielikumā minētos pakalpojumus, piemēram, digitālos pakalpojumus (piemēram, mākoņdatošana vai tiešsaistes tirdzniecības vieta) vai tādus pakalpojumus kā DNS vai IPAP saskaņā ar TID direktīvas II pielikuma 7. punktu, uz uzņēmumu attiecina TID direktīvas drošības un paziņošanas prasības saistībā tieši ar šo pakalpojumu sniegšanu. Jāpiebilst, ka, tā kā II pielikuma 7. punktā minēto pakalpojumu sniedzēji pieder pie pamatpakalpojumu sniedzēju kategorijas, dalībvalstīm ir pienākums veikt identifikācijas procesu saskaņā ar 5. panta 2. punktu un norādīt, kādiem konkrētiem DNS, IPAP vai TLD pakalpojumu sniedzējiem ir jāievēro TID direktīvas prasības. Tas nozīmē, ka pēc šāda novērtējuma tikai tiem DNS, IPAP vai TLD pakalpojumu sniedzējiem, kas atbilst TID direktīvas 5. panta 2. punkta kritērijiem, tiks noteikts pienākums ievērot TID direktīvas prasības.

1. panta 3. punkts tālāk norāda, ka direktīvā noteiktās drošības un paziņošanas prasības neattiecas arī uz uzticamības pakalpojumu sniedzējiem, kas pakļauti līdzīgām prasībām saskaņā ar Regulas (ES) Nr. 910/2014 19. pantu.

6. Publicētie valstu kiberdrošības stratēģijas dokumenti.

	Dalībvalsts	Stratēģijas nosaukums un pieejamās saites
1	Austrija	*Austrijas kiberdrošības stratēģija* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Beļģija	*Kibertelpas aizsardzība* (2012.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgārija	*Kiberdroša Bulgārija 2020* (2016.) http://www.cyberbg.eu/ (BG)
4	Horvātija	*Horvātijas Republikas nacionālā kiberdrošības stratēģija* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Čehijas Republika	*Čehijas Republikas nacionālā kiberdrošības stratēģija laika periodam no 2015. līdz 2020. gadam* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Kipra	*Kipras Republikas kiberdrošības stratēģija* (2012.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Dānija	*Dānijas kiberdrošības un informācijas drošības stratēģija* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Igaunija	*Kiberdrošības stratēģija* (2014.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Somija	*Somijas kiberdrošības stratēģija* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Francija	*Francijas nacionālā digitālās drošības stratēģija* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Īrija	*Nacionālā kiberdrošības stratēģija 2015.-2017.* (2015.)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Itālija	*Nacionālā stratēģija kibertelpas drošībai* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Vācija	*Vācijas kiberdrošības stratēģija* (2016.) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ungārija	*Ungārijas nacionālā kiberdrošības stratēģija* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Latvija	*Latvijas kiberdrošības stratēģija 2014.–2018.* (2014.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Lietuva	*Elektroniskās informācijas drošības (kiberdrošības) attīstības programma 2011.–2019. gadam* (2011.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luksemburga	*Nacionālās kiberdrošības stratēģija II (2015.)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*Nacionālās kiberdrošības stratēģijas zaļā grāmata* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Nīderlande	*Nacionālā kiberdrošības stratēģija 2* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polija	*Polijas Republikas kibertelpas aizsardzības politika* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Rumānija	*Rumānijas kiberdrošības stratēģija* (2011.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugāle	*Nacionālā kiberdrošības stratēģija* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view

		(EN)
23	Slovākijas Republika	*Slovākijas Republikas kiberdrošības koncepcija 2015.–2020.* (2015.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovēnija	*Kiberdrošības stratēģija, kas nosaka augsta līmeņa kiberdrošības sistēmas izveidi* (2016.) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Spānija	*Nacionālā kiberdrošības stratēģija* (2013.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Zviedrija	*Zviedrijas nacionālā kiberdrošības stratēģija* (2017.) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Apvienotā Karaliste	*Nacionālā kiberdrošības stratēģija (2016.–2021.)* (2016.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. *ENISA* sagatavots labas prakses un ieteikumu saraksts.

Incidentu paziņošana

- ✓ Stratēģijas reaģēšanai uz incidentiem un sadarbība kiberdrošības krīzē[46]

Incidentu risināšana

- ✓ Incidentu risināšanas automatizācijas projekts[47]
- ✓ Labas prakses ceļvedis incidentu pārvaldībā[48]

Incidentu klasifikācija un taksonomija

- ✓ Esošu taksonomiju pārskats[49]
- ✓ Labas prakses ceļvedis, kā izmantot taksonomijas incidentu novēršanā un atklāšanā[50]

CSIRT briedums

- ✓ Valstu *CSIRT* risināmie uzdevumi Eiropā 2016. gadā: Pētījums par *CSIRT* briedumu[51]
- ✓ Pētījums par *CSIRT* briedumu — novērtējuma process[52]
- ✓ Vadlīnijas valstu un valdību *CSIRT* par brieduma novērtēšanu[53]

CSIRT spēju veidošana un apmācība

- ✓ Labas prakses ceļvedis par apmācības metodikām[54]

Kā atrast informāciju par Eiropā izveidotajiem *CSIRT* — *CSIRT* saraksts pa valstīm[55]

---

[46] *ENISA, Stratēģijas reaģēšanai uz incidentiem un sadarbība kiberdrošības krīzē* (2016.) Skatīt:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

[47] Sīkāka informācija: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

[48] *ENISA, Labas prakses ceļvedis incidentu pārvaldībā* (2010.) Skatīt:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[49] Sīkāka informācija: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

[50] *ENISA, Labas prakses ceļvedis, kā izmantot taksonomijas incidentu novēršanā un atklāšanā (2017.).* Skatīt:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection

[51] *ENISA, Valstu CSIRT risināmie uzdevumi Eiropā 2016. gadā: Pētījums par CSIRT briedumu* (2017.). Skatīt:https://www.enisa.europa.eu/publications/study-on-csirt-maturity

[52] *ENISA, Pētījums par CSIRT briedumu — novērtējuma process* (2017.). Skatīt:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[53] *ENISA*, CSIRT spējas. *Kā novērtēt briedumu? Vadlīnijas valstu un valdību CSIRT* (2016.). Skatīt: https://www.enisa.europa.eu/publications/csirt-capabilities

[54] *ENISA, Labas prakses ceļvedis par apmācību metodikām (2014.).* Skatīt:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies

[55] Sīkāka informācija: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map