

Briselē, 16.12.2020.
COM(2020) 823 final

2020/0359 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA,

**ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kibersdrošību visā
Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148**

(Dokuments attiecas uz EEZ)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Šis priekšlikums ir daļa no pasākumu kopuma, kura mērķis ir uzlabot publisko un privāto vienību, kompetento iestāžu un visas Savienības turpmāku noturību un spēju reaģēt uz incidentiem kibernetiskās drošības un kritisko infrastruktūru aizsardzības jomā. Tas atbilst Komisijas prioritātēm nodrošināt, ka Eiropa ir gatava digitālajam laikmetam, un veidot nākotnei sagatavotu ekonomiku, kas strādā cilvēku labā. Kibernetiskā drošība ir viena no Komisijas prioritātēm reaģēšanā uz Covid-19 krīzi. Pasākumu kopums ietver jaunu stratēģiju par kibernetiskās drošības, kuras mērķis ir nostiprināt Savienības stratēģisko autonomiju, lai uzlabotu tās noturību un kopīgu reaģēšanu un veidotu atvērtu un globālu internetu. Visbeidzot, pasākumu kopums ietver priekšlikumu direktīvai par pamatpakalpojumu kritisko sniedzēju noturību, kuras mērķis ir mazināt fiziskos draudus šādiem sniedzējiem.

Šā priekšlikuma pamatā ir Direktīva (ES) 2016/1148 par tīklu un informācijas sistēmu drošību (TID direktīva), un tas atceļ minēto direktīvu, kas bija pirmais ES mēroga tiesību akts par kibernetiskās drošības. Tas arī paredz juridiskus pasākumus vispārējā kibernetiskās drošības līmeņa uzlabošanai Savienībā. Ar TID direktīvu ir 1) veicināta kibernetiskās drošības spēju uzlabošanās valstu līmenī, pieprasot, lai dalībvalstis pieņem valsts kibernetiskās drošības stratēģijas un iecel kibernetiskās drošības iestādes; 2) palielināta sadarbība starp dalībvalstīm Savienības līmenī, izveidojot dažādus forumus, kas veicina stratēģiskās un operatīvās informācijas apmaiņu, un 3) uzlabota publisko un privāto vienību kibernetiskās drošības septiņās īpašās nozarēs (enerģētika, transports, banku pakalpojumi, finanšu tirgus infrastruktūras, veselības aprūpe, dzīvojamā ēdiena piegāde un sadale un digitālās infrastruktūras) un trīs digitālo pakalpojumu nozarēs (tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas un mākoņpakalpojumi), pieprasot dalībvalstīm nodrošināt, ka pamatpakalpojumu sniedzēji un digitālo pakalpojumu sniedzēji ievieš kibernetiskās drošības prasības un ziņo par incidentiem.

Ar priekšlikumu tiek modernizēts esošais tiesiskais regulējums, ņemot vērā pieaugošo iekšējā tirgus digitalizāciju iepriekšējos gados un mainīgos kibernetiskās drošības apstākļus. Abas šīs norises kopš Covid-19 krīzes sākšanās ir pastiprinājušās vēl vairāk. Priekšlikumā ir arī aplūkoti vairāki trūkumi, kas liegusi izmantot visu TID direktīvas potenciālu.

Neraugoties uz tās ievērojamiem sasniegumiem, TID direktīva, kas lika pamatus ievērojamām izmaiņām domāšanas veidā attiecībā uz institucionālo un regulatīvo pieeju kibernetiskās drošības daudzās dalībvalstīs, ir apliecinājusi savus ierobežojumus. Sabiedrības digitālā pārveide (ko pastiprināja Covid-19 krīze) ir paplašinājusi draudu ainu un rada jaunas problēmas, attiecībā uz kurām ir vajadzīgi pielāgoti un inovatīvi reaģēšanas pasākumi. Kibernetiskās drošības skaits turpina pieaugt, un no avotiem gan ES, gan ārpus tās tiek vērsti arvien sarežģītāki uzbrukumi.

TID direktīvas darbības izvērtējumā, kas veikts ietekmes novērtējuma vajadzībām, tika identificētas šādas problēmas: 1) uzņēmumu, kas darbojas ES, zemais kibernetiskās drošības līmenis; 2) nevienmērīga noturība starp dalībvalstīm un nozarēm un 3) kopējās situācijas apzināšanās zemais līmenis un kopīgas reaģēšanas uz krīzi trūkums. Piemēram, uz dažām lielām slimnīcām dalībvalstī TID direktīvas darbības joma neattiecas, un tāpēc tām nav jāsteno izrietošie drošības pasākumi, savukārt citā dalībvalstī gandrīz uz katru veselības aprūpes sniedzēju valstī attiecas TID drošības prasības.

Priekšlikumam, kas ir Normatīvās atbilstības un izpildes programmas (*REFIT*) iniciatīva, mērķis ir mazināt regulatīvo slogu kompetentajām iestādēm un atbilstības nodrošināšanas izmaksas publiskajām un privātajām vienībām. Tas jo īpaši tiek panākts, atceļot pienākumu

kompetentajām iestādēm noteikt pamatpakalpojumu sniedzējus un paaugstinot drošības un ziņošanas prasību saskaņošanas līmeni, lai sekmētu regulatīvo atbilstību attiecībā uz vienībām, kas sniedz pārrobežu pakalpojumus. Tajā pašā laikā kompetentajām iestādēm arī tiks noteikti jauni uzdevumi, tai skaitā vienību uzraudzība nozarēs, uz kurām līdz šim TID direktīva neattiecas.

- **Saskanība ar pašreizējiem noteikumiem konkrētajā politikas jomā**

Šis priekšlikums ir daļa no plašāka esošu tiesību instrumentu un gaidāmo iniciatīvu kopuma Savienības līmenī, kura mērķis ir palielināt publisko un privāto vienību noturību pret draudiem.

Kiberdrošības jomā to vidū ir jo īpaši Direktīva (ES) 2018/1972 par Eiropas Elektronisko sakaru kodeksa izveidi (kuras ar kiberdrošību saistītie noteikumi tiks aizstāti ar konkrētā priekšlikuma noteikumiem) un priekšlikums regulai par finanšu sektora digitālās darbības noturību (COM(2020) 595 *final*), kura tiks uzskatīta par konkrētā priekšlikuma *lex specialis*, kad abi akti būs stājušies spēkā.

Fiziskās drošības jomā priekšlikums papildina priekšlikumu direktīvai par kritisko vienību noturību, ar ko tiek pārskatīta Direktīva 2008/114/EK par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību (EKI direktīva), ar kuru tiek noteikts Savienības process Eiropas kritisko infrastruktūru apzināšanai un noteikšanai un kurā izklāstīta pieeja to aizsardzības uzlabošanai. Komisija 2020. gada jūlijā pieņēma ES Drošības savienības stratēģiju¹, kurā tika atzīts, ka savstarpējā saikne un atkarība starp fiziskajām un digitālajām infrastruktūrām palielinās. Tajā tika uzsvērtā vajadzība pēc saskaņotākas un konsekvētākas pieejas starp EKI direktīvu un Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

Tāpēc priekšlikums ir cieši saskaņots ar priekšlikumu direktīvai par kritisko vienību noturību, kuras mērķis ir uzlabot kritisko vienību noturību pret fiziskiem draudiem daudzās nozarēs. Priekšlikuma mērķis ir nodrošināt, ka kompetentās iestādes saskaņā ar abiem tiesību aktiem veic papildinošus pasākumus un pēc vajadzības apmainās ar informāciju par kiberneturību un cita veida noturību un ka jo īpaši uz kritiskajiem operatoriem nozarēs, ko uzskata par “būtiskām” konkrētā priekšlikuma kontekstā, attiecas arī vispārīgāki noturības veicināšanas pienākumi, uzsvaru liekot uz riskiem, kas nav saistīti ar kiberdrošību.

- **Saskanība ar citām Savienības politikas jomām**

Kā izklāstīts paziņojumā “Eiropas digitālās nākotnes veidošana”², Eiropai ir ļoti svarīgi izmantot visas digitālā laikmeta priekšrocības un stiprināt tās rūpniecības un inovācijas spējas, ievērojot drošas un ētiskas robežas. Eiropas Datu stratēģijā ir paredzēti četri pīlāri — datu aizsardzība, pamattiesības, drošums un kiberdrošība — kā būtiski priekšnoteikumi sabiedrībai, kam datu izmantošana sniedz iespējas.

Eiropas Parlaments 2019. gada 12. marta rezolūcijā aicināja “(..) Komisiju izvērtēt, vai ir nepieciešams paplašināt minētās TID direktīvas darbības jomu, attiecinot to arī uz citām kritiskām nozarēm un pakalpojumiem, uz kuriem neattiecas īpaši konkrēto nozari regulējoši

¹ COM(2020) 605 *final*.

² COM(2020) 67 *final*.

tiesību akti”³. Padome savos 2020. gada 9. jūnija secinājumos atzinīgi novērtēja “(..) Komisijas plānus nodrošināt konsekventus noteikumus tirgus dalībniekiem un veicināt drošu, stabilu un atbilstīgu informācijas par apdraudējumiem un incidentiem kopīgošanu, tostarp, pārskatot Tīklu un informācijas drošības direktīvu (TID direktīvu), lai izmantotu iespējas uzlabot kiberneturību un efektīvāk reaģētu uz kiberuzbrukumiem, jo īpaši attiecībā uz būtiskām ekonomiskām un sabiedriskām darbībām, vienlaikus ievērojot dalībvalstu kompetenci, tostarp atbildību par savu nacionālo drošību”⁴. Turklāt ierosinātais tiesību akts neskar Līgumā par Eiropas Savienības darbību (LESD) paredzēto konkurences noteikumu piemērošanu.

Ņemot vērā, ka ievērojamai daļai kiberdraudu avots ir ārpus ES, ir vajadzīga konsekventa pieeja attiecībā uz starptautisko sadarbību. Šī direktīva ir atsauces modelis, kas jāveicina saistībā ar ES sadarbību ar trešām valstīm, jo īpaši tad, kad sniedz ārēju tehnisko palīdzību.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

• Juridiskais pamats

TID direktīvas juridiskais pamats ir Līguma par Eiropas Savienības darbību 114. pants, kura mērķis ir iekšējā tirgus izveide un darbība, uzlabojot pasākumus valstu tiesisko regulējumu tuvināšanai. Kā ES Tiesa noteica savā spriedumā lietā C-58/08 *Vodafone un citi*, LESD 114. panta izmantošana ir pamatota, ja pastāv tādas atšķirības valstu tiesisko regulējumu starpā, kuras tiešā veidā ietekmē iekšējā tirgus darbību. Tāpat Tiesa nosprieda, ka, ja ar tiesību aktu, kura pamatā ir LESD 114. pants, jau ir novērsti visi šķēršļi tirdzniecībai jomā, ko ar šo aktu saskaņo, Savienības likumdevējam nevar liegt iespēju šo aktu pielāgot apstākļu izmaiņām vai jaunām zināšanām, ņemot vērā viņa uzdevumu uzraudzīt vispārējo Līgumā paredzēto interešu aizsardzību. Visbeidzot, Tiesa nosprieda, ka tuvināšanas pasākumi, uz kuriem attiecas LESD 114. pants, ir paredzēti, lai atkarībā no saskaņojamā jautājuma vispārējā konteksta un konkrētajiem apstākļiem piešķirtu rīcības brīvību attiecībā uz to, kāda aktu tuvināšanas tehnika ir vispiemērotākā vēlāmā rezultāta sasniegšanai. Ar ierosināto tiesību aktu tiks likvidēti iekšējā tirgus šķēršļi un uzlabota iekšējā tirgus izveide un darbība būtiskām un svarīgām vienībām, nosakot skaidrus vispārpiemērojamus noteikumus par TID direktīvas piemērošanu, saskaņojot noteikumus, kas piemērojami kiberdrošības riska pārvaldības un incidentu paziņošanas jomā. Pašreizējās likumdošanas un uzraudzības, kā arī valsts un ES līmeņu atšķirības šajā jomā ir šķēršļi iekšējam tirgum, jo vienības, kas veic pārrobežu darbības, saskaras ar atšķirīgām regulatīvajām prasībām, kas, iespējams, pārklājas, un/vai to piemērošanu, kas var kaitēt brīvības veikt uzņēmējdarbību un sniegt pakalpojumus īstenošanai. Atšķirīgiem noteikumiem arī ir negatīva ietekme uz konkurences apstākļiem iekšējā tirgū, kad runa ir par viena veida vienībām dažādās dalībvalstīs.

• Subsidiaritāte (neekskluzīvas kompetences gadījumā)

Kiberdrošības noturība visā Savienībā nevar būt efektīva, ja attiecībā uz to tiek īstenotas atšķirīgas valstu vai reģionālās pieejas. Ar TID direktīvu daļēji risināts šis trūkums, nosakot satvaru tīklu un informācijas sistēmu drošībai valstu un Savienības līmenī. Tomēr tās transponēšana un īstenošana arī atklāja konkrētiem noteikumiem un pieejām raksturīgos trūkumus un ierobežojumus, piemēram, neskaidro direktīvas darbības jomas norobežojumu, kā rezultātā radās būtiskas dalībvalstu līmenī īstenotās ES iejaukšanās tvēruma un dziļuma

³ https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_LV.html.

⁴ <https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/lv/pdf>.

atšķirības. Turklāt kopš Covid-19 krīzes Eiropas ekonomika ir kļuvusi tik atkarīga no tīklu un informācijas sistēmām kā nekad iepriekš, un nozares un pakalpojumi kļūst arvien vairāk savstarpēji atkarīgi. ES iejaukšanos, kas pārsniedz pašreizējos TID direktīvas pasākumus, pamato galvenokārt šādi faktori: i) tas, ka ar TID saistītajiem draudiem un problēmām arvien biežāk ir pārrobežu raksturs; ii) Savienības rīcības potenciāls uzlabot un veicināt efektīvu un koordinētu valsts politiku un iii) saskaņotas un sadarbīgas politikas rīcības ieguldījums efektīvā datu un privātuma aizsardzībā.

- **Proporcionalitāte**

Šajā direktīvā ierosinātie noteikumi nepārsniedz to, kas ir nepieciešams konkrēto mērķu apmierinošai sasniegšanai. Paredzētā drošības pasākumu un ziņošanas pienākumu saskaņošana un racionalizācija ir saistīta ar dalībvalstu un uzņēmumu lūgumiem uzlabot pašreizējo satvaru.

Priekšlikumā ir ņemta vērā dalībvalstīs jau pastāvošā prakse. Uzlabots aizsardzības līmenis, ko panāk, racionalizējot un koordinējot prasības, ir proporcionāls pieaugošajiem riskiem, arī tiem, kam piemīt pārrobežu elements; prasības ir pamatotas un kopumā atbilst to vienību interesēm, kuras iesaistītas savu pakalpojumu nepārtrauktības un kvalitātes nodrošināšanā. Izmaksas saistībā ar sistemātiskas sadarbības nodrošināšanu starp dalībvalstīm būs mazas salīdzinājumā ar ekonomiskajiem un sociālajiem zaudējumiem un kaitējumu, ko izraisa kibernetikas incidenti. Turklāt apspriedes ar ieinteresētajām personām, kas notikušas saistībā ar TID direktīvas pārskatīšanu, tai skaitā atklātās sabiedriskās apspriešanas un mērķtiecīgu aptauju rezultāti, norāda uz atbalstu TID direktīvas pārskatīšanai, kā izklāstīts iepriekš.

- **Tiesību instrumenta izvēle**

Ar priekšlikumu tiks vēl vairāk racionalizēti uzņēmumiem noteiktie pienākumi un nodrošināts augstāks to saskaņošanas līmenis. Tajā pašā laikā priekšlikuma mērķis ir nodrošināt dalībvalstīm elastīgumu, kas vajadzīgs, lai ņemtu vērā valstu specifiku (piemēram, iespēju noteikt būtiskas vai svarīgas papildu vienības, kas pārsniedz ar tiesību aktu noteikto pamatscenāriju). Tāpēc gaidāmajam tiesību aktam vajadzētu būt direktīvai, jo šis tiesību instruments ļauj mērķtiecīgi uzlabot saskaņotību, ka arī nodrošina zināmu elastīgumu kompetentajām iestādēm.

3. EX POST IZVĒRTĒJUMU, APSPIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- **Ex post izvērtējumi / spēkā esošo tiesību aktu atbilstības pārbaudes**

Komisija veica TID direktīvas darbības izvērtējumu⁵. Tā ir analizējusi direktīvas atbilstīgumu, ES pievienoto vērtību, saskaņotību, efektivitāti un lietderīgumu. Šīs analīzes galvenie konstatējumi ir izklāstīti turpmāk.

- TID direktīvas darbības joma ir pārāk ierobežota aptverto nozaru ziņā, galvenokārt šādu iemeslu dēļ: i) pieaugošā digitalizācija pēdējos gados un augstāka savstarpējās savienojamības pakāpe; ii) TID direktīvas darbības joma vairs neatspoguļo visas digitalizētās nozares, kas sniedz pamatpakalpojumus ekonomikai un sabiedrībai kopumā.

⁵ [Ietekmes novērtējuma 5. pielikums].

- TID direktīvas darbības joma nav pietiekami skaidra attiecībā uz pamatpakalpojumu sniedzējiem, un tās noteikumi nerada pietiekamu skaidrību par valstu kompetenci attiecībā uz digitālo pakalpojumu sniedzējiem. Tas ir radījis situāciju, kad noteiktu veidu vienības nav apzinātas visās dalībvalstīs, un tādējādi tām nav jāievieš drošības pasākumi un jāziņo par incidentiem.
- TID direktīva nodrošināja dalībvalstīm plašu rīcības brīvību, kad tās nosaka drošības un incidentu paziņošanas prasības pamatpakalpojumu sniedzējiem (turpmāk “PPS”). Izvērtējums liecina, ka dažos gadījumos dalībvalstis ir īstenojušas šīs prasības ļoti atšķirīgi, radot papildu slogu uzņēmumiem, kas darbojas vairāk nekā vienā dalībvalstī.
- TID direktīvas uzraudzības un izpildes režīms ir neefektīvs. Piemēram, dalībvalstis ir ļoti negribīgi piemērojušas sodus vienībām, kas nav ieviesušas drošības prasības vai nav ziņojušas par incidentiem. Tas var radīt negatīvas sekas individuālu vienību kibernoturībai.
- Finansiālie resursi un cilvēkresursi, ko dalībvalstis atvēlējušas savu uzdevumu izpildei (piemēram, PPS identificēšanai vai uzraudzībai), un attiecīgi dažādie brieduma līmeņi kiberdrošības risku pārvaldībā ievērojami atšķiras. Tas vēl vairāk pastiprina kibernoturības atšķirības starp dalībvalstīm.
- Dalībvalstis neveic sistemātisku informācijas apmaiņu savā starpā, un tas negatīvi ietekmē jo īpaši kiberdrošības pasākumu efektivitāti un kopējo situācijas apzināšanos ES līmenī. Tas attiecas arī uz informācijas apmaiņu starp privātām vienībām un iesaisti starp ES līmeņa sadarbības struktūrām un privātām vienībām.
- **Apspriešanās ar ieinteresētajām personām**

Komisija ir apspriedusies ar plašu ieinteresēto personu loku. Dalībvalstis un ieinteresētās personas tika uzaicinātas piedalīties atklātajā sabiedriskajā apspriešanās, kā arī apsekojumos un darbsemināros, ko organizēja *Wavestone*, *CEPS* un *ICF*, kurus Komisija ir nolīgusi pētījuma veikšanai, lai atbalstītu TID direktīvas pārskatīšanu. Starp ieinteresētajām personām, ar kurām notika apspriešanās, bija kompetentās iestādes, Savienības struktūras, kuru darbs saistīts ar kiberdrošību, pamatpakalpojumu sniedzēji, digitālo pakalpojumu sniedzēji, vienības, kas sniedz pakalpojumus ārpus pašreizējās TID direktīvas darbības jomas, arodasociācijas un patērētāju organizācijas, kā arī iedzīvotāji.

Turklāt Komisija pastāvīgi sazinājās ar kompetentajām iestādēm, kas atbild par TID direktīvas īstenošanu. Sadarbības grupa ir pārrunājusi dažādus transversālus un nozaru īstenošanas aspektus. Visbeidzot, veicot ar TID saistītus valstu apmeklējumus 2019. un 2020. gadā, Komisija nointervēja 154 publiskas un privātas vienības, kā arī 117 kompetentās iestādes.

- **Ekspertu atzinumu iegūšana un izmantošana**

Komisija ir nolīgusi *Wavestone*, *CEPS* un *ICF* konsorciju, lai tas atbalstītu Komisiju TID direktīvas pārskatīšanā⁶. Līgumslēdzējs ir ne tikai sazinājies ar ieinteresētajām personām, ko tieši skar TID direktīva, veicot mērķtiecīgas aptaujas un rīkojot darbseminārus, bet arī

⁶ Pētījums, lai atbalstītu Direktīvas (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (TID direktīva) pārskatīšanu — Nr. 2020-665. *Wavestone*, *CEPS* un *ICF*.

apspriedies ar plašu ekspertu loku kibersdrošības jomā, piemēram, kibersdrošības pētniekiem un kibersdrošības nozares speciālistiem.

- **Ietekmes novērtējums**

Šim priekšlikumam ir pievienots ietekmes novērtējums⁷, kas 2020. gada 23. oktobrī tika iesniegts Regulējuma kontroles padomei (RKP) un par ko 2020. gada 20. novembrī tika saņemts pozitīvs RKP atzinums ar komentāriem. RKP ieteica uzlabojumus dažās jomās, lai: 1) problēmu analīzē labāk atspoguļotu netiešo pārrobežu ietekmi; 2) labāk izskaidrotu, kādi varētu būt iniciatīvas panākumi; 3) stingrāk pamatotu politikas iespēju sarakstu; 4) plašāk raksturotu ierosināto pasākumu izmaksas. Ietekmes novērtējums tika pielāgots, lai ņemtu vērā šos punktus, kā arī sīkākus RKP komentārus. Tagad tajā ir ietverti sīkāki skaidrojumi par netiešās pārrobežu ietekmes lomu kibersdrošības jomā, ir sniegts skaidrāks pārskats par to, kā var novērtēt panākumus, ir sniegts sīkāks paskaidrojums par dažādo politikas iespēju struktūru un loģiku un iespējās ietilpstošajām aplūkotajām darbībām, ir sniegts sīkāks skaidrojums par aspektiem, kas analizēti saistībā ar TID direktīvas nozaru tvērumu, un ir sniegti sīkāki skaidrojumi par izmaksām.

Komisija izskatīja vairākas politikas iespējas, kā uzlabot tiesisko regulējumu saistībā ar kiberneturību un reaģēšanu uz incidentiem.

- “Nedarīt neko” — TID direktīva netiek mainīta un netiek veikti nekādi citi nelegislatīvi pasākumi, lai risinātu TID direktīvas izvērtējumā apzinātās problēmas.
- 1. iespēja — izmaiņas likumdošanas līmenī netiek ieviestas. Tā vietā Komisija izdod ieteikumus un pamatnostādnes (piemēram, par pamatpakalpojumu sniedzēju identificēšanu, drošības prasībām, incidentu paziņošanas procedūrām un uzraudzību), apspriežoties ar sadarbības grupu, ES Kibersdrošības aģentūru (*ENISA*) un attiecīgā gadījumā ar datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu.
- 2. iespēja — šī iespēja ietver mērķtiecīgus grozījumus TID direktīvā, tai skaitā darbības jomas paplašināšanu un vairākus citus grozījumus, kuru mērķis ir garantēt noteiktus tūlītējus risinājumus konstatētajām problēmām, nodrošinot lielāku skaidrību un turpmāku saskaņošanu (piemēram, noteikumi apzināšanas robežvērtību saskaņošanai). Tomēr grozītajā TID direktīvā tiek saglabāti tās struktūras pamatelementi, pieeja un loģiskais pamatojums.
- 3. iespēja — šis scenārijs ietver sistēmiskas un strukturētas izmaiņas TID direktīvā (pieņemot jaunu direktīvu), kuras paredz stingrāku pieejas novirzīšanu uz to, lai aptvertu plašāku tautsaimniecību segmentu visā Savienībā, un vienlaikus mērķtiecīgāku uzraudzību, kas vērsta uz lielajiem un galvenajiem tirgus dalībniekiem. Ar to arī racionalizēs pienākumus, kas noteikti uzņēmumiem, un nodrošinās augstāku to saskaņošanas līmeni, radīs efektīvāku vidi operatīvajiem aspektiem, kā arī noteiks skaidru pamatu uzlabotai dažādu ieinteresēto personu dalītai atbildībai un pārskatatbildībai attiecībā uz kibersdrošības pasākumiem.

Ietekmes novērtējumā ir secināts, ka vēlamā iespēja ir 3. iespēja (t. i., sistēmiskas un strukturālas izmaiņas TID regulējumā). No efektivitātes viedokļa vēlamā iespēja skaidri noteiktu TID direktīvas piemērošanas jomu, kas paplašināta, aptverot arī ES tautsaimniecību un sabiedrību reprezentatīvāku daļu, un prasību racionalizēšanu, vienlaikus paredzot skaidrāk definētu satvaru uzraudzībai un izpildei, lai paaugstinātu atbilstības līmeni. Tā arī ietver

⁷ [Jāpievieno saites uz galīgo dokumentu un kopsavilkuma lapu.]

pasākumus, kuru mērķis ir uzlabot politikas veidošanas pieejas dalībvalstu līmenī un mainīt to paradigmu, veicinot jaunus regulējumus attiecību ar piegādātājiem riska pārvaldībai un koordinētai neaizsargātības atklāšanai. Tajā pašā laikā vēlamā politikas iespēja nosaka skaidru pamatu dalītai atbildībai un pārskatatbildībai un paredz mehānismus, kuru mērķis ir veicināt lielāku uzticēšanos starp dalībvalstīm — gan iestādēm, gan nozares pārstāvjiem —, stimulējot informācijas apmaiņu un nodrošinot operatīvāku pieeju, piemēram, savstarpējās palīdzības un salīdzinošās izvērtēšanas mehānismus. Šī iespēja arī paredz ES krīžu pārvaldības satvaru, kas balstīts uz nesen atklāto ES operatīvo tīklu, un nodrošina ENISA plašāku iesaistīšanu tās pašreizējo pilnvaru ietvaros precīza pārskata sniegšanā par kibernetikas stāvokli Savienībā.

No efektivitātes viedokļa, lai gan vēlamā iespēja ietver papildu atbilstības un izpildes nodrošināšanas izmaksas uzņēmumiem un dalībvalstīm, tā arī radīs efektīvus kompromisus un sinerģijas, un tai ir no visām analizētajām politikas iespējām vislielākais potenciāls nodrošināt galvenajām vienībām uzlabotu un saskaņotu kibernetikas līmeni visā Savienībā, galu galā radot izmaksu ietaupījumus gan uzņēmumiem, gan sabiedrībai. Šī politikas iespēja radīs noteiktu papildu administratīvo slogu un atbilstības nodrošināšanas izmaksas dalībvalstu iestādēm. Tomēr kopumā vidējā termiņā un ilgtermiņā tā arī sniegs būtiskus ieguvumus, palielinot sadarbību starp dalībvalstīm, arī operatīvā līmenī, kā arī radot stimulus, izmantojot savstarpējo palīdzību, salīdzinošās izvērtēšanas mehānismus un labāku pārskatu par galvenajiem uzņēmumiem un to mijiedarbību, kopumā palielinot kibernetikas spējas valstu un reģionālā līmenī. Vēlamā politikas iespēja arī lielā mērā nodrošinās saskaņotību ar citiem tiesību aktiem, iniciatīvām un politikas pasākumiem, tai skaitā konkrētu nozaru *lex specialis*.

Pievēršoties pašreizējai sagatavotības nepietiekamībai kibernetikas jomā dalībvalstu līmenī un uzņēmumu un citu organizāciju līmenī, var gūt efektivitātes ieguvumus un samazināt papildu izmaksas, ko rada kibernetikas incidenti.

- Attiecībā uz būtiskām un svarīgām vienībām sagatavotības līmeņa paaugstināšana kibernetikas jomā var mazināt iespējamās ieņēmumu zaudējumus, kas rodas traucējumu dēļ — tai skaitā no rūpnieciskās spiegošanas —, un var samazināt lielos izdevumus *ad hoc* draudu mazināšanai. Šādi ieguvumi, visticamāk, pārsniegs nepieciešamās ieguldījumu izmaksas. Sadrumstalotības mazināšana iekšējā tirgū arī uzlabos vienlīdzīgus konkurences apstākļus operatoriem.
- Attiecībā uz dalībvalstīm tā var vēl vairāk samazināt risku, ka pieaugs budžeta izdevumi *ad hoc* draudu mazināšanai un papildu izmaksas ar kibernetikas incidentiem saistītos ārkārtas gadījumos.
- Attiecībā uz iedzīvotājiem ir paredzams, ka pievēršanās kibernetikas incidentiem samazinās ienākumu zaudējumus, ko rada ekonomikas traucējumi.

Paaugstinātais kibernetikas līmenis visās dalībvalstīs un uzņēmumu un iestāžu spēja ātri reaģēt uz incidentu un mazināt tā ietekmi, visticamāk, palielinās iedzīvotāju vispārējo uzticēšanos digitālajai ekonomikai, un tas varētu pozitīvi ietekmēt izaugsmi un ieguldījumus.

Vispārējā kibernetikas līmeņa paaugstināšanās varētu palielināt vispārējo drošību un veicināt sabiedrībai svarīgo pamatpakalpojumu netraucētu un nepārtrauktu darbību. Šī iniciatīva varētu arī veicināt citu sociālo ietekmi, piemēram, samazināt kibernetikas terorisma līmeni un palielināt civilo aizsardzību. Paaugstinot sagatavotības līmeni kibernetikas jomā uzņēmumiem un citām organizācijām, varētu izvairīties no iespējamajiem zaudējumiem, ko rada kibernetikas uzbrukumi, tādējādi novēršot vajadzību atlaist darbiniekus.

Vispārējā kibernetikas līmeņa paaugstināšana arī var novērst vides riskus / kaitējumu videi gadījumā, ja notiek uzbrukums pamatpakalpojumam. Tas var būt īpaši svarīgi attiecībā uz

enerģētikas, ūdens piegādes un sadales vai transporta nozarēm. Nostiprinot kiberdrošības spējas, šī iniciatīva varētu palielināt tādu jaunākās paaudzes IKT infrastruktūru un pakalpojumu izmantošanu, kuri ir arī ilgtspējīgāki no vides viedokļa, un veicināt neefektīvu un mazāk drošu mantoto infrastruktūru nomaiņu. Paredzams, ka tas arī veicinās dārgi izmaksājošu kiberincidentu skaita samazināšanos, atbrīvojot resursus, kas pieejami ilgtspējīgiem ieguldījumiem.

- **Normatīvā atbilstība un vienkāršošana**

Priekšlikums paredz vispārēji izslēgt mikrovienības un mazās vienības no TID darbības jomas un piemērot vieglāku *ex post* uzraudzības režīmu lielam skaitam jaunu vienību atbilstoši pārskatītajai darbības jomai (tā dēvētās “svarīgās vienības”). Šo pasākumu mērķis ir mazināt un līdzsvarot slogu, kas uzlikts uzņēmumiem un valsts pārvaldes iestādēm. Turklāt ar priekšlikumu sarežģītā identifikācijas sistēma pamatpakalpojumu sniedzējiem tiek aizstāta ar vispārpiemērojamu pienākumu un tiek ieviests augstāks drošības un ziņošanas pienākumu saskaņošanas līmenis, tādējādi samazinot atbilstības nodrošināšanas slogu, jo īpaši vienībām, kas sniedz pārrobežu pakalpojumus.

Ar priekšlikumu tiek samazinātas atbilstības nodrošināšanas izmaksas MVU, jo vienībām ir jāveic tikai tie pasākumi, kas nepieciešami riskam atbilstoša tīklu un informācijas sistēmu drošības līmeņa nodrošināšanai.

- **Pamattiesības**

ES ir apņēmusies nodrošināt augstus standartus pamattiesību aizsardzības jomā. Visi brīvprātīgie informācijas apmaiņas pasākumi starp vienībām, ko veicina šī direktīva, tiks veikti uzticamā vidē, pilnībā ievērojot Savienības datu aizsardzības noteikumus, jo īpaši Eiropas Parlamenta un Padomes Regulu (ES) 2016/679⁸.

4. IETEKME UZ BUDŽETU

Sk. finanšu pārskatu.

5. CITI ASPEKTI

- **Īstenošanas plāni un uzraudzības, izvērtēšanas un ziņošanas kārtība**

Priekšlikums ietver vispārēju plānu, kā uzraudzīt un izvērtēt ietekmi uz konkrētajiem mērķiem, un tas paredz, ka Komisijai vismaz [54 mēnešus] pēc spēkā stāšanās datuma ir jāveic pārskatīšana un jāziņo Eiropas Parlamentam un Padomei par tās galvenajiem konstatējumiem.

Pārskatīšana ir veicama atbilstoši Komisijas labāka regulējuma pamatnostādnēm.

- **Detalizēts konkrētu priekšlikuma noteikumu skaidrojums**

Priekšlikums ir strukturēts ap septiņām galvenajām politikas jomām, kas ir savstarpēji saistītas un kalpo mērķim paaugstināt kiberdrošības līmeni Savienībā.

Priekšmets un darbības joma (1. pants un 2. pants)

⁸ Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

Direktīva, jo īpaši: a) paredz dalībvalstīm pienākumu pieņemt valsts kiberdrošības stratēģiju, izraudzīties valsts kompetentās iestādes, vienotos kontaktpunktus un CSRT; b) paredz, ka dalībvalstīm ir jānosaka kiberdrošības riska pārvaldības un ziņošanas pienākumi vienībām, kas minētas kā būtiskas vienības I pielikumā un svarīgas vienības II pielikumā; c) paredz, ka dalībvalstīm ir jānosaka pienākumi attiecībā uz kiberdrošības informācijas apmaiņu.

Tā attiecas uz konkrētām publiskām vai privātām būtiskām vienībām, kas darbojas I pielikumā uzskaitītajās nozarēs (enerģētika, transports, banku pakalpojumi, finanšu tirgus infrastruktūras, veselība, dzeramais ūdens, notekūdeņi, digitālā infrastruktūra, valsts pārvalde un kosmoss), un konkrētām svarīgām vienībām, kas darbojas II pielikumā uzskaitītajās nozarēs (pasta un kurjeru pakalpojumi, atkritumu apsaimniekošana, ķīmisko vielu izgatavošana, ražošana un izplatīšana, pārtikas ražošana, pārstrāde un izplatīšana, ražošana un digitālo pakalpojumu sniedzēji). Mikrovienības un mazās vienības Komisijas 2003. gada 6. maija Ieteikuma 2003/361/EK nozīmē ir izslēgtas no direktīvas darbības jomas, izņemot elektronisko sakaru tīklu nodrošinātājus vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējus, uzticamības pakalpojumu sniedzējus, augstākā līmeņa domēnu (ALD) nosaukumu reģistrus un valsts pārvaldi, un konkrētas citas vienības, piemēram, pakalpojuma vienīgo sniedzēju dalībvalstī.

Valstu kiberdrošības sistēmas (5.–11. pants)

Dalībvalstīm ir jāpieņem valsts kiberdrošības stratēģija, kurā nosaka stratēģiskos mērķus un atbilstīgus politikas un regulatīvus pasākumus, lai sasniegtu un uzturētu augstu kiberdrošības līmeni.

Direktīva arī nosaka satvaru koordinētai neaizsargātības atklāšanai un paredz dalībvalstīm pienākumu izraudzīties CSIRT, kas darbojas kā uzticami starpnieki un veicina mijiedarbību starp ziņotājām vienībām un IKT produktu ražotājiem un IKT pakalpojumu sniedzējiem. ENISA ir jāizstrādā un jāuztur Eiropas neaizsargātības reģistrs attiecībā uz atklāto neaizsargātību.

Dalībvalstīm ir jāievieš valsts kiberdrošības krīžu pārvaldības satvars, *inter alia* izraugoties valsts kompetentās iestādes, kas atbild par plašapmēra kiberdrošības incidentu un krīžu pārvaldību.

Dalībvalstīm ir arī jāizraugās viena vai vairākas valsts kompetentās iestādes kiberdrošības jomā uzraudzības uzdevumu veikšanai saskaņā ar šo direktīvu un valsts vienotais kontaktpunkts kiberdrošības jautājumos (SPOC), kas koordinē sadarbību, lai nodrošinātu dalībvalstu iestāžu pārrobežu sadarbību. Dalībvalstīm ir arī jāizraugās CSIRT.

Sadarbība (12.–16. pants)

Ar direktīvu tiek izveidota sadarbības grupa, lai atbalstītu un sekmētu stratēģisko sadarbību un informācijas apmaiņu starp dalībvalstīm un attīstītu uzticēšanos un palāvību starp tām. Ar to arī tiek izveidots CSIRT tīkls, lai palīdzētu attīstīt palāvību un uzticēšanos starp dalībvalstīm un veicinātu ātru un efektīvu operatīvo sadarbību.

Tiek izveidots Eiropas Kiberkrīžu sadarbības organizāciju tīkls (EU-CyCLONe), lai atbalstītu plašapmēra kiberdrošības incidentu un krīžu koordinētu pārvaldību un nodrošinātu regulāru informācijas apmaiņu starp dalībvalstīm un ES iestādēm.

ENISA sadarbībā ar Komisiju ir jāizdod divgadu ziņojums par stāvokli kibernetiskās drošības jomā Savienībā.

Komisijai ir jāievieš salīdzinošās izvērtēšanas sistēma, kas ļauj regulāri veikt salīdzinošu izvērtējumu par dalībvalstu kibernetiskās drošības politikas efektivitāti.

Kibernetiskās drošības riska pārvaldības un ziņošanas pienākumi (17.–23. pants)

Direktīva nosaka dalībvalstīm pienākumu nodrošināt, ka visu darbības jomā ietilpstošo vienību pārvaldības struktūras apstiprina kibernetiskās drošības riska pārvaldības pasākumus, ko pieņēmušas attiecīgās vienības, un nodrošina ar kibernetiskās drošības saistīto apmācību.

Dalībvalstīm jānodrošina, lai darbības jomā ietilpstošās vienības veiktu atbilstīgus un samērīgus tehniskos un organizatoriskos pasākumus tādu kibernetiskās drošības risku pārvaldībai, kuri skar tīklu un informācijas sistēmu drošību. Tām ir arī jānodrošina, ka vienības paziņo valsts kompetentajām iestādēm vai CSIRT par visiem kibernetiskās drošības incidentiem, kas būtiski ietekmē to pakalpojumu sniegšanu.

ALD reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, savāc un uztur precīzus un pilnīgus domēnu nosaukumu reģistrācijas datus. Turklāt šādām vienībām ir jānodrošina legītimiem piekļuves prasītājiem efektīva piekļuve domēnu reģistrācijas datiem.

Jurisdikcija un reģistrācija (24. un 25. pants)

Parasti uzskata, ka būtiskās un svarīgās vienības ir tās dalībvalsts jurisdikcijā, kurā tās sniedz pakalpojumus. Tomēr konkrētu veidu vienības (DNS pakalpojumu sniedzējus, ALD nosaukumu reģistrus, mākoņpakalpojumu sniedzējus, datu centru pakalpojumu sniedzējus un satura piegādes tīklu nodrošinātājus, kā arī konkrētus digitālo pakalpojumu sniedzējus) uzskata par tādām, kas ir tās dalībvalsts jurisdikcijā, kurā atrodas to galvenā darbības vieta Savienībā. Tas vajadzīgs tāpēc, lai nodrošinātu, ka šādām vienībām nav jāizpilda vairākas atšķirīgas juridiskās prasības, jo tās īpaši daudz sniedz pārrobežu pakalpojumus. ENISA ir jāizveido un jāuztur pēdējā minētā veida vienību reģistrs.

Informācijas apmaiņa (26. un 27. pants)

Dalībvalstis paredz noteikumus, kas ļauj vienībām iesaistīties ar kibernetiskās drošības saistītās informācijas apmaiņā īpašu kibernetiskās drošības informācijas apmaiņas pasākumu ietvaros, ievērojot LESD 101. pantu. Turklāt dalībvalstis ļauj šīs direktīvas darbības jomā neietilpstošajām vienībām brīvprātīgi ziņot par nozīmīgiem incidentiem, kibernetiskajiem draudiem vai gandrīz notikušiem notikumiem.

Uzraudzība un izpilde (28.–34. pants)

Kompetentajām iestādēm ir jāuzrauga šīs direktīvas darbības jomā ietilpstošās vienības un jo īpaši jānodrošina, ka tās ievēro drošības un incidentu paziņošanas prasības. Tiek nošķirts *ex ante* uzraudzības režīms būtiskām vienībām un *ex post* uzraudzības režīms svarīgām vienībām; pēdējais minētais režīms nosaka, ka kompetentajām iestādēm ir jārīkojas, ja tām tiek iesniegti pierādījumi vai norādes, ka svarīga vienība neievēro drošības un incidentu paziņošanas prasības.

Direktīva arī nosaka, ka dalībvalstīm ir jāpiemēro administratīvi naudas sodi būtiskām un svarīgām vienībām, un paredz noteiktus sodu maksimālos apmērus.

Dalībvalstīm ir jāsadarbojas un pēc vajadzības jāpalīdz citām dalībvalstīm, ja vienības sniedz pakalpojumus vairāk nekā vienā dalībvalstī vai ja vienības galvenā darbības vieta vai tās pārstāvis atrodas konkrētā dalībvalstī, bet tās tīklu un informācijas sistēmas atrodas vienā vai vairākās citās dalībvalstīs.

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA,

ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu⁹,

ņemot vērā Reģionu komitejas atzinumu¹⁰,

saskaņā ar parasto likumdošanas procedūru,

tā kā:

- (1) Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/1148¹¹ mērķis bija veidot kiberdrošības spējas Savienībā, mazinot draudus tīklu un informācijas sistēmām, ko izmanto pamatpakalpojumu sniegšanai galvenajās nozarēs, un nodrošinot šādu pakalpojumu nepārtrauktību, kad notiek kiberdrošības incidenti, tādējādi sniedzot ieguldījumu Savienības ekonomikas un sabiedrības efektīvā darbībā.
- (2) Kopš Direktīvas (ES) 2016/1148 stāšanās spēkā ir panākts ievērojams progress Savienības kiberdrošības noturības līmeņa paaugstināšanā. Minētās direktīvas pārskatīšana apliecināja, ka direktīva ir bijusi kā katalizators institucionālajai un regulatīvajai pieejai attiecībā uz kiberdrošību Savienībā, bruģējot ceļu būtiskām pārmaiņām domāšanas veidā. Direktīva ir nodrošinājusi valstu regulējumu pabeigšanu, nosakot valsts kiberdrošības stratēģijas, veidojot valstu spējas un īstenojot regulatīvus pasākumus, kas aptver būtiskas infrastruktūras un dalībniekus, kurus noteikusi katra dalībvalsts. Tā ir arī veicinājusi sadarbību Savienības līmenī, izveidojot sadarbības grupu¹² un valstu datordrošības incidentu reaģēšanas vienību tīklu ("CSIRT tīkls")¹³. Neraugoties uz šiem sasniegumiem, Direktīvas (ES) 2016/1148 pārskatīšanā ir konstatētas nepilnības, kas liedz tai efektīvi risināt pašreizējās un jaunās kiberdrošības problēmas.

⁹ OV C (.), (.), (.), lpp.

¹⁰ OV C (.), (.), (.), lpp.

¹¹ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194/1, 19.7.2016., 1. lpp.).

¹² Direktīvas (ES) 2016/1148 11. pants.

¹³ Direktīvas (ES) 2016/1148 12. pants.

- (3) Tīklu un informācijas sistēmas ir kļuvušas par būtisku ikdienas dzīves iezīmi, ko raksturo ātra digitālā pārveide un sabiedrības savstarpējā savienotība, tai skaitā pārrobežu apmaiņa. Šīs attīstības rezultātā ir paplašinājusies kiberdraudu aina, radot jaunas problēmas, attiecībā uz kurām ir vajadzīgi pielāgoti, koordinēti un inovatīvi reaģēšanas pasākumi visās dalībvalstīs. Kiberdrošības incidentu skaits, apmērs, sarežģītība, biežums un ietekme pieaug un rada būtiskus draudus tīklu un informācijas sistēmu darbībai. Rezultātā kiberincidenti var kavēt saimniecisko darbību īstenošanu iekšējā tirgū, radīt finansiālus zaudējumus, apdraudēt lietotāju uzticēšanos un radīt lielu kaitējumu Savienības ekonomikai un sabiedrībai. Tāpēc sagatavotība kiberdrošības jomā un efektivitāte tagad iekšējā tirgus pienācīgai darbībai ir vēl svarīgākas nekā jebkad iepriekš.
- (4) Direktīvas (ES) 1148/2016 juridiskais pamats bija Līguma par Eiropas Savienības darbību (LESD) 114. pants, kura mērķis ir iekšējā tirgus izveide un darbība, uzlabojot pasākumus valstu regulējumu tuvināšanai. Kiberdrošības prasības, kas noteiktas vienībām, kuras sniedz pakalpojumus vai veic ekonomiski svarīgas darbības, ievērojami atšķiras starp dalībvalstīm prasību veida, to detalizācijas līmeņa un uzraudzības metodes ziņā. Minētās atšķirības rada papildu izmaksas un grūtības uzņēmumiem, kas piedāvā pārrobežu preces vai pakalpojumus. Prasības, ko nosaka viena dalībvalsts un kas atšķiras no citas dalībvalsts noteiktajām prasībām vai pat ir pretrunā tām, var būtiski ietekmēt minētās pārrobežu darbības. Turklāt iespējamība, ka kiberdrošības standartu struktūra vai īstenošana var nebūt optimāla vienā dalībvalstī, visticamāk, ietekmēs pārējo dalībvalstu kiberdrošības līmeni, jo īpaši ņemot vērā intensīvo pārrobežu apmaiņu. Direktīvas (ES) 2016/1148 pārskatīšanā ir atklājies, ka tās īstenošana dalībvalstīs ievērojami atšķiras, arī attiecībā uz tās darbības jomu, kuras precīza noteikšana lielā mērā tika atstāta dalībvalstu ziņā. Direktīva (ES) 2016/1148 arī sniedza dalībvalstīm ļoti plašu rīcības brīvību attiecībā uz tajā noteikto drošības un incidentu paziņošanas prasību īstenošanu. Tāpēc minētie pienākumi dalībvalstu līmenī tika īstenoti ļoti atšķirīgi. Līdzīgas īstenošanas atšķirības bija vērojamas attiecībā uz direktīvas noteikumiem par uzraudzību un izpildi.
- (5) Visas šīs atšķirības sadrumstalo iekšējo tirgu un tām var būt prejudiciāla ietekme uz tā darbību, jo īpaši ietekmējot pakalpojumu pārrobežu sniegšanu un kiberdrošības noturības līmeni, jo tiek piemēroti atšķirīgi standarti. Šīs direktīvas mērķis ir novērst šādas plašas atšķirības starp dalībvalstīm, jo īpaši izklāstot minimālos noteikumus attiecībā uz koordinēta tiesiskā regulējuma darbību, nosakot mehānismus efektīvai atbildīgo iestāžu sadarbībai katrā dalībvalstī, atjauninot to nozaru un darbību sarakstu, uz kurām attiecas kiberdrošības pienākumi, un paredzot efektīvus tiesiskās aizsardzības līdzekļus un sankcijas, kas ir svarīgas, lai šie pienākumi tiktu efektīvi izpildīti. Tāpēc Direktīva (ES) 2016/1148 būtu jāatceļ un jāaizstāj ar šo direktīvu.
- (6) Šī direktīva neietekmē dalībvalstu spēju veikt nepieciešamos pasākumus, lai nodrošinātu savu būtisko drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrisko drošību un lai ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem atbilstoši Savienības tiesību aktiem. Saskaņā ar LESD 346. pantu dalībvalstīm nav jāsniedz informācija, kuras izpaušana būtu pretrunā to būtiskajām sabiedriskās drošības interesēm. Šajā kontekstā svarīgi ir valstu un Savienības noteikumi par klasificētas informācijas aizsardzību, vienošanās par neizpaušanu un

neformālas vienošanās par informācijas neizpaušanu, piemēram, Gaismas signālu protokols¹⁴.

- (7) Līdz ar Direktīvas (ES) 2016/1148 atcelšanu būtu jāpaplašina piemērošanas joma pa nozarēm, aptverot lielāku ekonomikas daļu, ņemot vērā 4.–6. apsvērumā izklāstītos apsvērumus. Tāpēc to nozaru skaits, uz kurām attiecas Direktīva (ES) 2016/1148, būtu jāpalielina, lai nodrošinātu to nozaru un pakalpojumu pilnīgu aptvērumu, kuri ir ļoti svarīgi galvenajām sociālajām un saimnieciskajām darbībām iekšējā tirgū. Noteikumi nedrīkstētu atšķirties atkarībā no tā, vai vienības ir pamatpakalpojumu sniedzēji vai digitālo pakalpojumu sniedzēji. Ir pierādīts, ka šāda diferencēšana ir novecojusi, jo tā neatspoguļo nozaru vai pakalpojumu faktisko nozīmīgumu sociālajām un saimnieciskajām darbībām iekšējā tirgū.
- (8) Saskaņā ar Direktīvu (ES) 2016/1148 dalībvalstīm bija pienākums noteikt, kuras vienības atbilst kritērijiem, lai tās uzskatītu par pamatpakalpojumu sniedzējiem (“identifikācijas process”). Lai šajā ziņā mazinātu lielās atšķirības starp dalībvalstīm un nodrošinātu juridisko noteiktību attiecībā uz riska pārvaldības prasībām un ziņošanas pienākumiem visām attiecīgajām vienībām, būtu jāievieš vienots kritērijs to vienību noteikšanai, kuras ir šīs direktīvas piemērošanas jomā. Minētajam kritērijam vajadzētu būt maksimālā lieluma noteikumam, saskaņā ar kuru visi vidējie un lielie uzņēmumi, kas definēti Komisijas Ieteikumā 2003/361/EK¹⁵ un darbojas nozarēs vai sniedz pakalpojumus, uz kuriem attiecas šī direktīva, ir tās piemērošanas jomā. Dalībvalstīm nebūtu jānosaka prasība izveidot to vienību sarakstu, kuras atbilst šim vispārpiemērojamam ar lielumu saistītajam kritērijam.
- (9) Tomēr šī direktīva būtu jāattiecina arī uz mazām vienībām vai mikrovienībām, kas atbilst noteiktiem kritērijiem, kuri norāda uz būtisku lomu dalībvalstu tautsaimniecībā vai sabiedrībā vai konkrētās nozarēs vai pakalpojumu veidos. Dalībvalstīm vajadzētu būt atbildīgām par šādu vienību saraksta izveidi un būtu jāiesniedz saraksts Komisijai.
- (10) Komisija kopā ar sadarbības grupu var izdot pamatnostādnes par mikrouzņēmumiem un mazajiem uzņēmumiem piemērojamo kritēriju īstenošanu.
- (11) Atkarībā no nozares, kurā tie darbojas, vai to sniegto pakalpojumu veida vienības, kuras ir šīs direktīvas darbības jomā, būtu jāiedala divās kategorijās — būtiskas vienības un svarīgas vienības. Veicot to iedalīšanu kategorijās, būtu jāņem vērā nozares vai sniegto pakalpojumu veida svarīgums, kā arī atkarība no citām nozarēm vai pakalpojumu veidiem. Uz būtiskajām un svarīgajām vienībām būtu jāattiecina vienādas riska pārvaldības prasības un ziņošanas pienākumi. Uzraudzības un sodu režīmi starp šīm abām vienību kategorijām būtu jādiferencē, lai nodrošinātu taisnīgu līdzsvaru starp prasībām un pienākumiem, no vienas puses, un administratīvo slogu, kas izriet no atbilstības uzraudzības, no otras puses.
- (12) Īpaši nozaru tiesību akti un instrumenti var palīdzēt nodrošināt augstu kiberdrošības līmeni, vienlaikus pilnībā ņemot vērā šo nozaru specifiku un sarežģītību. Ja saskaņā ar konkrētas nozares Savienības tiesību aktu būtiskajām vai svarīgajām vienībām ir jāpieņem kiberdrošības riska pārvaldības pasākumi vai jāpaziņo incidenti vai nozīmīgi kiberdraudi, kam ir vismaz līdzvērtīga ietekme uz šajā direktīvā noteiktajiem

¹⁴ Gaismas signālu protokols (GSP) ir līdzeklis, ko izmanto informācijas apmaiņā, lai informētu mērķauditoriju par ierobežojumiem šīs informācijas turpmākā izplatīšanā. To izmanto gandrīz visās CSIRT kopienās un dažos informācijas apmaiņas un analīzes centros (ISAC).

¹⁵ Komisijas Ieteikums 2003/361/EK (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

pieņēmumiem, būtu jāpieņem minētie īpašie nozaru noteikumi, tai skaitā par uzraudzību un izpildi. Komisija var izdot pamatnostādnes par *lex specialis* īstenošanu. Šī direktīva neliedz pieņemt konkrētu nozaru Savienības papildu aktus, kuros pievēršas kibernetikas riska pārvaldības pasākumiem un incidentu paziņojumiem. Šī direktīva neskar esošās īstenošanas pilnvaras, kas piešķirtas Komisijai vairākās nozarēs, tai skaitā transporta un enerģētikas nozarē.

- (13) Eiropas Parlamenta un Padomes Regula XXXX/XXXX¹⁶ būtu jāuzskata par konkrētas nozares Savienības tiesību aktu saistībā ar šo direktīvu attiecībā uz finanšu sektora vienībām. Regulas XXXX/XXXX noteikumi par informācijas un komunikācijas tehnoloģiju (IKT) riska pārvaldības pasākumiem, ar IKT saistītu incidentu pārvaldību un jo īpaši incidentu paziņošanu, kā arī par digitālās darbības noturības testēšanu, informācijas apmaiņas pasākumiem un IKT trešo personu risku būtu jāpieņem to noteikumu vietā, kuri paredzēti saskaņā ar šo direktīvu. Tāpēc dalībvalstīm šīs direktīvas noteikumi par kibernetikas riska pārvaldību un ziņošanas pienākumiem, informācijas apmaiņu, kā arī uzraudzību un izpildi nebūtu jāpieņem finanšu vienībām, uz kurām attiecas Regula XXXX/XXXX. Vienaļpus ir svarīgi uzturēt ciešas attiecības un informācijas apmaiņu ar finanšu sektoru saskaņā ar šo direktīvu. Šajā nolūkā Regula XXXX/XXXX ļauj visām finanšu uzraudzības iestādēm, Eiropas uzraudzības iestādēm (EUI) attiecībā uz finanšu sektoru un valsts kompetentajām iestādēm atbilstoši Regulai XXXX/XXXX piedalīties sadarbības grupas stratēģiskajās politikas apspriedēs un tehniskajā darbā un apmainīties ar informāciju un sadarboties ar vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar šo direktīvu, un valstu CSIRT. Kompetentajām iestādēm atbilstoši Regulai XXXX/XXXX būtu jānosūta ziņas par būtiskiem ar IKT saistītiem incidentiem arī vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar šo direktīvu. Turklāt dalībvalstīm arī turpmāk būtu jāiekļauj finanšu sektors savās kibernetikas stratēģijās, un valstu CSIRT finanšu sektoru var ietvert savās darbībās.
- (14) Ņemot vērā saikni starp kibernetiku un vienību fizisko drošību, Eiropas Parlamenta un Padomes Direktīvā (ES) XXX/XXX¹⁷ un šajā direktīvā būtu jānodrošina saskaņota pieeja. Lai to panāktu, dalībvalstīm būtu jānodrošina, ka kritiskās vienības un tām līdzvērtīgas vienības atbilstoši Direktīvai (ES) XXX/XXX tiek uzskatītas par būtiskām vienībām atbilstoši šai direktīvai. Dalībvalstīm būtu arī jānodrošina, ka to kibernetikas stratēģijās ir paredzēts politikas satvars uzlabotai koordinācijai starp kompetento iestādi atbilstoši šai direktīvai un kompetento iestādi atbilstoši Direktīvai (ES) XXX/XXX saistībā ar informācijas apmaiņu par incidentiem un kibernetikas draudiem un uzraudzības uzdevumu īstenošanu. Iestādēm būtu jāsadarbjas un jāapmainās ar informāciju atbilstoši abām direktīvām, jo īpaši saistībā ar kritisko vienību noteikšanu, kibernetikas draudiem, kibernetikas riskiem, incidentiem, kas ietekmē kritiskās vienības, kā arī kibernetikas pasākumiem, ko veikušas kritiskās vienības. Ja to pieprasa kompetentās iestādes atbilstoši Direktīvai (ES) XXX/XXX, kompetentajām iestādēm atbilstoši šai direktīvai vajadzētu būt iespējām īstenot savas uzraudzības un izpildes pilnvaras attiecībā uz būtisku vienību, kas identificēta kā kritiska. Abu veidu iestādēm šajā nolūkā būtu jāsadarbjas un jāapmainās ar informāciju.
- (15) Uzticamas, noturīgas un drošas domēnu nosaukumu sistēmas (DNS) veicināšana un saglabāšana ir svarīgs faktors interneta integritātes uzturēšanā un ir svarīga tā

¹⁶ [ieraksta pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

¹⁷ [ieraksta pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

nepārtrauktai un stabilai darbībai, no kuras ir atkarīga digitālā ekonomika un sabiedrība. Tāpēc šī direktīva būtu jāpiemēro visiem DNS pakalpojumu sniedzējiem visā DNS atrisināšanas ķēdē, arī saknes serveru, augstākā līmeņa domēnu (ALD) nosaukumu serveru operatoriem, autoritatīvo nosaukumu serveru operatoriem attiecībā uz domēnu nosaukumiem, kā arī rekursīvajiem atrisinātājiem.

- (16) Mākoņpakalpojumos būtu jāiekļauj pakalpojumi, kas ļauj pēc pieprasījuma plaši un attālināti piekļūt kopīgojamu un sadalītu datu resursu mērogojamam un elastīgam pūlam. Minētie datu resursi ietver tādus resursus kā tīkli, serveri vai cita infrastruktūra, operētājsistēmas, programmatūra, glabāšana, lietošanas un pakalpojumi. Mākoņdatu izvietojuma modeļos būtu jāiekļauj privāts, kopienas, publisks un hibrīds mākonis. Iepriekš minēto pakalpojumu un izvietojuma modeļu nozīme ir tāda pati kā terminiem “pakalpojums” un “izvietojuma modeļi” standartā ISO/IEC 17788:2014. Mākoņdatu lietotāja spēju vienpusēji sev nodrošināt datu resursus, piemēram, servera laiku vai tīkla glabāšanu, bez cilvēcisks mijiedarbības ar mākoņpakalpojumu sniedzēju varētu raksturot kā pārvaldību pēc pieprasījuma. Termins “plaša un attālināta piekļuve” ir izmantots, lai raksturotu to, ka mākoņdatu resursus tiek nodrošinātas visā tīklā un tām piekļūst, izmantojot mehānismus, kas veicina neviendabīgu plāno vai biezo klientiem paredzēto platformu (tai skaitā mobilo tālruni, planšetdatoru, klēpj datoru, darbstaciju) izmantošanu. Termins “mērogojams” attiecas uz datu resursiem, kurus mākoņpakalpojuma sniedzējs elastīgi piešķir neatkarīgi no resursu ģeogrāfiskās atrašanās vietas, lai risinātu pieprasījuma svārstības. Termins “elastīgs pūls” ir izmantots, lai aprakstītu tos datu resursus, kuri tiek nodrošināti un atbrīvoti saskaņā ar pieprasījumu, lai pieejamos resursus ātri palielinātu un samazinātu atkarībā no noslodzes. Termins “kopīgojams” ir izmantots, lai aprakstītu tos datu resursus, kas tiek sniegti daudziem lietotājiem, kuriem ir kopīga piekļuve pakalpojumam, bet apstrāde notiek katram lietotājam atsevišķi, kaut arī pakalpojums tiek sniegts no vienas un tās pašas elektroniskās iekārtas. Termins “sadalīts” ir izmantots, lai aprakstītu tos datu resursus, kas atrodas dažādos tīklotos datoros vai ierīcēs un kas īsteno savstarpēju saziņu un koordināciju, izmantojot ziņojumu sūtīšanu.
- (17) Ņemot vērā inovatīvu tehnoloģiju parādīšanos un jaunus darbības modeļus, paredzams, ka, reaģējot uz jaunām klientu vajadzībām, tirgū parādīsies jauni mākoņdatu izvietojuma un pakalpojuma modeļi. Šajā kontekstā mākoņpakalpojumus var sniegt īpaši sadalītā formā, pat tuvāk vietai, kur dati tiek ģenerēti vai savākti, tādējādi pārejot no tradicionālā modeļa uz īpaši sadalītu modeli (“perifērdatošana”).
- (18) Pakalpojumus, ko piedāvā datu centru pakalpojumu sniedzēji, ne vienmēr var sniegt mākoņpakalpojuma veidā. Tas nozīmē, ka datu centri var nebūt daļa no mākoņdatu infrastruktūras. Lai pārvaldītu visus riskus tīklu un informācijas sistēmu drošībai, šī direktīva būtu jāattiecinā arī uz tādu datu centru pakalpojumu sniedzējiem, kuri nav mākoņpakalpojumi. Šajā direktīvā termins “datu centra pakalpojums” būtu jāattiecinā uz tāda pakalpojuma sniegšanu, kas ietver struktūras vai struktūru grupas, kuras paredzētas tāda informācijas tehnoloģijas un tīkla aprīkojuma centralizētai izmitināšanai, savstarpējai savienošanai un darbībai, kas sniedz datu uzglabāšanu, apstrādes un transportēšanas pakalpojumus kopā ar visām ierīcēm un infrastruktūrām jaudas sadalei un vides kontrolei. Termins “datu centra pakalpojums” neattiecas uz iekšējiem, korporatīviem datu centriem, ko tur īpašumā un ekspluatē attiecīgās vienības vajadzībām.

- (19) Pasta pakalpojumu sniedzēji Eiropas Parlamenta un Padomes Direktīvas 97/67/EK¹⁸ nozīmē, kā arī eksprespiegādes un kurjeru piegādes pakalpojumu sniedzēji būtu jāiekļauj šīs direktīvas darbības jomā, ja tie nodrošina vismaz vienu no posmiem pasta piegādes ķēdē un jo īpaši sniedz atmuitošanas, šķirošanas vai sadales pakalpojumus, arī savākšanas pakalpojumus. Transporta pakalpojumi, kurus neveic saistībā ar kādu no minētajiem posmiem, būtu jāizslēdz no pasta pakalpojumu jomas.
- (20) Šī pieaugošā savstarpējā atkarība ir rezultāts tam, ka pakalpojumu sniegšanas tīklam arvien biežāk ir pārrobežu raksturs un tas arvien vairāk ir savstarpēji atkarīgs, izmantojot pamatinfrastruktūras visā Savienībā tādās nozarēs kā enerģētika, transports, digitālā infrastruktūra, dzeramais ūdens un notekūdeņi, veselība, konkrēti valsts pārvaldes aspekti, kā arī kosmoss, ciktāl tas attiecas uz tādu konkrētu pakalpojumu sniegšanu, kuri ir atkarīgi no virszemes infrastruktūrām, ko tur īpašumā, pārvalda vai ekspluatē dalībvalstis vai attiecīgās privātpersonas, tādējādi neaptverot infrastruktūras, ko tur īpašumā, pārvalda vai ekspluatē Savienība vai tās vārdā kā daļu no tās kosmosa programmām. Šī savstarpējā atkarība nozīmē, ka jebkuram traucējumam, pat tādām, kas sākotnēji ierobežots līdz vienai vienībai vai vienai nozarei, var būt plašāka lavīnveida ietekme, iespējams, rezultātā izraisot tālejošas un ilgstošas negatīvas sekas pakalpojumu sniegšanā iekšējā tirgū. Covid-19 pandēmija ir parādījusi mūsu arvien vairāk savstarpēji atkarīgās sabiedrības neaizsargātību, neraugoties uz zemas varbūtības riskiem.
- (21) Ņemot vērā atšķirības valstu pārvaldes struktūrās un lai garantētu jau esošo nozaru noteikumu izpildi vai aizsargātu Savienības uzraudzības un regulatīvās struktūras, dalībvalstīm būtu jāspēj izraudzīties vairāk nekā vienu valsts kompetento iestādi, kas ir atbildīga par to, lai saskaņā ar šo direktīvu pildītu uzdevumus saistībā ar būtisko un svarīgo vienību tīklu un informācijas sistēmu drošību. Dalībvalstīm būtu jāspēj uzticēt šo funkciju esošai iestādei.
- (22) Lai veicinātu pārrobežu sadarbību un saziņu starp iestādēm un lai varētu efektīvi īstenot šo direktīvu, katrai dalībvalstij būtu jāizraugās valsts vienotais kontaktpunkts, kas atbild par to jautājumu koordināciju, kuri saistīti ar tīklu un informācijas sistēmu drošību un pārrobežu sadarbību Savienības līmenī.
- (23) Kompetentajām iestādēm vai *CSIRT* būtu efektīvi un lietpratīgi jāsaņem paziņojumi par incidentiem no vienībām. Būtu jānosaka vienotajiem kontaktpunktiem pienākums pārsūtīt incidentu paziņojumus citu skarto dalībvalstu vienotajiem kontaktpunktiem. Dalībvalstu iestāžu līmenī, lai nodrošinātu vienu vienotu kontaktpunktu katrā dalībvalstī, vienotajiem kontaktpunktiem arī būtu jāsaņem attiecīgā informācija par incidentiem saistībā ar finanšu sektora vienībām no kompetentajām iestādēm atbilstoši Regulai XXXX/XXXX, un tiem būtu jāspēj šo informāciju attiecīgā gadījumā pārsūtīt attiecīgajām valsts kompetentajām iestādēm vai *CSIRT* saskaņā ar šo regulu.
- (24) Visās dalībvalstīs vajadzētu būt atbilstīgam aprīkojumam gan tehnisko, gan organizatorisko spēju ziņā, lai novērstu un atklātu tīklu un informācijas sistēmu incidentus un riskus, reaģētu uz tiem un tos mazinātu. Tāpēc dalībvalstīm būtu jānodrošina, ka tajās ir labi funkcionējošas, pamatprasībām atbilstīgas *CSIRT*, kas tiek dēvētas arī par datorapdraudējumu reaģēšanas vienībām (*CERT*), lai nodrošinātu efektīvas un saderīgas spējas incidentu risināšanai un risku novēršanai un efektīvas

¹⁸ Eiropas Parlamenta un Padomes Direktīva 97/67/EK (1997. gada 15. decembris) par kopīgiem noteikumiem Kopienas pasta pakalpojumu iekšējā tirgus attīstībai un pakalpojumu kvalitātes uzlabošanai (OV L 15, 21.1.1998., 14. lpp.).

sadarbības nodrošināšanai Savienības līmenī. Lai uzlabotu uzticības pilnas attiecības starp vienībām un *CSIRT*, gadījumos, kad *CSIRT* ir kompetentās iestādes daļa, dalībvalstīm būtu jāapsver funkcionāls nošķirums starp *CSIRT* veiktajiem operatīvajiem uzdevumiem, jo īpaši attiecībā uz informācijas apmaiņu un atbalstu vienībām, un kompetento iestāžu uzraudzības darbībām.

- (25) Attiecībā uz persondatiem *CSIRT* saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679¹⁹, ja to pieprasa vienības atbilstoši šai direktīvai un to vārdā, būtu jāspēj nodrošināt to pakalpojumu sniegšanai izmantoto tīklu un informācijas sistēmu proaktīvu skenēšanu. Dalībvalstīm būtu jāizvirza mērķis nodrošināt vienlīdzīgu tehnisko spēju līmeni visām nozaru *CSIRT*. Dalībvalstis var lūgt Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) palīdzību valsts *CSIRT* attīstīšanā.
- (26) Ņemot vērā to, cik svarīga ir starptautiskā sadarbība kiberdrošības jomā, *CSIRT* būtu jāspēj piedalīties starptautiskos sadarbības tīklos papildus *CSIRT* tīklam, ko izveido ar šo direktīvu.
- (27) Saskaņā ar pielikumu Komisijas Ieteikumam (ES) 2017/1548 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (“Plāns”)²⁰ plašapmēra incidents būtu jāsaprot kā incidents, kuram ir nozīmīga ietekme uz vismaz divām dalībvalstīm vai kura radītie traucējumi pārsniedz dalībvalsts spēju uz tiem reaģēt. Atkarībā no to cēloņa un ietekmes plašapmēra incidenti var izvērsties par visaptverošām krīzēm, kas padara neiespējamu iekšējā tirgus pienācīgu darbību. Ņemot vērā šādu incidentu plašo tvērumu un to, ka vairākumā gadījumu tiem ir pārrobežu raksturs, dalībvalstīm un attiecīgajām Savienības iestādēm, struktūrām un aģentūrām būtu jāsadarbojas tehniskā, operatīvā un politiskā līmenī, lai pienācīgi koordinētu reaģēšanu visā Savienībā.
- (28) Tā kā tīklu un informācijas sistēmu neaizsargātības ļaunprātīga izmantošana var izraisīt būtiskus traucējumus un kaitējumu, kiberdrošības riska mazināšanā svarīgs faktors ir šādas neaizsargātības ātra apzināšana un novēršana. Tāpēc vienībām, kas attīsta šādas sistēmas, būtu jāievieš atbilstīgas procedūras rīcībai gadījumos, kad tiek atklāta neaizsargātība. Tā kā neaizsargātību bieži konstatē un paziņo (atklāj) trešās personas (ziņotājas vienības), IKT produktu ražotājam vai pakalpojumu sniedzējam būtu arī jāievieš nepieciešamās procedūras informācijas par neaizsargātību saņemšanai no trešām personām. Šajā saistībā starptautiskie standarti ISO/IEC 30111 un ISO/IEC 29417 sniedz norādījumus attiecīgi par rīcību neaizsargātības gadījumā un neaizsargātības atklāšanu. Attiecībā uz neaizsargātības atklāšanu īpaši svarīga ir koordinācija starp ziņotājām vienībām un IKT produktu ražotājiem vai pakalpojumu sniedzējiem. Koordinēta neaizsargātības atklāšana ir strukturēts process, kurā par neaizsargātību tiek ziņots organizācijām tādā veidā, lai organizācija varētu diagnosticēt un novērst neaizsargātību, pirms sīkāka informācija par to tiek darīta zināma trešām personām vai sabiedrībai. Koordinētā neaizsargātības atklāšanā būtu arī jāietver koordinācija starp ziņotāju vienību un organizāciju attiecībā uz neaizsargātības izlabošanas un publiskošanas termiņu.

¹⁹ Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

²⁰ Komisijas Ieteikums (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (OV L 239, 19.9.2017., 36. lpp.).

- (29) Tāpēc dalībvalstīm būtu jāveic pasākumi, lai veicinātu koordinētu neaizsargātības atklāšanu, ieviešot atbilstošu valsts politiku. Šajā saistībā dalībvalstīm būtu jāizraugās *CSIRT*, lai tā uzņemtos “koordinatora” lomu, nepieciešamības gadījumā darbodamās kā starpnieks starp ziņotājām vienībām un IKT produktu ražotājiem vai pakalpojumu sniedzējiem. *CSIRT* koordinatora pienākumos būtu jo īpaši jāiekļauj attiecīgo vienību apzināšana un saziņa ar tām, ziņotāju vienību atbalstīšana, atklāšanas termiņu apspriešana un vairākas organizācijas ietekmējošas neaizsargātības pārvaldība (vairāku pušu neaizsargātības atklāšana). Ja neaizsargātība ietekmē vairākus IKT produktu ražotājus vai pakalpojumu sniedzējus, kas veic darījumdarbību vairāk nekā vienā dalībvalstī, izraudzītajām *CSIRT* no katras skartās dalībvalsts būtu jāsadarbojas ar *CSIRT* tīklu.
- (30) Piekļuve pareizai un savlaicīgai informācijai par neaizsargātību, kas skar IKT produktus un pakalpojumus, veicina kiberdrošības riska pārvaldības uzlabošanu. Šajā ziņā publiski pieejamas informācijas par neaizsargātību avoti ir svarīgs rīks vienībām un to lietotājiem, kā arī valsts kompetentajām iestādēm un *CSIRT*. Šā iemesla dēļ *ENISA* būtu jāizveido brīvprātīgs neaizsargātības reģistrs, kurā būtiskas un svarīgas vienības un to piegādātāji, kā arī vienības, uz kurām neattiecas šīs direktīvas piemērošanas joma, var atklāt neaizsargātību un sniegt neaizsargātības informāciju, kas ļauj lietotājiem veikt atbilstīgus riska mazināšanas pasākumus.
- (31) Lai gan līdzīgi neaizsargātības reģistri vai datubāzes jau pastāv, to mitinātāji un uzturētāji ir vienības, kuru darījumdarbības vieta nav Savienībā. Eiropas neaizsargātības reģistrs, ko uztur *ENISA*, nodrošinātu uzlabotu pārredzamību attiecībā uz publiskošanas procesu, pirms neaizsargātība tiek oficiāli atklāta, un noturību gadījumos, kad notiek traucējumi vai pārtraukumi līdzīgu pakalpojumu sniegšanā. Lai, ciktāl iespējams, izvairītos no centienu dublēšanās un nodrošinātu papildināmību, *ENISA* būtu jāizvērtē iespēja noslēgt strukturētus sadarbības nolīgumus ar līdzīgiem reģistriem trešo valstu jurisdikcijās.
- (32) Sadarbības grupai būtu reizi divos gados jāizstrādā darba programma, kurā iekļauj darbības, kas grupai jāveic, lai īstenotu tās mērķus un uzdevumus. Saskaņā ar šo direktīvu pieņemtās pirmās programmas termiņš būtu jāpielāgo saskaņā ar Direktīvu (ES) 2016/1148 pieņemtās pēdējās programmas termiņam, lai izvairītos no iespējamajiem traucējumiem grupas darbā.
- (33) Izstrādājot norādījumu dokumentus, sadarbības grupai būtu konsekventi jāapzina valsts risinājumi un pieredze, jānovērtē sadarbības grupas nodevumu ietekme uz valstu pieejām, jāapspriež īstenošanas problēmas un jāformulē īpaši ieteikumi, kas jāizpilda, labāk īstenojot esošos noteikumus.
- (34) Sadarbības grupai arī turpmāk vajadzētu būt elastīgam forumam un būtu jāspēj reaģēt uz mainīgām un jaunām politikas prioritātēm un problēmām, vienlaikus ņemot vērā resursu pieejamību. Tai būtu jāorganizē regulāras kopīgas sanāksmes ar attiecīgajām privātā sektora ieinteresētajām personām no visas Savienības, lai apspriestu grupas veiktās darbības un apkopotu informāciju par jaunām politikas problēmām. Lai uzlabotu sadarbību Savienības līmenī, grupai būtu jāapsver iespēja pieaicināt Savienības struktūras un aģentūras, kas iesaistītas kiberdrošības politikā, piemēram, Eiropas Kibernoziedzības apkarošanas centru (*EC3*), Eiropas Savienības Aviācijas drošības aģentūru (*EASA*) un Eiropas Savienības Kosmosa programmas aģentūru (*EUSPA*), lai tās piedalītos tās darbā.
- (35) Lai uzlabotu sadarbību, kompetentajām iestādēm un *CSIRT* vajadzētu būt iespējai piedalīties apmaiņas shēmās, kas paredzētas amatpersonām no citām dalībvalstīm.

Kompetentajām iestādēm būtu jāveic pasākumi, kas nepieciešami, lai amatpersonas no citām dalībvalstīm varētu efektīvi piedalīties uzņēmējas kompetentās iestādes pasākumos.

- (36) Attiecīgā gadījumā Savienībai saskaņā ar LESD 218. pantu būtu jānoslēdz starptautiski nolīgumi ar trešām valstīm vai starptautiskām organizācijām, ļaujot tām piedalīties un organizējot to dalību atsevišķās sadarbības grupas un CSIRT tīkla darbībās. Šādos nolīgumos būtu jānodrošina pienācīga datu aizsardzība.
- (37) Dalībvalstīm būtu jāsniedz ieguldījums Ieteikumā (ES) 2017/1584 noteiktā ES satvara reaģēšanai kibernetiskās drošības krīzēs izveidošanā, izmantojot esošos sadarbības tīklus, jo īpaši Kiberkrīžu sadarbības organizāciju tīklu (*EU-CyCLONe*), CSIRT tīklu un sadarbības grupu. *EU-CyCLONe* un CSIRT tīklam būtu jāsadarbojas, pamatojoties uz procedūram, kas nosaka šādas sadarbības procesuālo kārtību. *EU-CyCLONe* reglamentā būtu jāprecizē kārtība, kādā tīklam būtu jādarbojas, cita starpā paredzot uzdevumus, sadarbības veidus, mijiedarbību ar citiem attiecīgiem dalībniekiem un veidnes informācijas apmaiņai, kā arī saziņas līdzekļus. Attiecībā uz krīžu pārvaldību Savienības līmenī attiecīgajām pusēm būtu jāpaļaujas uz integrētajiem krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismiem. Šim nolūkam Komisijai būtu jāizmanto krīzes augstlīmeņa starpnozaru koordinācijas process *ARGUS*. Ja krīzei ir nozīmīgs ārējās politikas vai kopīgās drošības un aizsardzības politikas (KDAP) aspekts, būtu jāiedarbina Eiropas Ārējās darbības dienesta (EĀDD) mehānisms reaģēšanai krīzes situācijās (*CRM*).
- (38) Šajā direktīvā termins “risks” būtu jāattiecina uz tādu zaudējumu vai traucējumu iespējamību, ko izraisa kibernetiskās drošības incidents, un tas būtu jāinterpretē kā šādu zaudējumu vai traucējumu apmēra un minētā incidenta varbūtības apvienojums.
- (39) Šajā direktīvā termins “gandrīz noticis notikums” būtu jāattiecina uz notikumu, kurš būtu varējis izraisīt kaitējumu, bet kura pilnīga izvēršanās tika veiksmīgi novērsta.
- (40) Riska pārvaldības pasākumos būtu jāietver pasākumi nolūkā identificēt visus incidentu riskus, novērst, atklāt incidentus un reaģēt uz tiem, un mazināt to ietekmi. Tīklu un informācijas sistēmu drošībai būtu jāietver glabāto, pārsūtīto un apstrādāto datu drošība.
- (41) Lai izvairītos no nesamērīga finansiāla un administratīva sloga radīšanas būtiskajām un svarīgajām vienībām, kibernetiskās riska pārvaldības prasībām vajadzētu būt samērīgām ar risku, ko rada attiecīgā tīklu un informācijas sistēma, ņemot vērā jaunākos sasniegumus saistībā ar šādiem pasākumiem.
- (42) Būtiskajām un svarīgajām vienībām būtu jānodrošina savās darbībās izmantoto tīklu un informācijas sistēmu drošība. Tās galvenokārt ir privātas tīklu un informācijas sistēmas, kuras pārvalda iekšējais IT personāls vai kuru drošība tiek nodrošināta, izmantojot ārpakalpojumus. Kibernetiskās riska pārvaldības un ziņošanas prasības atbilstoši šai direktīvai būtu jāattiecina uz būtiskajām un svarīgajām vienībām neatkarīgi no tā, vai tās veic savu tīklu un informācijas sistēmu uzturēšanu iekšēji vai šim nolūkam izmanto ārpakalpojumus.
- (43) Risināt kibernetiskās riskus, kas izriet no vienības piegādes ķēdes un tās attiecībām ar tās piegādātājiem, ir īpaši svarīgi, ņemot vērā tādu incidentu izplatību, kuros vienības ir cietušas kibernetiskās drošības un kuros ļaunprātīgi dalībnieki ir spējuši apdraudēt vienības tīklu un informācijas sistēmu drošību, izmantojot neaizsargātību, kas skar trešo personu produktus un pakalpojumus. Tāpēc vienībām būtu jānovērtē un jāņem

vērā to piegādātāju un pakalpojumu sniedzēju produktu vispārējā kvalitāte un kiberdrošības prakse, tai skaitā to drošas attīstības procedūras.

- (44) Pakalpojumu sniedzēju vidū pārvaldītas drošības pakalpojumu sniedzējiem (*MSSP*) tādās jomās kā reaģēšana uz incidentiem, ielaušanās testēšana, drošības revīzijas un konsultācijas ir īpaši svarīga loma, palīdzot vienībām to centienos atklāt incidentus un reaģēt uz tiem. Tomēr arī šādi *MSSP* paši ir bijuši kiberuzbrukumu mērķis, un tie rada īpašu kiberdrošības risku, jo ir cieši iesaistīti operatoru darbībās. Tāpēc vienībām, izvēloties *MSSP*, būtu jāievēro īpaša piesardzība.
- (45) Vienībām būtu arī jāpievēršas kiberdrošības riskiem, kas izriet no to mijiedarbības un attiecībām ar citām ieinteresētajām personām plašākā ekosistēmā. Vienībām jo īpaši būtu jāveic atbilstīgi pasākumi, lai nodrošinātu, ka to sadarbība ar akadēmiskajām un pētniecības iestādēm notiek atbilstoši to kiberdrošības politikai un ka tās ietvaros tiek ievērota laba prakse attiecībā uz drošu piekļuvi un informācijas izplatīšanu kopumā un jo īpaši intelektuālā īpašuma aizsardzību. Līdzīgi, ņemot vērā datu nozīmīgumu un vērtību vienību darbībās, vienībām, paļaujoties uz trešo personu sniegtiem datu transformēšanas un datu analīzes pakalpojumiem, būtu jāveic visi atbilstīgie kiberdrošības pasākumi.
- (46) Lai turpinātu pievērsties galvenajiem piegādes ķēdes riskiem un palīdzētu vienībām, kas darbojas nozarēs, uz kurām attiecas šī direktīva, pienācīgi pārvaldīt ar piegādes ķēdēm un piegādātājiem saistītus kiberdrošības riskus, sadarbības grupai, iesaistot attiecīgās valsts iestādes un sadarbojoties ar Komisiju un *ENISA*, būtu jāveic koordinēti nozaru piegādes ķēžu riska novērtējumi, kā tas jau tika darīts attiecībā uz 5G tīkliem saskaņā ar Ieteikumu (ES) 2019/534 par 5G tīklu kiberdrošību²¹, lai par katru nozari apzinātu, kuri ir kritiskie IKT pakalpojumi, sistēmas vai produkti, attiecīgie draudi un neaizsargātība.
- (47) Piegādes ķēžu riska novērtējumos, ievērojot attiecīgās nozares iezīmes, būtu jāņem vērā gan tehniski, gan attiecīgā gadījumā netehniski faktori, tai skaitā tie, kas definēti Ieteikumā (ES) 2019/534, ES mēroga koordinētajā 5G tīklu drošības novērtējumā un ES rīkkopā par 5G kiberdrošību, kuru saskaņojusi sadarbības grupa. Lai apzinātu piegādes ķēdes, par kurām būtu jāveic koordinēts riska novērtējums, būtu jāņem vērā šādi kritēriji: i) tas, ciktāl būtiskās un svarīgās vienības izmanto īpašus kritiskus IKT pakalpojumus, sistēmas vai produktus un paļaujas uz tiem; ii) īpašu kritisku IKT pakalpojumu, sistēmu vai produktu nozīmīgums kritisku vai sensitīvu funkciju veikšanā, arī persondatu apstrādē; iii) alternatīvu IKT pakalpojumu, sistēmu vai produktu pieejamība; iv) IKT pakalpojumu, sistēmu vai produktu vispārējās piegādes ķēdes noturība pret notikumiem, kas izraisa traucējumus, un v) attiecībā uz jauniem IKT pakalpojumiem, sistēmām vai produktiem — to iespējamais turpmākais nozīmīgums vienību darbībām.
- (48) Lai racionalizētu juridiskos pienākumus, kas noteikti publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem un uzticamības pakalpojumu sniedzējiem saistībā ar to tīklu un informācijas sistēmu drošību, un lai šīs vienības un to attiecīgās kompetentās iestādes varētu gūt labumu no tiesiskā regulējuma, kas izveidots ar šo direktīvu (ieskaitot par riska un incidentu risināšanu atbildīgo *CSIRT* izraudzīšanos, kompetento iestāžu un struktūru piedalīšanos sadarbības grupas un *CSIRT* tīkla darbā), tie būtu jāiekļauj šīs

²¹ Komisijas Ieteikums (ES) 2019/534 (2019. gada 26. marts) par 5G tīklu kiberdrošību (OV L 88, 29.3.2019., 42. lpp.).

direktīvas piemērošanas jomā. Tāpēc atbilstošie noteikumi, kas paredzēti Eiropas Parlamenta un Padomes Regulā (ES) Nr. 910/2014²² un Eiropas Parlamenta un Padomes Direktīvā (ES) 2018/1972²³ saistībā ar drošības un paziņošanas prasības piemērošanu šo veidu vienībām, būtu jāatceļ. Noteikumiem par ziņošanas pienākumiem nebūtu jāskar Regula (ES) 2016/679 un Eiropas Parlamenta un Padomes Direktīva 2002/58/EK²⁴.

- (49) Attiecīgā gadījumā un lai izvairītos no nevajadzīgiem traucējumiem, kompetentajām iestādēm, kas atbild par uzraudzību un izpildi šīs direktīvas nolūkos, būtu jāturpina izmantot esošās valsts pamatnostādnes un valsts tiesību aktus, kas pieņemti, lai transponētu ar drošības pasākumiem saistītos noteikumus, kuri paredzēti Direktīvas (ES) 2018/1972 40. panta 1. punktā, kā arī minētās direktīvas 40. panta 2. punkta prasības attiecībā uz parametriem, kas saistīti ar incidenta nozīmīgumu.
- (50) Tā kā palielinās numurneatkarīgo starppersonu sakaru pakalpojumu nozīme, ir jānodrošina, ka uz tiem attiecas arī piemērotas drošības prasības, ņemot vērā to specifiku un ekonomisko svaru. Šādu pakalpojumu sniedzējiem tādējādi būtu arī jānodrošina radītajam riskam atbilstošs tīklu un informācijas sistēmu drošības līmenis. Tā kā numurneatkarīgo starppersonu sakaru pakalpojumu sniedzēji nemēdz faktiski kontrolēt signālu pārraidi tīklos, risku šādiem pakalpojumiem savā ziņā var uzskatīt par zemāku nekā tradicionālajiem elektronisko sakaru pakalpojumiem. Tas pats attiecas uz starppersonu sakaru pakalpojumiem, kuros izmanto numurus un kuros netiek īstenota faktiska kontrole pār signālu pārraidi.
- (51) Iekšējais tirgus ir vairāk atkarīgs no interneta darbības nekā jebkad iepriekš. Praktiski visu būtisko un svarīgo vienību pakalpojumi ir atkarīgi no internetā sniegtajiem pakalpojumiem. Lai nodrošinātu būtisko un svarīgo vienību pakalpojumu netraucētu sniegšanu, ir svarīgi, lai publiskajiem elektronisko sakaru tīkliem, piemēram, interneta pamattīkliem vai zemūdens sakaru kabeļiem, būtu ieviesti atbilstīgi kiberdrošības pasākumi un lai tie ziņotu par saistītajiem incidentiem.
- (52) Attiecīgā gadījumā vienībām būtu jāinformē to pakalpojumu saņēmēji par īpašiem un nozīmīgiem draudiem un par pasākumiem, kurus tās var veikt, lai mazinātu izrietošo risku, kas tām rodas. Prasībai informēt lietotājus par šādiem apdraudējumiem nebūtu jāatbrīvo vienības no pienākuma par saviem līdzekļiem veikt atbilstīgus un steidzamus pasākumus, lai izlabotu vai likvidētu jebkurus kiberdraudus un atjaunotu normālu pakalpojuma drošības līmeni. Šāda informācija par drošības apdraudējumiem būtu jāsniedz saņēmējiem bez maksas.
- (53) Jo īpaši publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem būtu jāinformē pakalpojumu saņēmēji par konkrētiem un nozīmīgiem kiberdraudiem un par pasākumiem, ko tie var veikt, lai aizsargātu to sakaru drošību, izmantojot, piemēram, konkrētu veidu programmatūru vai šifrēšanas tehnoloģijas.

²² Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).

²³ Eiropas Parlamenta un Padomes Direktīva (ES) 2018/1972 (2018. gada 11. decembris) par Eiropas Elektronisko sakaru kodeksa izveidi (OV L 321, 17.12.2018., 36. lpp.).

²⁴ Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

- (54) Lai garantētu elektronisko sakaru tīklu un pakalpojumu drošību, būtu jāveicina šifrēšanas, jo īpaši pilnīgas šifrēšanas, izmantošana, kam nepieciešamības gadījumā saskaņā ar principiem par drošību un privātumu pēc noklusējuma 18. panta nolūkos vajadzētu būt obligātai šādu pakalpojumu sniedzējiem un tīklu nodrošinātājiem. Pilnīgas šifrēšanas izmantošana būtu jāsaskaņo ar dalībvalstu pilnvarām, lai nodrošinātu dalībvalstu būtisko drošības interešu un sabiedrības aizsardzību un ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem atbilstoši Savienības tiesību aktiem. Risinājumos par likumīgu piekļuvi informācijai pilnīgi šifrētos sakaros būtu jā saglabā šifrēšanas efektivitāte privātuma un sakaru drošības aizsardzībā, vienlaikus efektīvi reaģējot uz noziedzīgiem nodarījumiem.
- (55) Šī direktīva nosaka divposmu pieeju attiecībā uz incidentu paziņošanu, lai panāktu pareizo līdzsvaru starp ātru ziņošanu, kas palīdz mazināt incidentu iespējamo izplatīšanos un ļauj vienībām lūgt atbalstu, no vienas puses, un padziļinātu ziņošanu, kurā gūst vērtīgu mācību no individuāliem incidentiem un laika gaitā uzlabo individuālu uzņēmumu un visu nozaru noturību pret kiberdraudiem, no otras puses. Ja vienības konstatē incidentu, tām vajadzētu būt pienākamam iesniegt sākotnējo paziņojumu 24 stundu laikā, kā arī galīgo ziņojumu ne vēlāk kā viena mēneša laikā. Sākotnējā paziņojumā būtu jāiekļauj tikai informācija, kas ir obligāti nepieciešama, lai informētu kompetentās iestādes par incidentu un vajadzības gadījumā ļautu vienībai lūgt palīdzību. Šādā paziņojumā attiecīgā gadījumā būtu jānorāda, vai incidentu varētu būt izraisījusi nelikumīga vai ļaunprātīga darbība. Dalībvalstīm būtu jānodrošina, ka prasība iesniegt šo sākotnējo paziņojumu nenovirza ziņotājas vienības resursus no darbībām, kas saistītas ar incidentu risināšanu un kas būtu jānosaka par prioritārām. Lai turpmāk novērstu to, ka incidentu paziņošanas pienākumi novirza resursus no reaģēšanas uz incidentiem vai var citādi traucēt vienību centienus šajā saistībā, dalībvalstīm būtu arī jāparedz, ka pienācīgi pamatotos gadījumos un pēc vienošanās ar kompetentajām iestādēm vai CSIRT attiecīgā vienība var atkāpties no 24 stundu termiņa sākotnējam paziņojumam un viena mēneša termiņa galīgajam ziņojumam.
- (56) Būtiskas un svarīgas vienības bieži atrodas situācijā, kad konkrēts incidents, ņemot vērā tā iezīmes, ir jāpaziņo dažādām iestādēm, jo to paredz paziņošanas pienākumi, kas ietverti dažādos tiesību instrumentos. Šādi gadījumi rada papildu slogus un var arī izraisīt nenoteiktību attiecībā uz šādu paziņojumu formātu un procedūram. Ņemot to vērā, kā arī lai vienkāršotu ziņošanu par drošības incidentiem, dalībvalstīm būtu jāizveido *vienots kontaktpunkts* visiem paziņojumiem, kas jāsniedz saskaņā ar šo direktīvu un arī citiem Savienības tiesību aktiem, piemēram, Regulu (ES) 2016/679 un Direktīvu 2002/58/EK. ENISA kopā ar sadarbības grupu būtu jāizstrādā vienotas ziņojumu veidnes, pieņemot pamatnostādnes, ar kurām vienkāršo un racionalizē ziņojamo informāciju, ko pieprasa Savienības tiesību akti, un mazina slogus uzņēmumiem.
- (57) Ja ir aizdomas, ka incidents ir saistīts ar smagām noziedzīgām darbībām, kas noteiktas Savienības vai valsts tiesību aktos, dalībvalstīm būtu jā mudina būtiskās un svarīgās vienības, pamatojoties uz piemērojamiem kriminālprocesa noteikumiem atbilstoši Savienības tiesībām, ziņot attiecīgajām tiesībaizsardzības iestādēm par incidentiem, kam varētu būt smagas noziedzības raksturs. Attiecīgos gadījumos un neskarot persondatu aizsardzības noteikumus, kas piemērojami Eiropalam, vēlams, ka EC3 un ENISA veicina koordināciju starp dažādu dalībvalstu kompetentajām iestādēm un tiesībaizsardzības iestādēm.
- (58) Incidentu dēļ daudzos gadījumos tiek apdraudēti persondati. Šajā saistībā kompetentajām iestādēm būtu jāsadarbjas un jāapmainās ar informāciju par visiem

būtiskajiem jautājumiem ar datu aizsardzības iestādēm un uzraudzības iestādēm atbilstoši Direktīvai 2002/58/EK.

- (59) Lai garantētu DNS drošību, stabilitāti un noturību, kas savukārt veicina vienādi augsta līmeņa kiberdrošību Savienībā, ir svarīgi uzturēt precīzas un pilnīgas domēnu nosaukumu un reģistrācijas datu (tā dēvētie “*WHOIS* dati”) datubāzes un nodrošināt likumīgu piekļuvi šādiem datiem. Ja tiek apstrādāti persondati, šādā apstrādē ievēro Savienības datu aizsardzības tiesību aktus.
- (60) Šādu datu savlaicīga pieejamība publiskajām iestādēm, tai skaitā kompetentajām iestādēm atbilstoši Savienības vai valstu tiesību aktiem, lai novērstu un izmeklētu noziedzīgus nodarījumus vai sodītu par tiem, *CERT*, *CSIRT* un — attiecībā uz to klientu datiem — elektronisko sakaru tīklu nodrošinātājiem un pakalpojumu sniedzējiem un kiberdrošības tehnoloģiju nodrošinātājiem un pakalpojumu sniedzējiem, kas darbojas minēto klientu vārdā, ir svarīga, lai novērstu un apkarotu domēnu nosaukumu sistēmu ļaunprātīgu izmantošanu, jo īpaši lai novērstu un atklātu kiberdrošības incidentus un ziņotu par tiem. Šādā piekļuvē būtu jāievēro Savienības datu aizsardzības tiesību akti, ciktāl tā ir saistīta ar persondatiem.
- (61) Lai nodrošinātu precīzu un pilnīgu domēnu nosaukumu reģistrācijas datu pieejamību, ALD reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD (tā dēvētajiem reģistratoriem), būtu jāsavāc domēnu nosaukumu reģistrācijas dati un jāgarantē to integritāte un pieejamība. Konkrētāk, ALD reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, būtu jānosaka politika un procedūras precīzu un pilnīgu reģistrācijas datu vākšanai un uzturēšanai, kā arī neprecīzu reģistrācijas datu novēršanai un izlabošanai saskaņā ar Savienības datu aizsardzības noteikumiem.
- (62) ALD reģistriem un vienībām, kas tiem sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jādara publiski pieejami domēnu nosaukumu reģistrācijas dati, uz kuriem neattiecas Savienības datu aizsardzības noteikumi, piemēram, dati, kas attiecas uz juridiskām personām²⁵. ALD reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, būtu arī jānodrošina legītīmiem piekļuves prasītājiem likumīga piekļuve īpašiem domēnu nosaukumu reģistrācijas datiem par fiziskām personām saskaņā ar Savienības datu aizsardzības tiesību aktiem. Dalībvalstīm būtu jānodrošina, ka ALD reģistri un vienības, kas tiem sniedz domēnu nosaukumu reģistrācijas pakalpojumus, bez nepamatotas kavēšanās atbild uz legītīmo piekļuves prasītāju pieprasījumiem izpaust domēnu nosaukumu reģistrācijas datus. ALD reģistriem un vienībām, kas tiem sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jānosaka politika un procedūras reģistrācijas datu, tai skaitā pakalpojumu līmeņa līgumu, publicēšanai un izpaušanai, lai izpildītu legītīmo piekļuves prasītāju piekļuves pieprasījumus. Piekļuves procedūrā var arī ietvert saskarnes, portāla vai cita tehniska rīka izmantošanu, lai nodrošinātu efektīvu sistēmu reģistrācijas datu pieprasīšanai un piekļūšanai tiem. Lai veicinātu saskaņotu praksi visā iekšējā tirgū, Komisija var pieņemt pamatnostādnes par šādām procedūrām, neskarot Eiropas Datu aizsardzības kolēģijas kompetences.

²⁵

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/679 14. apsvērums: “ši regula neattiecas uz tādu personas datu apstrādi, kas skar juridiskas personas un jo īpaši uzņēmumus, kuriem ir juridiskas personas statuss, tostarp juridiskās personas nosaukumu, uzņēmējdarbības formu un kontaktinformāciju”.

- (63) Visām būtiskajām un svarīgajām vienībām atbilstoši šai direktīvai vajadzētu būt tās dalībvalsts jurisdikcijā, kurā tās sniedz pakalpojumus. Ja vienība sniedz pakalpojumus vairāk nekā vienā dalībvalstī, tai vajadzētu būt katras attiecīgās dalībvalsts atsevišķā un vienlaicīgā jurisdikcijā. Šo dalībvalstu kompetentajām iestādēm būtu jāsadarbjas, jāsniedz savstarpēja palīdzība un attiecīgā gadījumā jāveic kopīgas uzraudzības darbības.
- (64) Lai ņemtu vērā DNS pakalpojumu sniedzēju, ALD nosaukumu reģistru, satura piegādes tīklu nodrošinātāju, mākoņpakalpojumu sniedzēju, datu centru pakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju pakalpojumu un darbību pārrobežu raksturu, tikai vienai dalībvalstij vajadzētu būt jurisdikcijai pār šīm vienībām. Jurisdikcija būtu jāpiedēvē tai dalībvalstij, kurā attiecīgajai vienībai ir tās galvenā darbījumsdarbības vieta Savienībā. Darbījumsdarbības vietas kritērijs šīs direktīvas nolūkos ietver darbības efektīvu īstenošanu ar stabila veidojuma starpniecību. Šāda veidojuma juridiskā forma neatkarīgi no tā, vai tas ir filiāle vai meitasuzņēmums ar juridiskas personas statusu, šajā saistībā nav noteicošais faktors. Tam, vai šis kritērijs ir izpildīts, vajadzētu būt atkarīgam no tā, vai tīklu un informācijas sistēmas fiziski atrodas noteiktā vietā; šādu sistēmu klātbūtne un izmantošana pati par sevi nav uzskatāma par šādu galveno darbījumsdarbības vietu un tāpēc nav izšķirošs kritērijs galvenās darbījumsdarbības vietas noteikšanai. Par galveno darbījumsdarbības vietu būtu jāuzskata vieta, kur Savienībā tiek pieņemti ar kiberdrošības riska pārvaldības pasākumiem saistīti lēmumi. Parasti tā ir vieta, kur atrodas uzņēmumu centrālā administrācija Savienībā. Ja šādus lēmumus nepieņem Savienībā, būtu jāuzskata, ka galvenā darbījumsdarbības vieta ir dalībvalstīs, kurās vienībai ir darbījumsdarbības vieta ar vislielāko darbinieku skaitu Savienībā. Ja pakalpojumus sniedz uzņēmumu grupa, par uzņēmumu grupas galveno uzņēmējdarbības vietu būtu jāuzskata kontrolējošā uzņēmuma galvenā darbījumsdarbības vieta.
- (65) Gadījumos, kad DNS pakalpojumu sniedzējs, ALD nosaukumu reģistrs, satura piegādes tīklu nodrošinātājs, mākoņpakalpojumu sniedzējs, datu centra pakalpojumu sniedzējs un digitālo pakalpojumu sniedzējs, kam nav darbījumsdarbības vietas Savienībā, piedāvā pakalpojumus Savienībā, tam būtu jāizraugās pārstāvis. Lai noteiktu, vai šāda vienība piedāvā pakalpojumus Savienībā, būtu jāpārlicinās, vai ir acīmredzami tas, ka vienība plāno piedāvāt pakalpojumus personām vienā vai vairākās dalībvalstīs. Lai pārlicinātos par šādu nodomu, nepietiek tikai ar to vien, ka Savienībā ir pieejama vienības vai starpnieka tīmekļa vietne vai e-pasta adrese un cita kontaktinformācija vai ka tiek izmantota valoda, ko parasti izmanto trešā valstī, kurā ir vienības darbījumsdarbības vieta. Tomēr tādi faktori kā, piemēram, izmantotā valoda vai valūta, ko parasti izmanto vienā vai vairākās dalībvalstīs, piedāvājot pasūtīt pakalpojumus šajā citā valodā, vai Savienībā esošu klientu vai lietotāju pieminēšana var liecināt par to, ka vienība plāno piedāvāt pakalpojumus Savienībā. Pārstāvim būtu jārīkojas vienības vārdā, un kompetentajām iestādēm vai CSIRT vajadzētu būt iespējai sazināties ar pārstāvi. Pārstāvis būtu jāizraugās nepārprotami ar vienības rakstisku pilnvarojumu rīkoties tās vārdā attiecībā uz tās pienākumiem saskaņā ar šo direktīvu, tai skaitā attiecībā uz ziņošanu par incidentiem.
- (66) Ja notiek apmaiņa ar informāciju, ko saskaņā ar valsts vai Savienības tiesību aktiem uzskata par klasificētu, vai šāda informācija tiek paziņota vai citādi koplietota atbilstoši šīs direktīvas noteikumiem, būtu jāpiemēro atbilstošie īpašie noteikumi par rīcību ar klasificētu informāciju.
- (67) Tā kā kiberdraudi kļūst sarežģītāki un attīstītāki, labi atklāšanas un profilakses pasākumi lielā mērā ir atkarīgi no regulāras apdraudējumu un neaizsargātības

izlūkdatu apmaiņas starp vienībām. Informācijas apmaiņa veicina lielāku informētību par kiberdraudiem, kas savukārt uzlabo vienību spēju novērst draudu pārtapšanu reālos incidentos un ļauj vienībām labāk ierobežot incidentu ietekmi un efektīvāk novērst to sekas. Nepastāvot Savienības līmeņa norādījumiem, šādu izlūkdatu apmaiņu, šķiet, ir kavējuši vairāki faktori, jo īpaši nenoteiktība attiecībā uz saderību ar konkurences un atbildības noteikumiem.

- (68) Vienības būtu jāmudina kolektīvi izmantot to individuālās zināšanas un praktisko pieredzi stratēģiskā, taktiskā un darbības līmenī, lai uzlabotu to spējas pienācīgi novērtēt un uzraudzīt kiberdraudus, aizsargāties pret tiem un reaģēt uz tiem. Tādējādi ir nepieciešams nodrošināt iespējas, lai parādītos Savienības līmeņa mehānismi brīvprātīgiem informācijas apmaiņas pasākumiem. Šajā nolūkā dalībvalstīm būtu aktīvi jāatbalsta un jāmudina šādos informācijas apmaiņas mehānismos piedalīties arī attiecīgās vienības, kas nav šīs direktīvas darbības joma. Minētie mehānismi būtu jāvada, pilnībā ievērojot Savienības konkurences noteikumus, kā arī Savienības datu aizsardzības tiesību aktu noteikumus.
- (69) Persondatu apstrādei, ciktāl tā ir stingri nepieciešama un samērīga, lai vienības, publiskās iestādes, *CERT*, *CSIRT* un drošības tehnoloģiju nodrošinātāji un pakalpojumu sniedzēji nodrošinātu tīklu un informācijas drošību, būtu jānotiek attiecīgā datu pārziņa leģitīmajās interesēs, kā minēts Regulā (ES) 2016/679. Tajā būtu jāietver pasākumi, kas saistīti ar incidentu novēršanu, atklāšanu, analīzi un reaģēšanu uz tiem, pasākumi, kas veicina informētību par īpašiem kiberdraudiem, informācijas apmaiņu neaizsargātības izlabošanas un koordinētas atklāšanas kontekstā, brīvprātīgu informācijas apmaiņu par minētajiem incidentiem, kā arī kiberdraudiem un neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem. Šādiem pasākumiem var būt vajadzīga šādu veidu persondatu apstrāde: IP adreses, vienotie resursu vietraži (*URL*), domēnu nosaukumi un e-pasta adreses.
- (70) Lai nostiprinātu uzraudzības pilnvaras un darbības, kas palīdz nodrošināt efektīvu atbilstību, šajā direktīvā būtu jāparedz minimāls to uzraudzības darbību un līdzekļu saraksts, ar kuru starpniecību kompetentās iestādes var uzraudzīt būtiskas un svarīgas vienības. Turklāt šajā direktīvā būtu jānosaka uzraudzības režīma nošķirums starp būtiskajām un svarīgajām vienībām, lai nodrošinātu pienākumu taisnīgu līdzsvaru gan vienībām, gan kompetentajām iestādēm. Tādējādi būtiskajām vienībām būtu jāpiemēro pilnīgs uzraudzības režīms (*ex ante* un *ex post*), savukārt svarīgajām vienībām būtu jāpiemēro vieglais uzraudzības režīms — tikai *ex post*. Attiecībā uz pēdējām minētajām tas nozīmē, ka svarīgajām vienībām nebūtu sistemātiski jādokumentē atbilstība kiberdrošības riska pārvaldības prasībām, savukārt kompetentajām iestādēm būtu jāīsteno atpakaļejoša *ex post* pieeja uzraudzībai, un tādējādi tām nav vispārēja pienākuma uzraudzīt minētās vienības.
- (71) Lai izpilde būtu efektīva, būtu jānosaka minimāls to administratīvo sankciju saraksts, kuras piemēro par šajā direktīvā paredzēto kiberdrošības riska pārvaldības un ziņošanas pienākumu pārkāpumiem, izveidojot skaidru un konsekventu satvaru šādām sankcijām visā Savienībā. Būtu pienācīgi jāņem vērā pārkāpuma veids, smagums un ilgums, faktiskais izraisītais kaitējums vai zaudējumi vai iespējamais kaitējums vai zaudējumi, kas būtu varējuši rasties, tas, vai pārkāpums izdarīts tīši vai nolaidības dēļ, darbības, kas veiktas, lai novērstu vai mazinātu radīto kaitējumu un/vai zaudējumus, atbildības pakāpe vai jebkādi būtiski iepriekšēji pārkāpumi, sadarbības ar kompetento iestādi pakāpe un jebkādi citi vainu pastiprinoši vai mīkstinoši apstākļi. Sodu, arī administratīvu naudas sodu, uzlikšanai būtu jāpiemēro atbilstīgas procesuālās

garantijas saskaņā ar vispārīgiem Savienības tiesību principiem un Eiropas Savienības Pamattiesību hartu, tai skaitā efektīva tiesību aizsardzība tiesā un pienācīgas procedūras.

- (72) Lai nodrošinātu šajā direktīvā noteikto pienākumu efektīvu izpildi, katrai kompetentajai iestādei vajadzētu būt pilnvarām uzlikt administratīvus naudas sodus vai pieprasīt to uzlikšanu.
- (73) Ja administratīvi naudas sodi tiek uzlikti uzņēmumam, minētajā nolūkā uzņēmums būtu jāsaprot kā uzņēmums saskaņā ar LESD 101. un 102. pantu. Ja administratīvi naudas sodi tiek uzlikti personām, kas nav uzņēmums, uzraudzības iestādei, apsverot atbilstošo naudas soda apjomu, būtu jāņem vērā vispārējais ienākumu līmenis dalībvalstī, kā arī attiecīgās personas ekonomiskā situācija. Dalībvalstīm būtu jānosaka, vai un kādā apmērā administratīvi naudas sodi būtu piemērojami publiskām iestādēm. Administratīva naudas soda uzlikšana neietekmē citu kompetento iestāžu pilnvaru piemērošanu vai citu tādu sodu piemērošanu, kas noteikti valsts tiesību normās, ar kurām transponē šo direktīvu.
- (74) Dalībvalstīm būtu jāspēj pieņemt noteikumus par kriminālsodiem, ko piemēro, ja tiek pārkāptas valsts tiesību normas, ar kurām transponē šo direktīvu. Tomēr kriminālsodu piemērošanai par šādu valsts tiesību normu pārkāpumiem un saistītu administratīvu sodu piemērošanai nebūtu jāizraisa *ne bis in idem* principa pārkāpšana, kā to interpretējusi Tiesa.
- (75) Ja ar šo direktīvu netiek saskaņoti administratīvie sodi vai ja tas nepieciešams citos gadījumos, piemēram, šajā direktīvā noteikto pienākumu smagu pārkāpumu gadījumos, dalībvalstīm būtu jāievieš sistēma, kas paredz iedarbīgus, samērīgus un atturošus sodus. Šādu sodu — kriminālu vai administratīvu — raksturs būtu jānosaka ar dalībvalsts tiesību aktiem.
- (76) Lai vēl vairāk nostiprinātu to sodu iedarbīgumu un atturošo ietekmi, kuri piemērojami par atbilstoši šai direktīvai noteikto pienākumu pārkāpumiem, kompetentajām iestādēm vajadzētu būt pilnvarotām piemērot sankcijas, kas var būt sertifikācijas vai atļaujas darbības apturēšana attiecībā uz visiem būtiskas vienības sniegtajiem pakalpojumiem vai to daļu un pagaidu aizliegums fiziskai personai pildīt vadības funkcijas. Ņemot vērā šādu sankciju smagumu un ietekmi uz vienību darbībām un galu galā uz to patērētājiem, tās būtu jāpiemēro tikai tā, lai tās būtu samērīgas attiecībā pret pārkāpuma smagumu, un ņemot vērā katra gadījuma īpašos apstākļus, tai skaitā to, vai pārkāpums izdarīts tīši vai neuzmanības dēļ, un veiktās darbības radītā kaitējuma un/vai zaudējumu novēršanai vai mazināšanai. Šādas sankcijas būtu jāpiemēro tikai kā *ultima ratio*, proti, tikai pēc tam, kad visas citas attiecīgās izpildes darbības, kas noteiktas šajā direktīvā, jau ir izsmeltas, un tikai par laikposmu līdz brīdim, kad vienības, uz kurām sankcijas attiecas, veic nepieciešamās darbības, lai izlabotu trūkumus vai izpildītu kompetentās iestādes prasības, saistībā ar kurām šādas sankcijas tikušas piemērotas. Šādu sankciju piemērošanā ievēro atbilstīgas procesuālās garantijas saskaņā ar vispārīgiem Savienības tiesību principiem un Eiropas Savienības Pamattiesību hartu, tai skaitā efektīvu tiesību aizsardzību tiesā, pienācīgas procedūras, nevainīguma prezumpciju un tiesības uz aizstāvību.
- (77) Ar šo direktīvu būtu jānosaka noteikumi par sadarbību starp kompetentajām iestādēm un uzraudzības iestādēm saskaņā ar Regulu (ES) 2016/679, lai vērstos pret pārkāpumiem, kas saistīti ar persondatiem.

- (78) Šajā direktīvā būtu jāizvirza mērķis nodrošināt augstu atbildības līmeni par kiberdrošības riska pārvaldības pasākumiem un ziņošanas pienākumiem organizāciju līmenī. Šā iemesla dēļ to vienību pārvaldības struktūrām, uz kurām attiecas šīs direktīvas darbības joma, būtu jāapstiprina kiberdrošības riska pasākumi un jāuzrauga to īstenošana.
- (79) Būtu jāievieš salīdzinošās izvērtēšanas mehānisms, ļaujot dalībvalstu izraudzītajiem ekspertiem novērtēt kiberdrošības politikas īstenošanu, tai skaitā dalībvalstu spēju līmeni un pieejamos resursus.
- (80) Lai ņemtu vērā jaunus kiberdraudus, tehnoloģiju attīstību vai nozaru specifiku, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu attiecībā uz elementiem, kas saistīti ar šajā direktīvā prasītajiem riska pārvaldības pasākumiem. Komisija būtu arī jāpilnvaro pieņemt deleģētus aktus, ar ko nosaka, kurām būtisko vienību kategorijām ir jāsaņem sertifikāts un atbilstoši kurām īpašajām Eiropas kiberdrošības sertifikācijas shēmām. Ir īpaši svarīgi, lai Komisija, veicot sagatavošanās darbus, rīkotu atbilstīgas apspriešanās, arī ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu²⁶. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienlīdzīgu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.
- (81) Lai nodrošinātu vienotus nosacījumus šīs direktīvas attiecīgo noteikumu īstenošanai attiecībā uz procesuālo kārtību, kas nepieciešama sadarbības grupas darbībai, ar riska pārvaldības pasākumiem saistītajiem tehniskajiem elementiem vai informācijas veidu, incidentu paziņojumu formātu un procedūru, būtu jādeleģē Komisijai īstenošanas pilnvaras. Minētās pilnvaras būtu jāīsteno saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011²⁷.
- (82) Komisijai, apspriežoties ar ieinteresētajām personām, būtu periodiski jāpārskata šī direktīva, jo īpaši lai noteiktu izmaiņu veikšanas nepieciešamību, ņemot vērā izmaiņas sociālajos, politiskajos, tehnoloģiskajos vai tirgus apstākļos.
- (83) Ņemot vērā to, ka šīs direktīvas mērķi, proti, panākt vienādi augsta līmeņa kiberdrošību Savienībā, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet rīcības ietekmes dēļ to var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā direktīvā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai.
- (84) Šajā direktīvā ir respektētas pamattiesības un ievēroti principi, kas atzīti Eiropas Savienības Pamattiesību hartā, jo īpaši tiesības uz privātās dzīves un saziņas neaizskaramību, tiesības uz persondatu aizsardzību, darījumdarbības brīvība, tiesības uz īpašumu, tiesības uz efektīvu tiesību aizsardzību tiesā un tiesības tikt uzklausi.
- Šī direktīva būtu jāīsteno saskaņā ar minētajām tiesībām un principiem,

²⁶ OV L 123, 12.5.2016., 1. lpp.

²⁷ Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

I NODAĻA

Vispārīgi noteikumi

1. pants

Priekšmets

1. Šī direktīva paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienībā.
2. Minētajam nolūkam šajā direktīvā:
 - (a) ir noteikti dalībvalstu pienākumi pieņemt valsts kiberdrošības stratēģijas, izraudzīties valsts kompetentās iestādes, vienotos kontaktpunktus un datordrošības incidentu reaģēšanas vienības (*CSIRT*);
 - b) ir noteikti kiberdrošības riska pārvaldības un ziņošanas pienākumi vienībām, kas minētas kā būtiskas vienības I pielikumā un svarīgas vienības II pielikumā;
 - (c) ir noteikti pienākumi attiecībā uz kiberdrošības informācijas apmaiņu.

2. pants

Darbības joma

1. Šī direktīva ir piemērojama publiskām un privātām vienībām, kas minētas kā būtiskas vienības I pielikumā un kā svarīgas vienības II pielikumā. Šī direktīva nav piemērojama vienībām, kas kvalificējas kā mikrouzņēmumi un mazie uzņēmumi Komisijas Ieteikuma 2003/361/EK²⁸ nozīmē.
2. Tomēr šī direktīva ir piemērojama arī I un II pielikumā minētajām vienībām neatkarīgi no to lieluma, ja:
 - (a) pakalpojumus sniedz kāda no šīm vienībām:
 - i) publisko elektronisko sakaru tīklu nodrošinātāji vai publiski pieejamo elektronisko sakaru pakalpojumu sniedzēji, kas minēti I pielikuma 8. punktā;
 - ii) uzticamības pakalpojumu sniedzēji, kas minēti I pielikuma 8. punktā;
 - iii) augstākā līmeņa domēnu nosaukumu reģistri un domēnu nosaukumu sistēmu (DNS) pakalpojumu sniedzēji, kas minēti I pielikuma 8. punktā;
 - b) vienība ir valsts pārvaldes vienība, kas definēta 4. panta 23. punktā;
 - c) vienība ir vienīgais pakalpojuma sniedzējs dalībvalstī;

²⁸

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

- d) vienības sniegtā pakalpojuma iespējamam traucējumam var būt ietekme uz sabiedrības aizsardzību, sabiedrisko drošību un sabiedrības veselību;
- e) vienības sniegtā pakalpojuma iespējams traucējums var izraisīt sistēmiskus riskus, jo īpaši nozarēm, kurās šādam traucējumam var būt pārrobežu ietekme;
- f) vienība ir kritiska, jo tā ir īpaši nozīmīga reģionālā vai valsts līmenī konkrētā veida nozarei vai pakalpojuma veidam vai citām savstarpēji neatkarīgām nozarēm dalībvalstī;
- g) vienība ir identificēta kā kritiska vienība atbilstoši Eiropas Parlamenta un Padomes Direktīvai (ES) XXXX/XXXX²⁹ [Kritisko vienību noturības direktīva] vai kā vienība, kas ir līdzvērtīga kritiskai vienībai atbilstoši minētās direktīvas 7. pantam.

Dalībvalstis izveido atbilstoši b)–f) punktam noteikto vienību sarakstu, ko iesniedz Komisijai līdz [seši mēneši pēc transponēšanas termiņa]. Dalībvalstis pārskata minēto sarakstu regulāri un pēc tam vismaz reizi divos gados un pēc nepieciešamības to atjaunina.

- 3. Šī direktīva neskar dalībvalstu kompetenci attiecībā uz sabiedriskās drošības, aizsardzības un valsts drošības uzturēšanu atbilstoši Savienības tiesību aktiem.
- 4. Šo direktīvu piemēro, neskarot Padomes Direktīvu 2008/114/EK³⁰ un Eiropas Parlamenta un Padomes Direktīvas 2011/93/ES³¹ un 2013/40/ES³².
- 5. Neskarot LESD 346. pantu, informācijas — kas ir konfidenciāla, ievērojot Savienības un valstu tiesību normas, piemēram, normas par darījumdarbības konfidencialitāti, — apmaiņa notiek ar Komisiju un citām attiecīgajām iestādēm tikai tad, ja šāda apmaiņa ir nepieciešama šīs direktīvas piemērošanai. Apmainās tikai ar to informāciju, kas ir atbilstīga un samērīga šādas apmaiņas nolūkam. Informācijas apmaiņā ievēro minētās informācijas konfidencialitāti un aizsargā būtisko vai svarīgo vienību drošību un komerciālās intereses.
- 6. Ja saskaņā ar īpašu nozaru Savienības tiesību aktu noteikumiem būtiskajām vai svarīgajām vienībām ir vai nu jāpieņem kiberdrošības riska pārvaldības pasākumi, vai jāpaziņo incidenti vai nozīmīgi kiberdraudi un ja šādas prasības to ietekmes ziņā ir vismaz līdzvērtīgas šajā direktīvā noteiktajiem pienākumiem, attiecīgos šīs direktīvas noteikumus, tai skaitā noteikumu par uzraudzību un izpildi, kas paredzēts VI nodaļā, nepiemēro.

²⁹ [ieraksta pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

³⁰ Padomes Direktīva 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību (OV L 345, 23.12.2008., 75. lpp.).

³¹ Eiropas Parlamenta un Padomes Direktīva 2011/93/ES (2011. gada 13. decembris) par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, un ar kuru aizstāj Padomes Pamatlēmumu 2004/68/TI (OV L 335, 17.12.2011., 1. lpp.).

³² Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI (OV L 218, 14.8.2013., 8. lpp.).

3. pants *Minimālā saskaņošana*

Neskarot to pienākumus atbilstoši Savienības tiesību aktiem, dalībvalstis saskaņā ar šo direktīvu var pieņemt vai paturēt spēkā noteikumus, kas nodrošina augstāku kiberdrošības līmeni.

4. pants *Definīcijas*

Šajā direktīvā piemēro šādas definīcijas:

- 1) “tīklu un informācijas sistēma” ir:
 - a) elektronisko sakaru tīkls Direktīvas (ES) 2018/1972 2. panta 1. punkta nozīmē;
 - b) jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču grupa, no kurām viena vai vairākas ierīces, ievērojot programmu, veic digitālu datu automātisku apstrādi;
 - c) digitāli dati, ko a) un b) apakšpunktā minētie elementi glabā, apstrādā, iegūst vai sūta to darbības, izmantošanas, aizsardzības un uzturēšanas nolūkos;
- 2) “tīklu un informācijas sistēmu drošība” ir tīklu un informācijas sistēmu spēja noteiktā uzticamības līmenī pretoties jebkurām darbībām, kas apdraud glabājamo vai pārraidāmo, vai apstrādājamo datu pieejamību, autentiskumu, integritāti vai konfidencialitāti vai minēto tīklu un informācijas sistēmu piedāvātos vai ar to starpniecību pieejamos saistītos pakalpojumus;
- 3) “kiberdrošība” ir kiberdrošība Eiropas Parlamenta un Padomes Regulas (ES) 2019/881³³ 2. panta 1. punkta nozīmē;
- 4) “valsts kiberdrošības stratēģija” ir saskaņots dalībvalsts satvars, kas paredz stratēģiskus mērķus un prioritātes attiecībā uz tīklu un informācijas sistēmu drošību attiecīgajā dalībvalstī;
- 5) “incidents” ir jebkurš notikums, kas apdraud uzglabātu, pārsūtītu vai apstrādātu datu vai saistītu pakalpojumu, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību, pieejamību, autentiskumu, integritāti vai konfidencialitāti;
- 6) “incidenta risināšana” ir visas darbības un procedūras, kuru mērķis ir atklāt, analizēt un ierobežot incidentu, un reaģēšana uz to;
- 7) “kiberdrauds” ir kiberdrauds Regulas (ES) 2019/881 2. panta 8. punkta nozīmē;
- 8) “neaizsargātība” ir aktīva, sistēmas, procesa vai kontroles trūkums, uzņēmība vai nepilnība, ko var izmantot kiberdraudu gadījumā;
- 9) “pārstāvis” ir jebkura fiziska vai juridiska persona, kura atrodas Savienībā un ir skaidri izraudzīta rīkoties, lai pārstāvētu i) DNS pakalpojumu sniedzēju, augstākā

³³ Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

līmeņa domēnu (ALD) nosaukumu reģistru, mākoņpakalpojumu sniedzēju, datu centra pakalpojumu sniedzēju, satura piegādes tīkla nodrošinātāju, kā minēts I pielikuma 8. punktā, vai ii) vienības, kuras minētas II pielikuma 6. punktā un kuras neatrodas Savienībā, un pie kurām var vērsties valsts kompetentā iestāde vai *CSIRT* vienības vietā attiecībā uz minētās vienības pienākumiem atbilstoši šai direktīvai;

- 10) “standarts” ir standarts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012³⁴ 2. panta 1. punkta nozīmē;
- 11) “tehniskā specifikācija” ir tehniskā specifikācija Regulas (ES) Nr. 1025/2012 2. panta 4. punkta nozīmē;
- 12) “interneta plūsmu apmaiņas punkts (IPAP)” ir tīkla ierīce, kas nodrošina vairāk nekā divu neatkarīgu tīklu (autonomu sistēmu) savstarpēju savienošanu, galvenokārt lai veicinātu interneta datplūsmas apmaiņu; IPAP nodrošina savstarpēju savienošanu tikai autonomām sistēmām; IPAP nav vajadzīga interneta datplūsmas starp jebkuru iesaistīto autonomo sistēmu pāri, lai šķērsotu jebkuru trešo autonomo sistēmu, un tas nemaina šādu datplūsmu un citādi neiejaucas tajā;
- 13) “domēnu nosaukumu sistēma (DNS)” ir hierarhiska sadalīta nosaukumu sistēma, kas ļauj galalietotājiem sasniegt pakalpojumus un resursus internetā;
- 14) “DNS pakalpojumu sniedzējs” ir vienība, kas sniedz rekursīvus vai autoritatīvus domēnu nosaukumu atbildes pakalpojumus interneta galalietotājiem un citiem DNS pakalpojumu sniedzējiem;
- 15) “augstākā līmeņa domēnu nosaukumu reģistrs” ir vienība, kam deleģēts īpašs ALD un kas atbild par ALD pārvaldību, tai skaitā domēnu nosaukumu reģistrāciju ALD un ALD tehnisko darbību, kā arī tā nosaukumu serveru darbību, datubāzu uzturēšanu un ALD zonas datņu sadalīšanu starp nosaukumu serveriem;
- 16) “digitāls pakalpojums” ir pakalpojums Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/1535³⁵ 1. panta 1. punkta b) apakšpunkta nozīmē;
- 17) “tiešsaistes tirdzniecības vieta” ir digitāls pakalpojums Eiropas Parlamenta un Padomes Direktīvas 2005/29/EK³⁶ 2. panta n) punkta nozīmē;
- 18) “tiešsaistes meklētājprogramma” ir digitāls pakalpojums Eiropas Parlamenta un Padomes Regulas (ES) 2019/1150³⁷ 2. panta 5. punkta nozīmē;

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

³⁵ Eiropas Parlamenta un Padomes Direktīva (ES) 2015/1535 (2015. gada 9. septembris), ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā (OV L 241, 17.9.2015., 1. lpp.).

³⁶ Eiropas Parlamenta un Padomes Direktīva 2005/29/EK (2005. gada 11. maijs), kas attiecas uz uzņēmēju negodīgu komercpraksi iekšējā tirgū attiecībā pret patērētājiem un ar ko groza Padomes Direktīvu 84/450/EEK un Eiropas Parlamenta un Padomes Direktīvas 97/7/EK, 98/27/EK un 2002/65/EK un Eiropas Parlamenta un Padomes Regulu (EK) Nr. 2006/2004 (“Negodīgas komercprakses direktīva”) (OV L 149, 11.6.2005., 22. lpp.).

³⁷ Eiropas Parlamenta un Padomes Regula (ES) 2019/1150 (2019. gada 20. jūnijs) par taisnīguma un pārrēķināmības veicināšanu komerciālajiem lietotājiem paredzētos tiešsaistes starpniecības pakalpojumos (OV L 186, 11.7.2019., 57. lpp.).

- 19) “mākoņpakalpojums” ir digitāls pakalpojums, kas dod iespēju plaši un attālināti piekļūt kopīgojamu un sadalītu datu resursu mērogojamam un elastīgam pūlam un pēc pieprasījuma to pārvaldīt;
- 20) “datu centra pakalpojums” ir pakalpojums, kas ietver struktūras vai struktūru grupas, kuras paredzētas tāda informācijas tehnoloģijas un tīkla aprīkojuma centralizētai izmitināšanai, savstarpējai savienošanai un darbībai, kas sniedz datu uzglabāšanas, apstrādes un transportēšanas pakalpojumus kopā ar visām ierīcēm un infrastruktūrām jaudas sadalei un vides kontrolei;
- 21) “satura piegādes tīkls” ir ģeogrāfiski sadalītu serveru tīkls, kas nodrošina digitālā satura un pakalpojumu augstu pieejamību, piekļūstamību vai ātru piegādi interneta lietotājiem satura un pakalpojumu sniedzēju vārdā;
- 22) “sociālās tīklošanās pakalpojumu platforma” ir platforma, kas ļauj galalietotājiem pieslēgties, koplietot saturu, atklāt informāciju un savstarpēji sazināties, izmantojot vairākas ierīces, jo īpaši ar tērzētavu, paziņojumu, video un ieteikumu starpniecību;
- 23) “valsts pārvaldes vienība” ir dalībvalstī pastāvoša vienība, kas atbilst šādiem kritērijiem:
- (a) tā ir nodibināta ar mērķi apmierināt vispārējas vajadzības, un tai nav rūpnieciska vai komerciāla rakstura;
 - (b) tai ir juridiskas personas statuss;
 - (c) to galvenokārt finansē valsts, reģionāla iestāde vai citi publisko tiesību subjekti, vai tās pārvaldību uzrauga minētās iestādes vai subjekti, vai tās vadībā, valdē vai uzraudzības padomē vairāk nekā pusi locekļu ieceļ valsts, reģionālās iestādes vai citi publisko tiesību subjekti;
 - (d) tai ir pilnvaras adresēt fiziskām vai juridiskām personām administratīvus vai regulatīvus lēmumus, kas skar to tiesības saistībā ar personu, preču, pakalpojumu vai kapitāla pārrobežu pārvietošanos vai apriti.
- Minētais neattiecas uz valsts pārvaldes vienībām, kas veic darbības sabiedriskās drošības, tiesībsardzības, aizsardzības vai valsts drošības jomās;
- 24) “vienība” ir jebkura fiziska vai juridiska persona, kas izveidota un atzīta kā tāda atbilstoši tās darbīgdarbības vietas valsts tiesību aktiem un kas var savā vārdā īstenot tiesības un uzņemties pienākumus;
- 25) “būtiska vienība” ir jebkura tāda veida vienība, kas minēta kā būtiska vienība I pielikumā;
- 26) “svarīga vienība” ir jebkura tāda veida vienība, kas minēta kā svarīga vienība II pielikumā.

II NODAĻA

Koordinēti kiberdrošības tiesiskie regulējumi

5. pants

Valsts kiberdrošības stratēģija

1. Katra dalībvalsts pieņem valsts kiberdrošības stratēģiju, kurā nosaka stratēģiskos mērķus un atbilstīgus politikas un regulatīvus pasākumus, lai sasniegtu un uzturētu augstu kiberdrošības līmeni. Valsts kiberdrošības stratēģijā jo īpaši iekļauj:
 - (a) dalībvalstu kiberdrošības stratēģijas mērķu un prioritāšu definīciju;
 - (b) pārvaldības satvaru minēto mērķu un prioritāšu sasniegšanai, tostarp politikas nostādnes, kas minētas 2. punktā, un publisko struktūru un vienību, kā arī citu attiecīgo dalībnieku uzdevumus un pienākumus;
 - (c) novērtējumu attiecīgo aktīvu un kiberdrošības risku apzināšanai konkrētajā dalībvalstī;
 - (d) to pasākumu identifikāciju, kas nodrošina sagatavotību, reaģēšanu un atkopi pēc incidentiem, tostarp sadarbību starp publisko un privāto sektoru;
 - (e) valsts kiberdrošības stratēģijas īstenošanā iesaistīto dažādo iestāžu un dalībnieku sarakstu;
 - (f) politikas satvaru uzlabotai koordinācijai starp kompetentajām iestādēm atbilstoši šai direktīvai un Eiropas Parlamenta un Padomes Direktīvai (ES) XXXX/XXXX³⁸ [Kritisko vienību noturības direktīva], lai apmainītos ar informāciju par incidentiem un kiberdraudiem un uzraudzības uzdevumu īstenošanu.
2. Kā valsts kiberdrošības stratēģijas daļu dalībvalstis jo īpaši pieņem šādas politikas nostādnes:
 - a) politika, kas vērsta uz kiberdrošību piegādes ķēdē attiecībā uz IKT produktiem un pakalpojumiem, kurus būtiskās un svarīgās vienības izmanto pakalpojumu sniegšanai;
 - b) pamatnostādnes par to, kā publiskajā iepirkumā iekļaut un noteikt ar kiberdrošību saistītas prasības IKT produktiem un pakalpojumiem;
 - c) politika koordinētas neaizsargātības atklāšanas veicināšanai un sekmēšanai 6. panta nozīmē;
 - d) politika saistībā ar atvērtā interneta publiskā kodola vispārējās pieejamības un integritātes uzturēšanu;
 - e) politika kiberdrošības prasmju, izpratnes veidošanas, kā arī pētniecības un izstrādes iniciatīvu veicināšanai un attīstīšanai;
 - f) politika par atbalstu akadēmiskās un pētniecības iestādēm kiberdrošības rīku un drošas tīklu infrastruktūras attīstīšanā;

³⁸

[ieraksta pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

- g) politika, attiecīgas procedūras un atbilstīgi informācijas apmaiņas rīki, ar kuriem atbalstīta brīvprātīgu kiberdrošības informācijas apmaiņu starp uzņēmumiem, ievērojot Savienības tiesību aktus;
 - h) politika, kas vērsta uz MVU īpašajām vajadzībām, jo īpaši to MVU vajadzībām, kas nav šīs direktīvas darbības jomā, saistībā ar norādījumiem un atbalstu to noturības pret kiberdraudiem uzlabošanai.
3. Dalībvalstis paziņo savas valsts kiberdrošības stratēģijas Komisijai trīs mēnešu laikā pēc to pieņemšanas. Dalībvalstis var nepaziņot konkrētu informāciju, ja un ciktāl tas ir stingri nepieciešams, lai saglabātu valsts drošību.
4. Dalībvalstis novērtē savas valsts kiberdrošības stratēģijas vismaz reizi četros gados, pamatojoties uz galvenajiem darbības rādītājiem, un nepieciešamības gadījumā tās groza. Eiropas Savienības Kiberdrošības aģentūra (ENISA) pēc dalībvalstu lūguma palīdz tām izstrādāt valsts stratēģiju un galvenos darbības rādītājus stratēģijas novērtēšanai.

6. pants

Koordinēta neaizsargātības atklāšana un Eiropas neaizsargātības reģistrs

1. Katra dalībvalsts izraugās vienu no savām CSIRT, kā minēts 9. pantā, par koordinatoru koordinētas neaizsargātības atklāšanas vajadzībām. Izraudzītā CSIRT rīkojas kā uzticams starpnieks, nepieciešamības gadījumā veicinot mijiedarbību starp ziņotāju vienību un IKT produktu ražotāju vai IKT pakalpojumu sniedzēju. Ja paziņotā neaizsargātība attiecas uz vairākiem IKT produktu ražotājiem vai IKT pakalpojumu sniedzējiem visā Savienībā, katras attiecīgās dalībvalsts izraudzītā CSIRT sadarbojas ar CSIRT tīklu.
2. ENISA izstrādā un uztur Eiropas neaizsargātības reģistru. Šajā nolūkā ENISA izveido un uztur atbilstīgas informācijas sistēmas, politikas nostādnes un procedūras, jo īpaši lai svarīgās un būtiskās vienības un to tīklu un informācijas sistēmu piegādātāji varētu atklāt un reģistrēt neaizsargātību, kas saistīta ar IKT produktiem vai IKT pakalpojumiem, kā arī lai nodrošinātu visām ieinteresētajām personām piekļuvi reģistrā ietvertajai informācijai par neaizsargātību. Reģistrā jo īpaši iekļauj informāciju, kas raksturo neaizsargātību, ietekmēto IKT produktu vai IKT pakalpojumus un neaizsargātības smagumu, proti, apstākļus, kādos to var izmantot, saistītu ielāpu pieejamību un — ja nav pieejamu ielāpu — neaizsargātu produktu lietotājiem adresētus norādījumus par to, kā var mazināt no atklātās neaizsargātības izrietošos riskus.

7. pants

Valstu kiberdrošības krīžu pārvaldības satvari

1. Katra dalībvalsts izraugās vienu vai vairākas kompetentās iestādes, kas atbild par plašapmēra incidentu un krīžu pārvaldību. Dalībvalstis nodrošina, ka kompetentajām iestādēm ir pietiekami resursi, lai efektīvi un lietpratīgi veiktu tām uzticētos uzdevumus.

2. Katra dalībvalsts nosaka spējas, aktīvus un procedūras, ko var izmantot krīzes gadījumā šīs direktīvas nolūkos.
3. Katra dalībvalsts pieņem valsts plānu reaģēšanai uz kibernetikas drošības incidentiem un krīzēm, kurā izklāsta plašāpmēra kibernetikas drošības incidentu un krīžu pārvaldības mērķus un kārtību. Plānā jo īpaši nosaka:
 - a) valsts sagatavotības pasākumu un darbību mērķus;
 - b) valsts kompetento iestāžu uzdevumus un pienākumus;
 - c) krīžu pārvaldības procedūras un informācijas apmaiņas kanālus;
 - d) sagatavotības pasākumus, tostarp vingrinājumus un apmācības darbības;
 - e) attiecīgās iesaistītās publiskās un privātās ieinteresētās personas un infrastruktūru;
 - f) valsts procedūras un pasākumus starp attiecīgajām valsts iestādēm un struktūrām, lai nodrošinātu dalībvalstu efektīvu dalību un atbalstu koordinētā plašāpmēra kibernetikas drošības incidentu un krīžu pārvaldībā Savienības līmenī.
4. Dalībvalstis paziņo Komisijai savas izraudzītās 1. punktā minētās kompetentās iestādes un iesniedz savus 3. punktā minētos valsts plānus reaģēšanai uz kibernetikas drošības incidentiem un krīzēm trīs mēnešu laikā no izraudzīšanās un minēto plānu pieņemšanas. Dalībvalstis var neiekļaut savos plānos konkrētu informāciju, ja un ciktāl tas ir stingri nepieciešams, lai saglabātu valsts drošību.

8. pants

Valstu kompetentās iestādes un vienotie kontaktpunkti

1. Katra dalībvalsts izraugās vienu vai vairākas kompetentās iestādes, kas atbild par kibernetikas drošību un par uzraudzības uzdevumiem, kas minēti šīs direktīvas VI nodaļā. Šim nolūkam dalībvalstis var izraudzīties esošu iestādi vai iestādes.
2. Kompetentās iestādes, kas minētas 1. punktā, uzrauga šīs direktīvas piemērošanu valsts līmenī.
3. Katra dalībvalsts izraugās vienu valsts kontaktpunktu kibernetikas drošības jautājumos ("vienotais kontaktpunkts"). Ja dalībvalsts izraugās tikai vienu kompetento iestādi, minētā kompetentā iestāde ir arī attiecīgās dalībvalsts vienotais kontaktpunkts.
4. Katrs vienotais kontaktpunkts koordinē sadarbību, lai nodrošinātu dalībvalstu iestāžu pārrobežu sadarbību ar attiecīgajām iestādēm citās dalībvalstīs, kā arī lai nodrošinātu starpnozaru sadarbību ar citām valsts kompetentajām iestādēm dalībvalstī.
5. Dalībvalstis nodrošina, ka kompetentajām iestādēm, kas minētas 1. punktā, un vienotajiem kontaktpunktiem ir pietiekami resursi, lai efektīvi un lietpratīgi veiktu tiem uzticētos uzdevumus un tādējādi sasniegtu šīs direktīvas mērķus. Dalībvalstis nodrošina izraudzīto pārstāvju efektīvu, lietpratīgu un drošu sadarbību sadarbības grupā, kas minēta 12. pantā.
6. Katra dalībvalsts nekavējoties paziņo Komisijai izraudzīto kompetento iestādi, kas minēta 1. punktā, un vienoto kontaktpunktu, kas minēts 3. punktā, to uzdevumus un visas turpmākās ar tām saistītās izmaiņas. Katra dalībvalsts publisko izraudzītās iestādes un kontaktpunktus. Komisija publicē izraudzīto vienoto kontaktpunktu sarakstu.

9. pants

Datordrošības incidentu reaģēšanas vienības (CSIRT)

1. Katra dalībvalsts izraugās vienu vai vairākas *CSIRT*, kuras atbilst 10. panta 1. punktā izklāstītajām prasībām, kuru darbība attiecas vismaz uz I un II pielikumā minētajām nozarēm, apakšnozarēm vai vienībām un kuras ir atbildīgas par incidentu risināšanu saskaņā ar labi definētu procesu. *CSIRT* var izveidot kompetentajā iestādē, kas minēta 8. pantā.
2. Dalībvalstis nodrošina, ka katrai *CSIRT* ir pietiekami resursi, lai tās efektīvi pildītu to uzdevumus, kā izklāstīts 10. panta 2. punktā.
3. Dalībvalstis nodrošina, ka katras *CSIRT* rīcībā ir atbilstīga, droša un noturīga sakaru un informācijas infrastruktūra, lai apmainītos ar informāciju ar būtiskajām un svarīgajām vienībām un citām attiecīgajām ieinteresētajām personām. Šajā nolūkā dalībvalstis nodrošina, ka *CSIRT* sniedz ieguldījumu drošu informācijas apmaiņas rīku izmantošanā.
4. *CSIRT* sadarbojas un attiecīgā gadījumā saskaņā ar 26. pantu apmainās ar būtisko informāciju ar būtisko un svarīgo vienību uzticamām nozaru un starpnozaru kopienām.
5. *CSIRT* piedalās salīdzinošajā izvērtēšanā, ko organizē saskaņā ar 16. pantu.
6. Dalībvalstis nodrošina savu *CSIRT* efektīvu, lietpratīgu un drošu sadarbību 13. pantā minētajā *CSIRT* tīklā.
7. Dalībvalstis nekavējoties paziņo Komisijai *CSIRT*, kas izraudzītas saskaņā ar 1. punktu, *CSIRT* koordinatoru, kas izraudzīts saskaņā ar 6. panta 1. punktu, un to attiecīgos uzdevumus, kas paredzēti saistībā ar vienībām, kuras minētas I un II pielikumā.
8. Dalībvalstis var lūgt *ENISA* palīdzību valstu *CSIRT* izveidē.

10. pants

Prasības CSIRT un to uzdevumi

1. *CSIRT* atbilst šādām prasībām:
 - a) *CSIRT* nodrošina savu sakaru pakalpojumu plašu pieejamību, izvairoties no atsevišķu informācijas ķēdes punktu kļūdainas darbības, un tai ir vairāki saziņas līdzekļi, kas jebkurā laikā ļauj ar to sazināties un nodrošina saziņu ar citiem. *CSIRT* skaidri nosaka saziņas kanālus un dara tos zināmus ieinteresētajām personām un sadarbības partneriem;
 - b) *CSIRT* telpas un izmantotās informācijas sistēmas atrodas drošās vietās;
 - c) *CSIRT* ir aprīkotas ar atbilstīgu sistēmu pieprasījumu pārvaldībai un novirzīšanai, jo īpaši lai atvieglotu efektīvu un lietpratīgu nodošanu;
 - d) *CSIRT* ir pietiekams darbinieku skaits, lai nodrošinātu pieejamību jebkurā brīdī;
 - e) *CSIRT* ir nodrošinātas ar rezerves sistēmām un dublēšanas darba telpu, lai nodrošinātu pakalpojumu nepārtrauktību;

- f) *CSIRT* ir iespēja piedalīties starptautiskos sadarbības tīklos.
2. *CSIRT* uzdevumi ir šādi:
- a) kiberdraudu, neaizsargātības un incidentu uzraudzība valsts līmenī;
 - b) agrīnu brīdinājumu, trauksmju, paziņojumu sniegšana un informācijas izplatīšana būtiskajām un svarīgajām vienībām, kā arī citām ieinteresētajām personām par kiberdraudiem, neaizsargātību un incidentiem;
 - c) reaģēšana uz incidentiem;
 - d) dinamiskas risku un incidentu analīzes un situācijas apzināšanas nodrošināšana attiecībā uz kiberdrošību;
 - e) pēc vienības pieprasījuma — to pakalpojumu sniegšanā izmantoto tīklu un informācijas sistēmu proaktīvas skenēšanas nodrošināšana;
 - f) piedalīšanās *CSIRT* tīklā un savstarpējas palīdzības sniegšana citiem tīkla dalībniekiem pēc to lūguma.
3. *CSIRT* nodibina sadarbības attiecības ar attiecīgajiem dalībniekiem privātajā sektorā, lai labāk sasniegtu direktīvas mērķus.
4. Lai veicinātu sadarbību, *CSIRT* veicina vienotas vai standartizētas prakses, klasifikācijas shēmu un taksonomiju pieņemšanu un izmantošanu attiecībā uz:
- a) incidentu risināšanas procedūrām;
 - b) kiberdrošības krīžu pārvaldību;
 - c) koordinētu neaizsargātības atklāšanu.

11. pants

Sadarbība valsts līmenī

1. Vienas un tās pašas dalībvalsts kompetentās iestādes, kas minētas 8. pantā, vienotais kontaktpunkts un *CSIRT* — ja tās ir atsevišķas struktūras — sadarbojas attiecībā uz šajā direktīvā noteikto pienākumu izpildi.
2. Dalībvalstis nodrošina, ka vai nu to kompetentās iestādes, vai arī to *CSIRT* saņem paziņojumus par incidentiem, nozīmīgiem kiberdraudiem un gandrīz notikušiem notikumiem, kurus iesniedz atbilstoši šai direktīvai. Ja dalībvalsts nolemj, ka tās *CSIRT* nesaņem minētos paziņojumus, *CSIRT* — ciktāl tas ir nepieciešams to uzdevumu izpildei — tiek piešķirta piekļuve datiem par incidentiem, kurus paziņojušas būtiskās vai svarīgās vienības atbilstoši 20. pantam.
3. Katra dalībvalsts nodrošina, ka tās kompetentās iestādes vai *CSIRT* informē tās vienoto kontaktpunktu par paziņojumiem, kas attiecas uz incidentiem, nozīmīgiem kiberdraudiem un gandrīz notikušiem notikumiem un kas sniegti atbilstoši šai direktīvai.
4. Ciktāl nepieciešams šajā direktīvā noteikto uzdevumu un pienākumu izpildei, dalībvalstis nodrošina atbilstīgu sadarbību starp kompetentajām iestādēm, vienotajiem kontaktpunktiem un tiesībaizsardzības iestādēm, datu aizsardzības iestādēm un iestādēm, kas atbild par kritiskajām infrastruktūrām atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], un valsts

finanšu iestādēm, kas izraudzītas saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) XXXX/XXXX³⁹ [DORA regula] minētajā dalībvalstī.

5. Dalībvalstis nodrošina, ka to kompetentās iestādes regulāri sniedz informāciju kompetentajām iestādēm, kas izraudzītas saskaņā ar Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], par kiberdrošības riskiem, kiberdraudiem un incidentiem, kas ietekmē būtiskās vienības, kuras identificētas kā kritiskas vai kā vienības, kas ir līdzvērtīgas kritiskām vienībām, atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], kā arī par pasākumiem, ko veikušas kompetentās iestādes, reaģējot uz šādiem riskiem un incidentiem.

III NODAĻA

Sadarbība

12. pants

Sadarbības grupa

1. Lai atbalstītu un veicinātu stratēģisku sadarbību un informācijas apmaiņu starp dalībvalstīm direktīvas piemērošanas jomā, izveido sadarbības grupu.
2. Sadarbības grupa veic savus uzdevumus, pamatojoties uz divgadu darba programmām, kas minētas 6. punktā.
3. Sadarbības grupas sastāvā ir pārstāvji no dalībvalstīm, Komisijas un ENISA. Sadarbības grupas darbībā kā novērotājs piedalās Eiropas Ārējās darbības dienests. Sadarbības grupas darbībā var piedalīties Eiropas uzraudzības iestādes (EUI) saskaņā ar Regulas (ES) XXXX/XXXX [DORA regula] 17. panta 5. punkta c) apakšpunktu.

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

Komisija nodrošina sekretariātu.

4. Sadarbības grupai ir šādi uzdevumi:
 - a) dot norādījumus kompetentajām iestādēm par šīs direktīvas transponēšanu un īstenošanu;
 - b) apmainīties ar paraugpraksi un informāciju saistībā ar šīs direktīvas īstenošanu, arī par kiberdraudiem, incidentiem, neaizsargātību, gandrīz notikušiem notikumiem, izpratnes veicināšanas iniciatīvām, apmācību, vingrinājumiem un prasmēm, spēju veidošanu, kā arī standartiem un tehniskajām specifikācijām;
 - c) apmainīties ar padomiem un sadarboties ar Komisiju jaunu kiberdrošības politikas iniciatīvu jomā;

³⁹

[ierakstīt pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

- d) apmainīties ar padomiem un sadarboties ar Komisiju saistībā ar Komisijas īstenošanas vai deleģēto aktu projektiem, ko pieņem atbilstoši šai direktīvai;
 - e) apmainīties ar paraugpraksi un informāciju ar attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām;
 - f) apspriest ziņojumus par salīdzinošo izvērtēšanu, kas minēti 16. panta 7. punktā;
 - g) apspriest kopējo uzraudzības darbību rezultātus pārrobežu lietās, kā minēts 34. pantā;
 - h) sniegt stratēģiskus norādījumus *CSIRT* tīklam par īpašām jaunām problēmām;
 - i) sniegt ieguldījumu kiberdrošības spējās visā Savienībā, veicinot valsts amatpersonu apmaiņu, īstenojot spēju veidošanas programmu, kurā iesaista darbiniekus no dalībvalstu kompetentajām iestādēm vai *CSIRT*;
 - j) organizēt regulāras kopīgas sanāksmes ar attiecīgajām privātā sektora ieinteresētajām personām visā Savienībā, lai apspriestu grupas veiktās darbības un apkopotu informāciju par jaunām politikas problēmām;
 - k) apspriest darbu, kas veikts saistībā ar kiberdrošības mācībām, tostarp *ENISA* veikto darbu.
5. Sadarbības grupa var pieprasīt no *CSIRT* tīkla tehnisku ziņojumu par atlasītiem tematiem.
 6. Līdz [...] [24 mēneši pēc šīs direktīvas spēkā stāšanās dienas] un pēc tam reizi divos gados sadarbības grupa izstrādā darba programmu par darbībām, kas veicamas, lai īstenotu tās mērķus un uzdevumus. Saskaņā ar šo direktīvu pieņemtās pirmās programmas termiņu pielāgo saskaņā ar Direktīvu (ES) 2016/1148 pieņemtās pēdējās programmas termiņam.
 7. Komisija var pieņemt īstenošanas aktus, ar kuriem nosaka procesuālo kārtību, kas nepieciešama sadarbības grupas darbībai. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 37. panta 2. punktā.
 8. Sadarbības grupa regulāri un vismaz reizi gadā tiekas ar Kritisko vienību noturības grupu, kas izveidota ar Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], lai veicinātu stratēģisko sadarbību un informācijas apmaiņu.

13. pants *CSIRT tīkls*

1. Lai palīdzētu attīstīt palāvību un uzticēšanos un veicinātu ātru un efektīvu operatīvo sadarbību starp dalībvalstīm, tiek izveidots valstu *CSIRT* tīkls.
2. *CSIRT* tīkls sastāv no dalībvalstu *CSIRT* un *CERT-EU* pārstāvjiem. Komisija piedalās *CSIRT* tīklā novērotāja statusā. *ENISA* nodrošina sekretariātu un aktīvi atbalsta sadarbību starp *CSIRT*.
3. *CSIRT* tīklam ir šādi uzdevumi:
 - (a) apmainīties ar informāciju par *CSIRT* spējām;

- (b) apmainīties ar būtisku informāciju par incidentiem, gandrīz notikušiem notikumiem, kiberdraudiem, riskiem un neaizsargātību;
 - (c) ja to lūdz *CSIRT* tīkla pārstāvis, kuru varētu ietekmēt incidents, — apmainīties ar informāciju un apspriest informāciju par attiecīgo incidentu un saistītajiem kiberdraudiem, riskiem un neaizsargātību;
 - (d) pēc *CSIRT* tīkla pārstāvja lūguma apspriest un, ja iespējams, īstenot saskaņotu reaģēšanu uz incidentu, kas ir identificēts attiecīgās dalībvalsts jurisdikcijā;
 - (e) sniegt dalībvalstīm atbalstu pārrobežu incidentu risināšanā atbilstoši šai direktīvai;
 - (f) sadarboties un sniegt palīdzību izraudzītajām *CSIRT*, kas minētas 6. pantā, attiecībā uz tādas daudzpusējas koordinētas neaizsargātības atklāšanas pārvaldību, kura ietekmē vairākus IKT produktu ražotājus vai IKT pakalpojumu sniedzējus un IKT procesu nodrošinātājus, kas nodibināti dažādās dalībvalstīs;
 - (g) apspriest un apzināt operatīvās sadarbības turpmākos veidus, arī attiecībā uz:
 - i) kiberdraudu un incidentu kategorijām;
 - ii) agrīniem brīdinājumiem;
 - iii) savstarpēju palīdzību;
 - iv) koordinēšanas principiem un kārtību, reaģējot uz pārrobežu riskiem un incidentiem;
 - v) ieguldījumu valsts plānā reaģēšanai uz kiberdrošības incidentiem un krīzēm, kas minēts 7. panta 3. punktā;
 - (h) informēt sadarbības grupu par savām darbībām un par operatīvās sadarbības turpmākajiem veidiem, kas apspriesti, ievērojot g) apakšpunktu, nepieciešamības gadījumā lūdzot norādījumus attiecībā uz tiem;
 - (i) apkopot informāciju no kiberdrošības mācībām, tostarp tām, ko organizē *ENISA*;
 - (j) pēc atsevišķas *CSIRT* pieprasījuma apspriest minētās *CSIRT* spējas un sagatavotību;
 - (k) sadarboties un apmainīties ar informāciju ar reģionālajiem un Savienības līmeņa drošības operāciju centriem (*SOC*), lai uzlabotu vienotu situācijas izpratni par incidentiem un draudiem Savienībā;
 - (l) apspriest salīdzinošās izvērtēšanas ziņojumus, kas minēti 16. panta 7. punktā;
 - (m) izdot vadlīnijas, lai atvieglotu operatīvās prakses konvergenci saistībā ar šā panta noteikumu piemērošanu attiecībā uz operatīvo sadarbību.
4. Šīs direktīvas 35. pantā minētās pārskatīšanas nolūkā *CSIRT* tīkls līdz [24 mēneši pēc šīs direktīvas spēkā stāšanās dienas] un pēc tam reizi divos gados novērtē gūto progresu operatīvajā sadarbībā un sagatavo ziņojumu. Ziņojumā izdara secinājumus par rezultātiem, kas gūti 16. pantā minētajā salīdzinošajā izvērtēšanā, kura veikta saistībā ar valstu *CSIRT*, tostarp secinājumus un ieteikumus, kas jāīsteno atbilstoši šim pantam. Minēto ziņojumu iesniedz arī sadarbības grupai.
5. *CSIRT* tīkls sev pieņem reglamentu.

14. pants

Eiropas Kiberkrīžu sadarbības organizāciju tīkls (EU-CyCLONe)

1. Lai atbalstītu plašapmēra kiberdrošības incidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošinātu regulāru informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām un aģentūrām, ar šo tiek izveidots Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*).
2. *EU-CyCLONe* sastāvā ir pārstāvji no dalībvalstu krīžu pārvaldības iestādēm, kas izraudzītas saskaņā ar 7. pantu, Komisijas un *ENISA*. *ENISA* nodrošina tīkla sekretariātu un atbalsta drošu informācijas apmaiņu.
3. *EU-CyCLONe* uzdevumi ir šādi:
 - a) paaugstināt plašapmēra incidentu un krīžu pārvaldības sagatavotības līmeni;
 - b) attīstīt vienotu situācijas izpratni par būtiskajiem kiberdrošības draudiem;
 - c) koordinēt plašapmēra incidentu un krīžu pārvaldību un atbalstīt lēmumu pieņemšanu politiskā līmenī saistībā ar šādiem incidentiem un krīzēm;
 - d) apspriest valstu plānus reaģēšanai uz kiberdrošības incidentiem un krīzēm, kas minēti 7. panta 2. punktā.
4. *EU-CyCLONe* sev pieņem reglamentu.
5. *EU-CyCLONe* regulāri ziņo sadarbības grupai par kiberdraudiem, incidentiem un tendencēm, īpaši pievēršoties to ietekmei uz būtiskajām un svarīgajām vienībām.
6. *EU-CyCLONe* sadarbojas ar *CSIRT* tīklu, pamatojoties uz saskaņotu procesuālo kārtību.

15. pants

Ziņojums par situāciju kiberdrošības jomā Savienībā

1. *ENISA*, sadarbojoties ar Komisiju, izdod divgadu ziņojumu par situāciju kiberdrošības jomā Savienībā. Ziņojumā īpaši iekļauj novērtējumu par:
 - (a) kiberdrošības spēju attīstību Savienībā;
 - (b) tehniskajiem un finansiālajiem resursiem un cilvēkresursiem, kas pieejami kompetentajām iestādēm, un kiberdrošības politikas nostādņēm, un uzraudzības pasākumu un izpildes darbību īstenošanu, ņemot vērā 16. pantā minētās salīdzinošās izvērtēšanas rezultātus;
 - (c) kiberdrošības rādītāju, kas paredz saskaņotu novērtējumu par kiberdrošības spēju brieduma līmeni.
2. Ziņojumā iekļauj īpašus politiskus ieteikumus kiberdrošības līmeņa paaugstināšanai Savienībā un konstatējumu kopsavilkumu par attiecīgo periodu no aģentūras ES kiberdrošības tehniskās situācijas ziņojumiem, ko izdevusi *ENISA* saskaņā ar Regulas (ES) 2019/881 7. panta 6. punktu.

16. pants

Salīdzinošā izvērtēšana

1. Komisija pēc apspriešanās ar sadarbības grupu un *ENISA*, vēlākais, 18 mēnešus pēc šīs direktīvas stāšanās spēkā nosaka salīdzinošās izvērtēšanas sistēmas metodiku un saturu dalībvalstu kiberdrošības politikas efektivitātes novērtēšanai. Izvērtēšanu veic kiberdrošības tehniskie eksperti no dalībvalstīm, kas nav dalībvalsts, par kuru tiek veikta izvērtēšana, un tajā aplūko vismaz šādus aspektus:
 - i) 18. un 20. pantā minēto kiberdrošības riska pārvaldības prasību un ziņošanas pienākumu īstenošanas efektivitāte;
 - ii) spēju līmenis, ieskaitot pieejamos finansiālos un tehniskos resursus un cilvēkresursus, un valsts kompetento iestāžu uzdevumu izpildes efektivitāte;
 - iii) *CSIRT* operatīvās spējas un efektivitāte;
 - iv) 34. pantā minētās savstarpējās palīdzības efektivitāte;
 - v) šīs direktīvas 26. pantā minētā informācijas apmaiņas satvara efektivitāte.
2. Metodika ietver objektīvus, nediskriminējošus, taisnīgus un pārredzamus kritērijus, uz kuru pamata dalībvalstis izraugās ekspertus, kas ir tiesīgi veikt salīdzinošo izvērtēšanu. *ENISA* un Komisija izraugās ekspertus, kuri piedalās salīdzinošajā izvērtēšanā novērotāja statusā. Komisija ar *ENISA* atbalstu 1. punktā minētajā metodikā nosaka objektīvu, nediskriminatīvu, taisnīgu un pārredzamu sistēmu ekspertu atlasei un piešķiršanai nejaušības kārtā katrai salīdzinošajai izvērtēšanai.
3. Par salīdzinošās izvērtēšanas organizatoriskajiem aspektiem izlemj Komisija, kuru atbalsta *ENISA*, pēc apspriešanās ar sadarbības grupu un pamatojoties uz kritērijiem, kas noteikti 1. punktā minētajā metodikā. Salīdzinošajā izvērtēšanā novērtē 1. punktā minētos aspektus attiecībā uz visām dalībvalstīm un nozarēm, tostarp mērķtiecīgiem jautājumiem, kas īpaši skar vienu vai vairākas dalībvalstis vai vienu vai vairākas nozares.
4. Salīdzinošā izvērtēšana ietver faktiskus vai virtuālus apmeklējumus klātienē un apmaiņu no tālienes. Ievērojot labas sadarbības principu, dalībvalstis, par kurām tiek veikta izvērtēšana, sniedz izraudzītajiem ekspertiem prasīto informāciju, kas nepieciešama pārskatīto aspektu novērtēšanai. Visu salīdzinošās izvērtēšanas procesa laikā iegūto informāciju izmanto tikai šim mērķim. Eksperti, kuri piedalās salīdzinošajā izvērtēšanā, neizpauž trešām personām sensitīvu vai konfidenciālu informāciju, kas iegūta izvērtēšanas laikā.
5. Vienus un tos pašus aspektus pēc to izvērtēšanas dalībvalstī turpmāk vairs neizvērtē tajā pašā dalībvalstī divus gadus pēc salīdzinošās izvērtēšanas noslēgšanas, ja Komisija, apspriežoties ar *ENISA* un sadarbības grupu, nenolemj citādi.
6. Dalībvalstis nodrošina, ka katrs interešu konflikta risks saistībā ar izraudzītajiem ekspertiem tiek nekavējoties darīts zināms pārējām dalībvalstīm, Komisijai un *ENISA*.
7. Eksperti, kuri piedalās salīdzinošajā izvērtēšanā, sagatavo ziņojumus par izvērtēšanas konstatējumiem un secinājumiem. Ziņojumus iesniedz Komisijai, sadarbības grupai, *CSIRT* tīklam un *ENISA*. Ziņojumus apspriež sadarbības grupā un *CSIRT* tīklā. Ziņojumus var publicēt sadarbības grupas specializētajā tīmekļa vietnē.

IV NODAĻA

Kiberdrošības riska pārvaldības un ziņošanas pienākumi

I IEDAĻA

Kiberdrošības riska pārvaldība un ziņošana

17. pants

Pārvalde

1. Dalībvalstis nodrošina, ka būtisko un svarīgo vienību pārvaldes struktūras apstiprina kiberdrošības riska pārvaldības pasākumus, ko veic minētās vienības, lai izpildītu 18. panta prasības, pārtrauga to īstenošanu un atbild, ja vienības neizpilda šajā pantā noteiktos pienākumus.
2. Dalībvalstis nodrošina, ka pārvaldības struktūras locekļi regulāri apgūst īpašu apmācību, kurā iegūst pietiekamas zināšanas un prasmes, lai izprastu un novērtētu kiberdrošības riskus un pārvaldības praksi, kā arī to ietekmi uz vienības darbībām.

18. pants

Kiberdrošības riska pārvaldības pasākumi

1. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības veic atbilstīgus un samērīgus tehniskos un organizatoriskos pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmu drošībai, ko tās izmanto savu pakalpojumu sniegšanā. Ņemot vērā jaunākos tehniskos sasniegumus, ar minētajiem pasākumiem nodrošina radītajam riskam atbilstošu tīklu un informācijas sistēmu drošības līmeni.
2. Pasākumos, kas minēti 1. punktā, ietver vismaz:
 - (a) riska analīzes un informācijas sistēmu drošības politiku;
 - (b) incidentu risināšanu (incidentu novēršana, atklāšana un reaģēšana uz tiem);
 - (c) darbības nepārtrauktības un krīžu pārvaldību;
 - (d) piegādes ķēdes drošību, tostarp ar drošību saistītus aspektus, kas skar attiecības starp katru vienību un tās piegādātājiem vai pakalpojumu sniedzējiem, piemēram, datu uzglabāšanas un apstrādes pakalpojumu vai pārvaldītas drošības pakalpojumu sniedzējiem;
 - (e) drošību tīklu un informācijas sistēmu ieguvē, attīstīšanā un uzturēšanā, tostarp rīcību neaizsargātības gadījumā un atklāšanā;
 - (f) politikas nostādnes un procedūras (testēšanu un revīziju), lai novērtētu kiberdrošības riska pārvaldības pasākumu efektivitāti;
 - (g) kriptogrāfijas un šifrēšanas izmantošanu.

3. Dalībvalstis nodrošina, ka, apsverot atbilstīgus pasākumus, kas minēti 2. punkta d) apakšpunktā, vienības ņem vērā neaizsargātību, kas raksturīga katram piegādātājam un pakalpojumu sniedzējam, un to piegādātāju un pakalpojumu sniedzēju produktu vispārējo kvalitāti un kiberdrošības praksi, ieskaitot to drošās attīstības procedūras.
4. Dalībvalstis nodrošina, ka tad, ja vienība konstatē, ka attiecīgi tās pakalpojumi vai uzdevumi neatbilst 2. punktā noteiktajām prasībām, tā nekavējoties veic visus nepieciešamos korektīvos pasākumus, lai nodrošinātu attiecīgā pakalpojuma atbilstību.
5. Komisija var pieņemt īstenošanas aktus, lai noteiktu 2. punktā minēto elementu tehniskās un metodiskās specifikācijas. Sagatavojot minētos aktus, Komisija rīkojas saskaņā ar pārbaudes procedūru, kas minēta 37. panta 2. punktā, un, ciktāl iespējams, ievēro starptautiskos un Eiropas standartus, kā arī attiecīgās tehniskās specifikācijas.
6. Komisija ir pilnvarota pieņemt deleģētos aktus saskaņā ar 36. pantu, lai papildinātu 2. punktā noteiktos elementus nolūkā ņemt vērā jaunus kiberdraudus, tehnoloģiju attīstību vai nozaru specifiku.

19. pants

ES koordinētie kritisko piegādes ķēžu riska novērtējumi

1. Sadarbības grupa kopā ar Komisiju un ENISA var veikt īpašu kritisku IKT pakalpojumu, sistēmu vai produktu piegādes ķēžu koordinētus drošības riska novērtējumus, ņemot vērā tehniskus un attiecīgā gadījumā netehniskus riska faktorus.
2. Komisija pēc apspriešanās ar sadarbības grupu un ENISA identificē īpašos kritiskos IKT pakalpojumus, sistēmas vai produktus, par kuriem var veikt 1. punktā minēto koordinēto riska novērtējumu.

20. pants

Ziņošanas pienākumi

1. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās paziņo kompetentajām iestādēm vai CSIRT saskaņā ar 3. un 4. punktu par ikvienu incidentu, kam ir būtiska ietekme uz to pakalpojumu sniegšanu. Attiecīgā gadījumā minētās vienības bez nepamatotas kavēšanās informē savus pakalpojumu saņēmējus par incidentiem, kas varētu nelabvēlīgi ietekmēt konkrētā pakalpojuma sniegšanu. Dalībvalstis nodrošina, ka minētās vienības cita starpā paziņo visu informāciju, kas ļauj kompetentajām iestādēm vai CSIRT noteikt incidenta pārrobežu ietekmi.
2. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās informē kompetentās iestādes vai CSIRT par visiem nozīmīgajiem kiberdraudiem, ko minētās vienības identificējušas kā tādas, kuri būtu varējuši izraisīt nozīmīgu incidentu.

Attiecīgā gadījumā minētās vienības bez nepamatotas kavēšanās informē savus pakalpojumu saņēmējus, kurus varētu skart ievērojami kiberdraudi, par visiem pasākumiem vai tiesiskās aizsardzības līdzekļiem, ko minētie saņēmēji var veikt,

reaģējot uz konkrētajiem draudiem. Attiecīgā gadījumā vienības arī informē minētos saņēmējus par pašiem draudiem. Paziņošana neuzliek ziņotājai vienībai lielāku atbildību.

3. Incidentu uzskata par nozīmīgu, ja:
 - (a) incidents ir izraisījis vai var izraisīt ievērojamu darbības traucējumu vai finansiālus zaudējumus attiecīgajai vienībai;
 - (b) incidents ir ietekmējis vai var ietekmēt citas fiziskas vai juridiskas personas, izraisot ievērojamus materiālus vai nemateriālus zaudējumus.
4. Dalībvalstis nodrošina, ka 1. punktā noteiktās paziņošanas nolūkos attiecīgās vienības iesniedz kompetentajām iestādēm vai *CSIRT*:
 - (a) bez nepamatotas kavēšanās un katrā ziņā 24 stundu laikā no brīža, kad uzzinājušas par incidentu, — sākotnēju paziņojumu, kurā attiecīgā gadījumā norāda, vai incidentu ir izraisījusi, domājams, nelikumīga vai ļaunprātīga rīcība;
 - (b) pēc kompetentās iestādes vai *CSIRT* pieprasījuma — starpposma ziņojumu par attiecīgajiem statusa atjauninājumiem;
 - (c) galīgu ziņojumu ne vēlāk kā mēnesi pēc a) apakšpunktā minētā ziņojuma iesniegšanas, tajā iekļaujot vismaz:
 - i) incidenta, tā smaguma un ietekmes sīku aprakstu;
 - ii) draudu veidu vai pamatcēloni, kas varētu būt izraisījis incidentu;
 - iii) piemērotos un notiekošos riska mazināšanas pasākumus.

Dalībvalstis nodrošina, ka pienācīgi pamatotos gadījumos un pēc vienošanās ar kompetentajām iestādēm vai *CSIRT* attiecīgā vienība var atkāpties no a) un c) apakšpunktā noteiktajiem termiņiem.

5. Valsts kompetentās iestādes vai *CSIRT* 24 stundu laikā no 4. punkta a) apakšpunktā minētā sākotnējā paziņojuma saņemšanas sniedz ziņotājai vienībai atbildi, kurā iekļauj sākotnējo atgriezenisko saiti par incidentu un — pēc vienības pieprasījuma — norādījumus par iespējamo riska mazināšanas pasākumu īstenošanu. Ja *CSIRT* nesaņem 1. un 2. punktā minēto paziņojumu, minētos norādījumus sniedz kompetentā iestāde, sadarbojoties ar *CSIRT*. Ja attiecīgā vienība lūdz papildu tehnisko atbalstu, *CSIRT* to sniedz. Ja ir aizdomas, ka incidents ir noziedzīgs, valsts kompetentās iestādes vai *CSIRT* arī dod norādījumus par incidenta paziņošanu tiesībsargsardzības iestādēm.
6. Attiecīgā gadījumā, īpaši tad, ja 1. punktā minētais incidents skar divas vai vairākas dalībvalstis, kompetentā iestāde vai *CSIRT* informē citas skartās dalībvalstis un *ENISA* par incidentu. To darot, kompetentās iestādes, *CSIRT* un vienotie kontaktpunkti saskaņā ar Savienības tiesību aktiem vai valsts tiesību aktiem, kas atbilst Savienības tiesību aktiem, nodrošina vienības drošību un komerciālās intereses, kā arī sniegtās informācijas konfidencialitāti.
7. Ja ir nepieciešams informēt sabiedrību, lai novērstu incidentu vai risinātu notiekošu incidentu, vai incidenta atklāšana citādi ir sabiedrības interesēs, kompetentā iestāde vai *CSIRT* un attiecīgā gadījumā citu iesaistīto dalībvalstu kompetentās iestādes vai *CSIRT* pēc apspriešanās ar attiecīgo vienību informē sabiedrību par incidentu vai pieprasa, lai to dara vienība.

8. Pēc kompetentās iestādes vai *CSIRT* pieprasījuma vienotais kontaktpunkts nosūta atbilstoši 1. un 2. punktam saņemtos paziņojumus citu skarto dalībvalstu vienotajiem kontaktpunktiem.
9. Vienotais kontaktpunkts reizi mēnesī iesniedz *ENISA* kopsavilkuma ziņojumu, kurā iekļauj anonimizētus un apkopotus datus par incidentiem, nozīmīgiem kiberdraudiem un gandrīz notikušiem notikumiem, par kuriem paziņots saskaņā ar 1. un 2. punktu un 27. pantu. Lai veicinātu salīdzināmas informācijas sniegšanu, *ENISA* var izdot tehniskus norādījumus par kopsavilkuma ziņojumā iekļautās informācijas parametriem.
10. Kompetentās iestādes kompetentajām iestādēm, kuras izraudzītas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], sniedz informāciju par incidentiem un kiberdraudiem, ko saskaņā ar 1. un 2. punktu paziņojušas būtiskās vienības, kas identificētas kā kritiskas vienības, vai vienības, kas ir līdzvērtīgas kritiskajām vienībām, atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva].
11. Komisija var pieņemt īstenošanas aktus, kuros sīkāk nosaka atbilstoši 1. un 2. punktam iesniegtajā ziņojumā iekļaujamās informācijas veidu, ziņojuma formātu un paziņošanas procedūru. Komisija var pieņemt īstenošanas aktus, lai precizētu, kuros gadījumos incidentu uzskata par nozīmīgu, kā minēts 3. punktā. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 37. panta 2. punktā.

21. pants

Eiropas kiberdrošības sertifikācijas shēmu izmantošana

1. Lai pierādītu atbilstību konkrētām 18. panta prasībām, dalībvalstis var pieprasīt, lai būtiskās un svarīgās vienības sertificē konkrētus IKT produktus, IKT pakalpojumus un IKT procesus atbilstoši īpašām Eiropas kiberdrošības sertifikācijas shēmām, kas pieņemtas saskaņā ar Regulas (ES) 2019/881 49. pantu. Produktus, pakalpojumus un procesus, uz kuriem attiecas sertifikācija, var izstrādāt būtiska vai svarīga vienība, vai tos var iepirkt no trešām personām.
2. Komisija ir pilnvarota pieņemt deleģētus aktus, ar ko nosaka, kurām būtisko vienību kategorijām ir jāsaņem sertifikāts un atbilstoši kurām īpašajām Eiropas kiberdrošības sertifikācijas shēmām saskaņā ar 1. punktu. Deleģētos aktus pieņem saskaņā ar 36. pantu.
3. Komisija var pieprasīt, lai gadījumos, kad nav pieejama neviena atbilstīga Eiropas kiberdrošības sertifikācijas shēma 2. punkta nolūkos, *ENISA* sagatavo kandidātshēmu atbilstoši Regulas (ES) 2019/881 48. panta 2. punktam.

22. pants

Standartizācija

1. Lai sekmētu 18. panta 1. un 2. punkta konverģentu īstenošanu, dalībvalstis, neliekot izmantot konkrētu tehnoloģijas veidu un nediskriminējot par labu tā izmantošanai, veicina tādu Eiropas vai starptautiski atzītu standartu un specifikāciju izmantošanu, kas ir atbilstīgi tīklu un informācijas sistēmu drošībai.

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

23. pants

Domēnu nosaukumu un reģistrācijas datu datubāzes

1. Lai veicinātu DNS drošību, stabilitāti un noturību, dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, ar pienācīgu rūpību savāc un uztur precīzus un pilnīgus domēnu nosaukumu reģistrācijas datus speciālā datubāzē, ievērojot Savienības datu aizsardzības tiesību aktus par datiem, kas ir persondati.
2. Dalībvalstis nodrošina, ka 1. punktā minētajās domēnu nosaukumu reģistrācijas datu datubāzēs ir ietverta attiecīga informācija, kas ļauj identificēt domēnu nosaukumu turētājus un kontaktpunktus, kuri pārvalda ALD nosaukumus, un sazināties ar tiem.
3. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, ir ieviesuši politiku un procedūras, lai nodrošinātu, ka datubāzēs ir iekļauta precīza un pilnīga informācija. Dalībvalstis nodrošina, ka šāda politika un procedūras tiek publiskotas.
4. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, bez nepamatotas kavēšanās pēc domēna nosaukuma reģistrācijas publicē domēnu reģistrācijas datus, kas nav persondati.
5. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, sniedz leģitīmiem piekļuves prasītājiem pēc to likumīgiem un pienācīgi pamatotiem pieprasījumiem piekļuvi īpašiem domēnu nosaukumu reģistrācijas datiem, ievērojot Savienības datu aizsardzības tiesību aktus. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, bez nepamatotas kavēšanās atbild uz visiem piekļuves pieprasījumiem. Dalībvalstis nodrošina, ka politika un procedūras šādu datu izpaušanai tiek publiskotas.

II iedaļa

Jurisdikcija un reģistrācija

24. pants

Jurisdikcija un teritorialitāte

1. DNS pakalpojumu sniedzējus, ALD nosaukumu reģistrus, mākoņpakalpojumu sniedzējus, datu centru pakalpojumu sniedzējus un satura piegādes tīklu nodrošinātājus, kas minēti I pielikuma 8. punktā, kā arī digitālo pakalpojumu sniedzējus, kas minēti II pielikuma 6. punktā, uzskata par tādiem, kas ir tās dalībvalsts jurisdikcijā, kurā atrodas to galvenā darbījumbāzes vieta Savienībā.
2. Šīs direktīvas nolūkos vienības, kas minētas 1. punktā, uzskata par tādām, kuru galvenā darbījumbāzes vieta Savienībā ir tajā dalībvalstī, kurā tiek pieņemti

lēmumi saistībā ar kiberdrošības riska pārvaldības pasākumiem. Ja šādi lēmumi netiek pieņemti darījumdarbības vietā Savienībā, uzskata, ka galvenā darījumdarbības vieta ir dalībvalstī, kurā vienībām ir darījumdarbības vieta ar vislielāko darbinieku skaitu Savienībā.

3. Ja 1. punktā minētajai vienībai nav darījumdarbības vietas Savienībā, bet tā piedāvā pakalpojumus Savienībā, tā izraugās pārstāvi Savienībā. Minētajam pārstāvim darījumdarbības vieta ir vienā no dalībvalstīm, kurās tiek piedāvāti pakalpojumi. Uzskata, ka šāda vienība ir tās dalībvalsts jurisdikcijā, kurā ir pārstāvja darījumdarbības vieta. Ja nav izraudzīta pārstāvja Savienībā atbilstoši šim pantam, jebkura dalībvalsts, kurā vienība sniedz pakalpojumus, var veikt tiesiskas darbības pret vienību sakarā ar neatbilstību šajā direktīvā noteiktajiem pienākumiem.
4. Vienības veiktā pārstāvja izraudzīšanās, kā minēts 1. punktā, neskar tiesiskās darbības, ko var ierosināt pret pašu vienību.

25. pants

Būtisko un svarīgo vienību reģistrs

1. *ENISA* izveido un uztur 24. panta 1. punktā minēto būtisko un svarīgo vienību reģistru. Vienības līdz [12 mēneši pēc šīs direktīvas stāšanās spēkā] iesniedz *ENISA* šādu informāciju:
 - (a) vienības nosaukums;
 - (b) tās galvenās darījumdarbības vietas adrese un tās citu darījumdarbības vietu adrese Savienībā vai, ja vienībai nav darījumdarbības vietas Savienībā, atbilstoši 24. panta 3. punktam izraudzītā tās pārstāvja darījumdarbības vietas adrese Savienībā;
 - (c) jaunākā kontaktinformācija, ieskaitot vienību e-pasta adreses un tālruna numurus.
2. Vienības, kas minētas 1. punktā, informē *ENISA* par visām izmaiņām informācijā, ko tās iesniegušas atbilstoši 1. punktam, nekavējoties un katrā ziņā trīs mēnešu laikā no attiecīgo izmaiņu stāšanās spēkā.
3. Saņemot informāciju atbilstoši 1. punktam, *ENISA* to nosūta vienotajiem kontaktpunktiem atkarībā no norādītās katras vienības galvenās darījumdarbības vietas vai, ja tai nav darījumdarbības vietas Savienībā, tās izraudzītā pārstāvja darījumdarbības vietas. Ja vienībai, kas minēta 1. punktā, papildus tās galvenajai darījumdarbības vietai Savienībā ir arī citas darījumdarbības vietas citās dalībvalstīs, *ENISA* informē arī šo dalībvalstu vienotos kontaktpunktus.
4. Ja vienība neregistrē savu darbību vai neiesniedz attiecīgo informāciju 1. punktā noteiktajā termiņā, jebkura dalībvalsts, kurā vienība sniedz pakalpojumus, ir kompetenta nodrošināt, ka attiecīgā vienība izpilda šajā direktīvā noteiktos pienākumus.

V NODAĻA

Informācijas apmaiņa

26. pants

Kiberdrošības informācijas apmaiņas pasākumi

1. Neskarot Regulu (ES) 2016/679, dalībvalstis nodrošina, ka būtiskās un svarīgās vienības var savstarpēji apmainīties ar būtisku kiberdrošības informāciju, ieskaitot informāciju, kas attiecas uz kiberdraudiem, neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem, ja šāda informācijas apmaiņa:
 - (a) ir paredzēta, lai novērstu vai atklātu incidentus vai reaģētu uz tiem, vai mazinātu to riskus;
 - (b) veicina kiberdrošības līmeni, it īpaši – palielinot informētību attiecībā uz kiberdraudiem, ierobežojot vai traucējot kiberdraudu izplatīšanos, atbalstot virkni aizsardzības spēju, neaizsargātības izlabošanu un atklāšanu, draudu atklāšanas metodes, seku mazināšanas stratēģijas vai reaģēšanas un seku novēršanas posmus.
2. Dalībvalstis nodrošina, ka informācijas apmaiņa notiek būtisko un svarīgo vienību uzticamās kopienās. Šādu apmaiņu īsteno, veicot informācijas apmaiņas pasākumus attiecībā uz informācijas iespējami sensitīvo raksturu un saskaņā ar 1. punktā minētajām Savienības tiesību aktu normām.
3. Dalībvalstis pieņem noteikumus, kuros precizē 2. punktā minēto informācijas apmaiņas pasākumu procedūru, operatīvos elementus (tostarp speciālu IKT platformu izmantošanu), saturu un nosacījumus. Šādos noteikumos arī sīkāk apraksta publisku iestāžu iesaistīšanos šādos pasākumos, kā arī operatīvos elementus, tostarp speciālu IT platformu izmantošanu. Dalībvalstis piedāvā atbalstu šādu pasākumu piemērošanā atbilstoši to politikas nostādņēm, kas minētas 5. panta 2. punkta g) apakšpunktā.
4. Būtiskās un svarīgās vienības informē kompetentās iestādes par savu dalību 2. punktā minētajos informācijas apmaiņas pasākumos, tiklīdz tās iesaistās šādos pasākumos, vai attiecīgā gadījumā — par izstāšanos no šādas dalības, tiklīdz izstāšanās stājas spēkā.
5. Ievērojot Savienības tiesību aktus, ENISA atbalsta 2. punktā minēto kiberdrošības informācijas apmaiņas pasākumu izveidi, nodrošinot paraugpraksi un sniedzot norādījumus.

27. pants

Būtiskas informācijas brīvprātīga paziņošana

Dalībvalstis nodrošina, ka, neskarot 3. pantu, vienības, uz kurām neattiecas šīs direktīvas darbības joma, var brīvprātīgi iesniegt paziņojumus par nozīmīgiem incidentiem, kiberdraudiem vai gandrīz notikušiem notikumiem. Apstrādājot paziņojumus, dalībvalstis rīkojas saskaņā ar 20. pantā noteikto procedūru. Dalībvalstis obligātos paziņojumus var apstrādāt, nosakot tiem prioritāti pār brīvprātīgajiem paziņojumiem. Brīvprātīgās paziņošanas

rezultātā ziņotājai vienībai netiek uzlikti nekādi papildu pienākumi, kas uz to neattiektos, ja tā nebūtu iesniegusi minēto paziņojumu.

VI NODAĻA

Uzraudzība un izpilde

28. pants

Vispārīgi uzraudzības un izpildes aspekti

1. Dalībvalstis nodrošina, ka kompetentās iestādes efektīvi uzrauga atbilstību šai direktīvai, it īpaši 18. un 20. pantā noteiktajiem pienākumiem, un veic nepieciešamos pasākumus, lai nodrošinātu atbilstību tiem.
2. Pievēršoties incidentiem, kuru rezultātā notiek persondatu aizsardzības pārkāpumi, kompetentās iestādes strādā ciešā sadarbībā ar datu aizsardzības iestādēm.

29. pants

Uzraudzība un izpilde attiecībā uz būtiskajām vienībām

1. Dalībvalstis nodrošina, ka uzraudzības vai izpildes pasākumi, kas noteikti būtiskajām vienībām attiecībā uz šajā direktīvā noteiktajiem pienākumiem, ir iedarbīgi, samērīgi un atturoši, ņemot vērā katra atsevišķa gadījuma apstākļus.
2. Dalībvalstis nodrošina, ka kompetentajām iestādēm, kad tās īsteno savus uzraudzības uzdevumus attiecībā uz būtiskajām vienībām, ir pilnvaras piemērot minētajām vienībām:
 - a) pārbaudes uz vietas un attālinātu uzraudzību, arī pārbaudes izlases veidā;
 - b) regulāru revīziju;
 - c) mērķtiecīgas drošības revīzijas, kas balstītas uz riska novērtējumiem vai ar risku saistītu pieejamo informāciju;
 - d) drošības skenēšanu, pamatojoties uz objektīviem, nediskriminējošiem, taisnīgiem un pārredzamiem riska novērtēšanas kritērijiem;
 - e) tādas informācijas pieprasījumus, kas nepieciešama, lai novērtētu vienības pieņemtos kiberdrošības pasākumus, tostarp dokumentētas kiberdrošības politikas nostādnes, kā arī atbilstību pienākumam informēt ENISA atbilstoši 25. panta 1. un 2. punktam;
 - f) pieprasījumus, lai piekļūtu datiem, dokumentiem vai jebkurai informācijai, kas nepieciešama to uzraudzības pienākumu izpildei;
 - g) pieprasījumus par pierādījumiem, ka tiek īstenotas kiberdrošības politikas nostādnes, piemēram, kvalificēta revidenta veikto drošības revīziju rezultātiem un attiecīgajiem pamatpierādījumiem.
3. Īstenojot savas pilnvaras atbilstoši 2. punkta e)–g) apakšpunktam, kompetentās iestādes norāda pieprasījuma mērķi un precizē prasīto informāciju.

4. Dalībvalstis nodrošina, ka kompetentajām iestādēm, īstenojot izpildes procedūras attiecībā uz būtiskajām vienībām, ir šādas pilnvaras:
- (a) izdot brīdinājumus par vienību neatbilstību šajā direktīvā noteiktajiem pienākumiem;
 - (b) izdot saistošus norādījumus vai rīkojumu, pieprasot, lai minētās vienības izlabo konstatētos trūkumus vai šajā direktīvā noteikto pienākumu pārkāpumus;
 - (c) uzdot minētajām iestādēm izbeigt rīcību, kas nav saderīga ar šajā direktīvā noteiktajiem pienākumiem, un atturēties no tādas rīcības atkārtošanas;
 - (d) uzdot minētajām vienībām nodrošināt savu riska pārvaldības pasākumu un/vai ziņošanas pienākumu atbilstību 18. un 20. pantā paredzētajiem noteikumiem noteiktā veidā un termiņā;
 - (e) uzdot minētajām vienībām informēt fizisko(-ās) vai juridisko(-ās) personu(-as), kam tās sniedz pakalpojumus vai veic darbības, kuras var ietekmēt nozīmīgi kibernetiskie draudi, par visiem iespējamajiem aizsardzības vai izlabošanas pasākumiem, ko attiecīgā(-ās) fiziskā(-ās) vai juridiskā(-ās) persona(-as) var veikt, reaģējot uz šādiem draudiem;
 - (f) uzdot minētajām vienībām saprātīgā termiņā īstenot ieteikumus, kas sniegti drošības revīzijas rezultātā;
 - (g) norīkot uzraudzības speciālistu, kam ir labi definēti uzdevumi, noteiktā laikposmā pārraudzīt atbilstību 18. un 20. pantā paredzētajiem pienākumiem;
 - (h) uzdot minētajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos vērojama neatbilstība šajā direktīvā noteiktajiem pienākumiem;
 - (i) sniegt publisku paziņojumu, kurā norāda fizisko(-ās) un juridisko(-ās) personu(-as), kas atbild par šajā direktīvā noteikta pienākuma pārkāpumu, un par attiecīgā pārkāpuma raksturu;
 - (j) piemērot — vai pieprasīt, lai attiecīgās struktūras vai tiesas piemēro — saskaņā ar valsts tiesību aktiem administratīvu naudas sodu atbilstoši 31. pantam, tādējādi papildinot vai aizstājot pasākumus, kas minēti šā punkta a)–i) apakšpunktā, atkarībā no katra atsevišķa gadījuma apstākļiem.
5. Ja izrādās, ka izpildes darbības, kas pieņemtas atbilstoši 4. punkta a)–d) un f) apakšpunktam, ir neefektīvas, dalībvalstis nodrošina, ka kompetentajām iestādēm ir pilnvaras noteikt termiņu, līdz kuram būtiskajai vienībai ir jāveic nepieciešamā rīcība, lai izlabotu trūkumus vai izpildītu minēto iestāžu prasības. Ja pieprasītā darbība netiek veikta noteiktajā termiņā, dalībvalstis nodrošina, ka kompetentajām iestādēm ir šādas pilnvaras:
- (a) apturēt — vai pieprasīt, lai sertifikācijas vai apstiprināšanas struktūra aptur — sertifikāciju vai atļauju attiecībā uz visiem būtiskās vienības sniegtajiem pakalpojumiem vai veiktajām darbībām vai to daļu;
 - (b) piemērot — vai pieprasīt, lai attiecīgās struktūras vai tiesas piemēro — saskaņā ar valsts tiesību aktiem pagaidu aizliegumu jebkurai personai, kura īsteno vadības pienākumus galvenās izpildpersonas vai juridiskā pārstāvja līmenī minētajā vienībā, un jebkurai citai fiziskai personai, kura ir atbildīga par pārkāpumu, īstenojot vadības funkcijas konkrētajā vienībā.

Šīs sankcijas piemēro tikai līdz brīdim, kad vienība veic nepieciešamo darbību, lai izlabotu trūkumus vai izpildītu kompetentās iestādes prasības, attiecībā uz kurām šādas sankcijas piemērotas.

6. Dalībvalstis nodrošina, ka jebkurai fiziskai personai, kura atbild par būtisko vienību vai rīkojas kā būtiskās vienības pārstāve, pamatojoties uz pilnvarām to pārstāvēt, pilnvarām pieņemt lēmumus tās vārdā vai pilnvarām īstenot kontroli pār to, ir pilnvaras nodrošināt vienības atbilstību šajā direktīvā noteiktajiem pienākumiem. Dalībvalstis nodrošina, ka minētās fiziskās personas var tikt sauktas pie atbildības, ja viņas pārkāpj savus pienākumus nodrošināt atbilstību šajā direktīvā noteiktajiem pienākumiem.
7. Veicot jebkuru no izpildes darbībām vai piemērojot jebkuru no sankcijām atbilstoši 4. un 5. punktam, kompetentās iestādes ievēro aizstāvības tiesības un ņem vērā katra atsevišķā gadījuma apstākļus, un vismaz pienācīgi ņem vērā:
 - (a) pārkāpuma nopietnumu un pārkāpto noteikumu svarīgumu. Pārkāpumi, kas jāuzskata par nopietniem, cita starpā ir šādi: atkārtoti pārkāpumi, tādu incidentu nepaziņošana vai neizlabošana, kam ir ievērojama traucējumu izraisošā ietekme, trūkumu neizlabošana saskaņā ar kompetento iestāžu saistošiem norādījumiem, šķēršļu likšana revīzijām vai uzraudzības darbībām, ko uzdevusi kompetentā iestāde pēc pārkāpuma konstatēšanas, nepatiesas vai ļoti neprecīzas informācijas sniegšana saistībā ar riska pārvaldības prasībām vai ziņošanas pienākumiem, kas noteikti 18. un 20. pantā;
 - (b) pārkāpumu ilgumu, tostarp atkārtotu pārkāpumu elementu;
 - (c) izraisīto faktisko kaitējumu vai radušos zaudējumus, vai iespējamo kaitējumu vai zaudējumus, kas būtu varējuši rasties, ciktāl tos var noteikt. Izvērtējot šo aspektu, cita starpā ņem vērā faktiskos vai iespējamos finansiālos vai ekonomiskos zaudējumus, ietekmi uz citiem pakalpojumiem, skarto vai iespējami skarto lietotāju skaitu;
 - (d) to, vai pārkāpums izdarīts tīši vai neuzmanības dēļ;
 - (e) pasākumus, ko vienība veikusi, lai novērstu vai mazinātu kaitējumu un/vai zaudējumus;
 - (f) apstiprinātu rīcības kodeksu vai apstiprinātu sertifikācijas mehānismu ievērošanu;
 - (g) to, cik lielā mērā pie atbildības sauktā(-ās) fiziskā(-ās) vai juridiskā(-ās) persona(-as) sadarbojas ar kompetentajām iestādēm.
8. Kompetentās iestādes sīki argumentē savus izpildes lēmumus. Pirms šādu lēmumu pieņemšanas kompetentās iestādes informē attiecīgās vienības par saviem sākotnējiem konstatējumiem un atvēl vienībām saprātīgu termiņu apsvērumu iesniegšanai.
9. Dalībvalstis nodrošina, ka to kompetentās iestādes, kad tās īsteno savas uzraudzības un izpildes pilnvaras, kuru mērķis ir nodrošināt, lai būtiska vienība, kas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva] identificēta kā kritiska, vai vienība, kas ir līdzvērtīga kritiskai vienībai, ievērotu šajā direktīvā noteiktos pienākumus, informē attiecīgās kompetentās iestādes citā dalībvalstī, kuras izraudzītas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva]. Ja to pieprasa kompetentās iestādes atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], kompetentās

iestādes var īstenot savas uzraudzības un izpildes pilnvaras attiecībā uz būtisku vienību, kas identificēta kā kritiska vai kritiskai līdzvērtīga vienība.

30. pants

Uzraudzība un izpilde attiecībā uz svarīgām vienībām

1. Saņemot pierādījumus vai norādes par to, ka svarīga vienība neizpilda šajā direktīvā un jo īpaši tās 18. un 20. pantā noteiktos pienākumus, dalībvalstis nodrošina, ka kompetentās iestādes rīkojas, nepieciešamības gadījumā īstenojot pēcuzraudzības pasākumus.
2. Dalībvalstis nodrošina, ka kompetentajām iestādēm, kad tās īsteno savus uzraudzības uzdevumus attiecībā uz svarīgām vienībām, ir pilnvaras piemērot minētajām vienībām:
 - (a) pārbaudes uz vietas un attālinātu pēcuzraudzību;
 - (b) mērķtiecīgas drošības revīzijas, kas balstītas uz riska novērtējumiem vai ar risku saistītu pieejamo informāciju;
 - (c) drošības skenēšanu, pamatojoties uz objektīviem, taisnīgiem un pārredzamiem riska novērtēšanas kritērijiem;
 - (d) tādas informācijas pieprasījumus, kas nepieciešama, lai novērtētu veiktos kiberdrošības pasākumus, tostarp dokumentētas kiberdrošības politikas nostādnes, kā arī atbilstību pienākumam informēt *ENISA* atbilstoši 25. panta 1. un 2. punktam;
 - (e) pieprasījumus, lai piekļūtu datiem, dokumentiem un/vai informācijai, kas nepieciešama uzraudzības pienākumu izpildei.
3. Īstenojot savas pilnvaras atbilstoši 2. punkta d) vai e) apakšpunktam, kompetentās iestādes norāda pieprasījuma mērķi un precizē prasīto informāciju.
4. Dalībvalstis nodrošina, ka kompetentajām iestādēm, īstenojot savas izpildes procedūras attiecībā uz svarīgām vienībām, ir šādas pilnvaras:
 - (a) izdot brīdinājumus par vienību neatbilstību šajā direktīvā noteiktajiem pienākumiem;
 - (b) izdot saistošus norādījumus vai rīkojumu, pieprasot, lai minētās vienības izlabo konstatētos trūkumus vai šajā direktīvā noteikto pienākumu pārkāpumu;
 - (c) uzdot minētajām iestādēm izbeigt rīcību, kas nav saderīga ar šajā direktīvā noteiktajiem pienākumiem, un atturēties no tādas rīcības atkārtēšanas;
 - (d) uzdot minētajām vienībām nodrošināt savu riska pārvaldības pasākumu vai ziņošanas pienākumu atbilstību 18. un 20. pantā paredzētajiem noteikumiem noteiktā veidā un termiņā;
 - (e) uzdot minētajām vienībām informēt fizisko(-ās) vai juridisko(-ās) personu(-as), kam tās sniedz pakalpojumus vai veic darbības, kuras var ietekmēt nozīmīgi kiberdraudi, par visiem iespējamajiem aizsardzības vai izlabošanas pasākumiem, ko attiecīgā(-ās) fiziskā(-ās) vai juridiskā(-ās) persona(-as) var veikt, reaģējot uz šādiem draudiem;

- (f) uzdot minētajām vienībām saprātīgā termiņā īstenot ieteikumus, kas sniegti drošības revīzijas rezultātā;
 - (g) uzdot minētajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos vērojama neatbilstība šajā direktīvā noteiktajiem to pienākumiem;
 - (h) sniegt publisku paziņojumu, kurā norāda fizisko(-ās) un juridisko(-ās) personu(-as), kas atbild par šajā direktīvā noteikta pienākuma pārkāpumu, un par attiecīgā pārkāpuma raksturu;
 - (i) piemērot — vai pieprasīt, lai attiecīgās struktūras vai tiesas piemēro — saskaņā ar valsts tiesību aktiem administratīvu naudas sodu atbilstoši 31. pantam, tādējādi papildinot vai aizstājot pasākumus, kas minēti šā punkta a)–h) apakšpunktā, atkarībā no katra atsevišķa gadījuma apstākļiem.
5. Uzraudzības un izpildes pasākumiem, kas paredzēti šajā pantā attiecībā uz II pielikumā uzskaitītajām svarīgajām vienībām, piemēro arī 29. panta 6.–8. punktu.

31. pants

Vispārīgi nosacījumi administratīvo naudas sodu piemērošanai būtiskajām un svarīgajām vienībām

1. Dalībvalstis nodrošina, ka administratīvo naudas sodu piemērošana būtiskajām un svarīgajām vienībām atbilstoši šim pantam saistībā ar šajā direktīvā noteikto pienākumu pārkāpumiem katrā atsevišķā gadījumā ir iedarbīga, samērīga un atturoša.
2. Administratīvos naudas sodus atkarībā no katra individuālā gadījuma apstākļiem piemēro, ar tiem papildinot vai aizstājot pasākumus, kas minēti 29. panta 4. punkta a)–i) apakšpunktā, 29. panta 5. punktā un 30. panta 4. punkta a)–h) apakšpunktā.
3. Izlemjot, vai piemērot administratīvu naudas sodu, un lemjot par tā summu, katrā individuālā gadījumā pienācīgi ņem vērā vismaz 29. panta 7. punktā paredzētos elementus.
4. Dalībvalstis nodrošina, ka par 18. vai 20. pantā noteikto pienākumu pārkāpumiem saskaņā ar šā panta 2. un 3. punktu piemēro administratīvu naudas sodu līdz ne vairāk kā 10 000 000 EUR vai 2 % no tā uzņēmuma kopējā apgrozījuma visā pasaulē, pie kura pieder būtiskā vai svarīgā vienība, iepriekšējā finanšu gadā atkarībā no tā, kura no summām ir lielāka.
5. Dalībvalstis var paredzēt pilnvaras piemērot periodiskus soda maksājumus, lai būtiskajai vai svarīgajai vienībai liktu izbeigt pārkāpumu, saskaņā ar kompetentās iestādes iepriekšēju lēmumu.
6. Neskarot 29. un 30. pantā noteiktās kompetento iestāžu pilnvaras, katra dalībvalsts var pieņemt noteikumus par to, vai un līdz kādam apjomam administratīvos naudas sodus var piemērot valsts pārvaldes vienībām, kas minētas 4. panta 23. punktā, ievērojot šajā direktīvā paredzētos pienākumus.

32. pants

Pārkāpumi, kas ietver persondatu aizsardzības pārkāpumu

1. Ja kompetentajām iestādēm ir sniegtas norādes, ka būtiskas vai svarīgas vienības izdarīts 18. un 20. pantā noteikto pienākumu pārkāpums ietver persondatu aizsardzības pārkāpumu, kas definēts Regulas (ES) 2016/679 4. panta 12. punktā un ko paziņo atbilstoši minētās regulas 33. pantam, tās saprātīgā termiņā informē uzraudzības iestādes, kas ir kompetentas atbilstoši minētās regulas 55. un 56. pantam.
2. Ja uzraudzības iestādes, kas ir kompetentas saskaņā ar Regulas (ES) 2016/679 55. un 56. pantu, nolemj īstenot savas pilnvaras atbilstoši minētās regulas 58. panta i) punktam un piemērot administratīvu naudas sodu, kompetentās iestādes nepiemēro administratīvu naudas sodu par to pašu pārkāpumu atbilstoši šīs direktīvas 31. pantam. Tomēr kompetentās iestādes var piemērot izpildes darbības vai īstenot sankciju piemērošanas pilnvaras, kas paredzētas šīs direktīvas 29. panta 4. punkta a)–i) apakšpunktā, 29. panta 5. punktā un 30. panta 4. punkta a)–h) apakšpunktā.
3. Ja uzraudzības iestāde, kas ir kompetenta atbilstoši Regulai (ES) 2016/679, veic darbību citā dalībvalstī, kas nav kompetentās iestādes dalībvalsts, kompetentā iestāde var informēt uzraudzības iestādi, kas veic darbību minētajā dalībvalstī.

33. pants

Sodi

1. Dalībvalstis paredz noteikumus par sodiem, kas piemērojami par to valsts tiesību normu pārkāpumiem, kuras pieņemtas, ievērojot šo direktīvu, un veic visus nepieciešamos pasākumus, lai nodrošinātu to piemērošanu. Paredzētie sodi ir iedarbīgi, samērīgi un atturoši.
2. Dalībvalstis, vēlākais, [divus] gadus pēc šīs direktīvas stāšanās spēkā informē Komisiju par minētajiem noteikumiem un pasākumiem un bez nepamatotas kavēšanās informē to par visiem turpmākajiem grozījumiem, kas tos skar.

34. pants

Savstarpēja palīdzība

1. Ja būtiska vai svarīga vienība sniedz pakalpojumus vairāk nekā vienā dalībvalstī vai ja tās galvenā darbījumbūvības vieta vai pārstāvis ir vienā dalībvalstī, bet tās tīklu un informācijas sistēmas atrodas vienā vai vairākās citās dalībvalstīs, tās dalībvalsts kompetentā iestāde, kurā atrodas galvenā uzņēmējdarbības vieta vai cita darbījumbūvības vieta, vai pārstāvis, un minēto citu dalībvalstu kompetentās iestādes sadarbojas un pēc vajadzības cita citai palīdz. Minētā sadarbība ietver vismaz turpmāk minēto:
 - (a) kompetentās iestādes, kas piemēro uzraudzības vai izpildes pasākumus dalībvalstī, ar vienotā kontaktpunkta starpniecību informē un konsultē pārējo attiecīgo dalībvalstu kompetentās iestādes par veiktajiem uzraudzības un izpildes pasākumiem un pēcpasākumiem saskaņā ar 29. un 30. pantu;
 - (b) kompetentā iestāde vai pieprasīt, lai cita kompetentā iestāde veic 29. un 30. pantā minētos uzraudzības vai izpildes pasākumus;
 - (c) kompetentā iestāde, saņemot pamatotu lūgumu no citas kompetentās iestādes, sniedz otrai kompetentajai iestādei palīdzību, lai 29. un 30. pantā minētos

uzraudzības vai izpildes pasākumus varētu īstenot efektīvi, iedarbīgi un konsekventi. Šāda savstarpējā palīdzība var ietvert informācijas pieprasījumus un uzraudzības pasākumus, tostarp pieprasījumus veikt pārbaudes uz vietas vai attālinātu uzraudzību, vai mērķtiecīgas drošības revīzijas. Kompetentā iestāde, kam adresēts lūgums sniegt palīdzību, nedrīkst atteikt palīdzību, ja vien pēc informācijas apmaiņas ar pārējām attiecīgajām iestādēm, ENISA un Komisiju netiek konstatēts, ka vai nu iestāde nav kompetenta sniegt lūgto palīdzību, vai arī lūgtā palīdzība nav samērīga ar kompetentās iestādes uzraudzības uzdevumiem, ko veic saskaņā ar 29. vai 30. pantu.

2. Attiecīgā gadījumā un pēc kopīgas vienošanās kompetentās iestādes no dažādām dalībvalstīm var veikt kopīgas uzraudzības darbības, kas minētas 29. un 30. pantā.

VII NODAĻA

Pārejas un nobeiguma noteikumi

35. pants

Pārskatīšana

Komisija periodiski pārskata šīs direktīvas darbību un iesniedz ziņojumu Eiropas Parlamentam un Padomei. Ziņojumā galvenokārt novērtē I un II pielikumā minēto nozaru, apakšnozaru un vienību lieluma un veida nozīmīgumu ekonomikas darbībai un sabiedrībai saistībā ar kibers drošību. Šim nolūkam un lai turpinātu attīstīt stratēģisko un operatīvo sadarbību, Komisija ņem vērā sadarbības grupas un CSIRT tīkla ziņojumus par stratēģiskā un operatīvā līmenī gūto pieredzi. Pirmo ziņojumu iesniedz līdz (..) [54 mēneši pēc šīs direktīvas spēkā stāšanās dienas].

36. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.
2. Pilnvaras pieņemt 18. panta 6. punktā un 21. panta 2. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no (..).
3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 18. panta 6. punktā un 21. panta 2. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar spēkā jau esošos deleģētos aktus.
4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar ekspertiem, kurus katra dalībvalsts izraudzījusi saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.
5. Tiklīdz Komisija pieņem deleģēto aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

6. Saskaņā ar 18. panta 6. punktu un 21. panta 2. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

37. pants

Komiteju procedūra

1. Komisijai palīdz komiteja. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 nozīmē.
2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.
3. Ja komitejas atzinums ir jāsaņem rakstiskā procedūrā, šādu procedūru beidz bez rezultāta, ja atzinuma sniegšanai noteiktajā termiņā tā nolemj komitejas priekšsēdētājs vai to pieprasa kāds komitejas loceklis.

38. pants

Transponēšana

1. Dalībvalstis līdz (..) [18 mēneši pēc šīs direktīvas spēkā stāšanās dienas] pieņem un publicē normatīvos un administratīvos aktus, kas nepieciešami šīs direktīvas prasību izpildei. Dalībvalstis tūlīt dara zināmu Komisijai minēto noteikumu tekstu. Tās piemēro minētos aktus no (..) [nākamā diena pēc pirmajā daļā minētā datuma].
2. Kad dalībvalstis pieņem minētos aktus, tajos iekļauj atsauci uz šo direktīvu vai arī šādu atsauci pievieno to oficiālajai publikācijai. Dalībvalstis nosaka metodes, kā izdarāma šāda atsauce.

39. pants

Grozījums Regulā (ES) Nr. 910/2014

Regulas (ES) Nr. 910/2014 19. pantu svīturo.

40. pants

Grozījums Direktīvā (ES) 2018/1972

Direktīvas (ES) 2018/1972 40. un 41. pantu svīturo.

41. pants

Atcelšana

Direktīva (ES) 2016/1148 tiek atcelta no (..) [direktīvas transponēšanas termiņa datums].

Atsauces uz Direktīvu (ES) 2016/1148 uzskata par atsaucēm uz šo direktīvu un lasa saskaņā ar III pielikumā sniegto atbilstības tabulu.

42. pants

Stāšanās spēkā

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

43. pants

Adresāti

Šī direktīva ir adresēta dalībvalstīm.

Briselē,

*Eiropas Parlamenta vārdā —
priekšsēdētājs*

*Padomes vārdā —
priekšsēdētājs*

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

Satura rādītājs

1.	PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS	2
1.1.	Priekšlikuma/iniciatīvas nosaukums	2
1.2.	Attiecīgā(-ās) rīcībpolitikas joma(-as) (<i>programmu kopums</i>).....	2
1.3.	Priekšlikums/iniciatīva attiecas uz:	2
1.4.	Priekšlikuma/iniciatīvas pamatojums	2
1.4.1.	Īstermiņā vai ilgtermiņā izpildāmās vajadzības, kā arī detalizēts iniciatīvas izvēršanas grafiks.....	2
1.4.2.	Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka efektivitāte vai papildinājums). Šajā punktā “Savienības iesaistīšanās pievienotā vērtība” ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.	2
1.4.3.	Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas.....	3
1.4.4.	Saderība un iespējamā sinerģija ar citiem atbilstošiem instrumentiem	3
1.5.	Ilgums un finansiālā ietekme	4
1.6.	Plānotais(-ie) pārvaldības veids(-i)	4
2.	PĀRVALDĪBAS PASĀKUMI.....	6
2.1.	Uzraudzības un ziņošanas noteikumi	6
2.2.	Pārvaldības un kontroles sistēma(-as).....	6
2.2.1.	Ierosinātā(-o) pārvaldības veida(-u), finansējuma apgūšanas mehānisma, maksāšanas kārtības un kontroles stratēģijas pamatojums	6
2.2.2.	Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto(-ajām) iekšējās kontroles sistēmu(-ām).....	6
2.2.3.	Pārbaužu izmaksas un to lietderības pamatojums (attiecība “kontroles izmaksas ÷ attiecīgo pārvaldīto fondu vērtība”), un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas un programmas slēgšanas brīdī)	6
2.3.	Krāpšanas un pārkāpumu novēršanas pasākumi	6
3.	PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME	7
3.1.	Daudzgaļu finanšu shēmas izdevumu kategorijas un ierosinātās jaunās budžeta izdevumu pozīcijas.....	7
3.2.	Aplēstā ietekme uz izdevumiem	8
3.2.1.	Kopsavilkums par paredzamo ietekmi uz izdevumiem	8
3.2.2.	Paredzamā ietekme uz administratīvajām apropriācijām.....	11
3.2.3.	Trešo personu iemaksas	13
3.3.	Aplēstā ietekme uz ieņēmumiem	13

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Priekšlikums "Direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148".

1.2. Attiecīgā(-ās) rīcībpolitikas joma(-as) (*programmu kopums*)

Sakaru tīkli, saturs un tehnoloģija

1.3. Priekšlikums/iniciatīva attiecas uz:

☐ jaunu darbību

☐ jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību⁴⁰

☒ esošas darbības pagarināšanu

☐ vienas vai vairāku darbību apvienošanu vai pārorientēšanu uz citu/jaunu darbību

1.4. Priekšlikuma/iniciatīvas pamatojums

1.4.1. *Īstermiņā vai ilgtermiņā izpildāmās vajadzības, kā arī detalizēts iniciatīvas izvērtēšanas grafiks*

Pārskatīšanas mērķis ir paaugstināt kibernetikas līmeni uzņēmumu, kas darbojas Eiropas Savienībā visās attiecīgajās nozarēs, visaptverošam kopumam, mazināt noturības atšķirības visā iekšējā tirgū nozarēs, uz kurām jau attiecas direktīva, un uzlabot kopējās izpratnes par situāciju līmeni un kolektīvo spēju sagatavoties un reaģēt.

1.4.2. *Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka efektivitāte vai papildinājums). Šajā punktā "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.*

Kiberdrošības noturība visā Savienībā nevar būt efektīva, ja attiecībā uz to tiek īstenotas atšķirīgas valstu vai reģionu pieejas. TID direktīva pievērsās šim trūkumam, nosakot satvaru tīklu un informācijas sistēmu drošībai valstu un Savienības līmenī. Tomēr TID direktīvas pirmajā periodiskajā pārskatīšanā tika konstatētas vairākas raksturīgas nepilnības, kas galu galā ir novedušas pie ievērojām atšķirībām starp dalībvalstīm spēju, plānošanas un aizsardzības līmeņa ziņā, kuras tajā pašā laikā ietekmē vienlīdzīgus konkurences apstākļus līdzīgiem uzņēmumiem iekšējā tirgū.

ES iesaistīšanos, kas pārsniedz pašreizējos TID direktīvas pasākumus, pamato galvenokārt šādi faktori: i) problēmas pārrobežu raksturs; ii) iespēja, ka ar ES rīcību tiks uzlabota un veicināta efektīva valstu politika; iii) saskaņotu un sadarbīgu TID politikas darbību ieguldījums efektīvā datu un privātuma aizsardzībā.

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

⁴⁰

Kā norādīts Finanšu regulas 58. panta 2. punkta a) vai b) apakšpunktā.

1.4.3. *Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas*

TID direktīva ir pirmais horizontālais iekšējā tirgus instruments, kura mērķis ir uzlabot tīklu un sistēmu noturību Savienībā pret kiberdrošības riskiem. Tā jau ir ievērojami veicinājusi vispārējā kiberdrošības līmeņa paaugstināšanos dalībvalstīs. Tomēr direktīvas darbības un īstenošanas pārskatīšanā tika konstatētas vairākas nepilnības, kas papildus pieaugošajai digitalizācijai un vajadzībai pēc faktiskajai situācijai atbilstošas reaģēšanas ir jārisina pārskatītā tiesību instrumentā.

1.4.4. *Saderība un iespējamā sinerģija ar citiem atbilstošiem instrumentiem*

Jaunais priekšlikums ir pilnībā saderīgs un saskaņots ar citām saistītām iniciatīvām, piemēram, priekšlikumu regulai par finanšu sektora digitālās darbības noturību (“DORA”) un priekšlikumu direktīvai par pamatpakalpojumu kritisko sniedzēju noturību. Tas ir arī saderīgs ar Eiropas Elektronisko sakaru kodeksu, Vispārīgo datu aizsardzības regulu un eIDAS regulu.

Priekšlikums ir ES Drošības savienības stratēģijas būtiska daļa.

1.5. Ilgums un finansiālā ietekme

☐ ierobežots ilgums

- ☐ darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.
- ☐ Finansiālā ietekme uz saistību apropriācijām — no GGGG. līdz GGGG. gadam, uz maksājumu apropriācijām — no GGGG. līdz GGGG. gadam.

☒ beztermiņa

- Īstenošana ar uzsākšanas periodu no 2022. līdz 2025. gadam,
- pēc kura turpinās normāla darbība.

1.6. Plānotais(-ie) pārvaldības veids(-i)⁴¹

Komisijas tieša pārvaldība,

- ☒ ko veic tās struktūrvienības, tostarp personāls Savienības delegācijās;
- ☐ ko veic izpildaģentūras.

☐ Dalīta pārvaldība kopā ar dalībvalstīm

☐ Netieša pārvaldība, uzticot budžeta izpildes uzdevumus:

- ☐ trešām valstīm vai to izraudzītām struktūrām;
- ☐ starptautiskām organizācijām un to aģentūrām (precizēt);
- ☐ EIB un Eiropas Investīciju fondam;
- ☒ Finanšu regulas 70. un 71. pantā minētajām struktūrām;
- ☐ publisko tiesību subjektiem;
- ☐ privāttiesību subjektiem, kas veic valsts pārvaldes uzdevumus, ja tie sniedz pienācīgas finanšu garantijas;
- ☐ struktūrām, kuru darbību reglamentē dalībvalsts privāttiesības, kurām ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuras sniedz pienācīgas finansiālas garantijas;
- ☐ personām, kurām ir uzticēts veikt īpašas darbības KĀDP saskaņā ar Līguma par Eiropas Savienību V sadaļu un kuras ir noteiktas attiecīgā pamataktā.
- *Ja norādīti vairāki pārvaldības veidi, iedaļā "Piezīmes" sniedziet papildu informāciju.*

Piezīmes

Eiropas Savienības Kiberdrošības aģentūra (ENISA), kam ar Kiberdrošības aktu ir uzticēts jauns pastāvīgs pilnvarojums, palīdzēs dalībvalstīm un Komisijai pārskatītās TID direktīvas īstenošanā.

Pārskatītās TID direktīvas rezultātā no 2022./2023. gada ENISA būs papildu rīcības jomas. Lai gan uz šīm rīcības jomām attieksies ENISA vispārējie uzdevumi atbilstoši tās pilnvarojumam, tās aģentūrai radīs papildu darba slodzi. Konkrētāk, papildus tās pašreizējām rīcības jomām atbilstoši Komisijas priekšlikumam par pārskatītu TID direktīvu ENISA savā darba programmā cita starpā būs arī jāiekļauj šādas darbības: i) izveidot un uzturēt Eiropas neaizsargātības reģistru (priekšlikuma 6. panta 2. punkts), ii) nodrošināt Eiropas Kiberkrīžu

⁴¹

Skaidrojumus par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt BudgWeb tīmekļa vietnē:
<https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>

sadarbības organizāciju tīklu (*CyCLONe*) (priekšlikuma 14. pants) un izdot gada ziņojumu par situāciju kibernetikas jomā ES (priekšlikuma 15. pants), iii) atbalstīt salīdzinošās izvērtēšanas organizēšanu starp dalībvalstīm (priekšlikuma 16. pants), iv) savākt apkopotus incidentu datus no dalībvalstīm un izdot tehniskus norādījumus (priekšlikuma 20. panta 9. punkts), v) izveidot un uzturēt to vienību reģistru, kuras sniedz pārrobežu pakalpojumus (priekšlikuma 25. pants).

Tāpēc no 2022. gada tiks pieprasīti pieci papildu pilnslodzes ekvivalenti (FTE) ar atbilstošo budžetu aptuveni 0,61 miljons gadā, lai finansētu šīs jaunās amata vietas (sk. atsevišķu finanšu pārskatu par aģentūrām).

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

Norādīt periodiskumu un nosacījumus.

Komisija periodiski pārskatīs direktīvas darbību un ziņos Eiropas Parlamentam un Padomei, pirmo reizi – trīs gadus pēc tās stāšanās spēkā.

Komisija arī novērtēs, vai dalībvalstīs direktīva tiek transponēta pareizi.

2.2. Pārvaldības un kontroles sistēma(-as)

2.2.1. *Ierosinātā(-o) pārvaldības veida(-u), finansējuma apgūšanas mehānisma, maksāšanas kārtības un kontroles stratēģijas pamatojums*

CNECT ĢD struktūrvienība, kas atbild par attiecīgās politikas jomu, pārvaldīs direktīvas īstenošanu.

2.2.2. *Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto(-ajām) iekšējās kontroles sistēmu(-ām)*

Ļoti zems risks, jo TID direktīvas ekosistēma jau pastāv.

2.2.3. *Pārbaužu izmaksas un to lietderības pamatojums (attiecība “kontroles izmaksas ÷ attiecīgo pārvaldīto fondu vērtība”), un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas un programmas slēgšanas brīdī)*

Neattiecas. Izmanto tikai administratīvo budžetu (vispārīgās apropriācijas)

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt pašreizējos vai paredzētos novēršanas un aizsardzības pasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.

Neattiecas. Izmanto tikai administratīvo budžetu (vispārīgās apropriācijas)

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Daudzgaļu finanšu shēmas izdevumu kategorijas un ierosinātās jaunās budžeta izdevumu pozīcijas

Daudzgaļu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Numurs [Pozīcija...7.....]]	Dif./nedif. ⁴²	no EBTA valstīm ⁴³	no kandidātvalstīm ⁴⁴	no trešām valstīm	Finanšu regulas [21. panta 2. punkta b) apakšpunkta] nozīmē
	20 02 06 pārvaldības izdevumi 20 02 06	Nedif.	NĒ	NĒ	NĒ	NĒ

⁴² Diff. = Dif. — diferencētās apropriācijas / Nedif. — nediferencētās apropriācijas.

⁴³ EBTA — Eiropas Brīvās tirdzniecības asociācija.

⁴⁴ Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

3.2. Aplēstā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

Miljonos EUR (līdz 3 zīmēm aiz komata)

Daudz gadu finanšu shēmas izdevumu kategorija	<...>	[Pozīcija.....]
--	-------	-----------------

			2021	2022	2023	2024	2025	2026	2027	Pēc 2027. gada	KOPĀ
Darbības apropriācijas (sadalījumā pa budžeta pozīcijām atbilstoši 3.1. punktam)	Saistības	1)									
	Maksājumi	2)									
Administratīvās apropriācijas, ko finansē no programmas piešķirumiem ⁴⁵	Saistības = Maksājumi	3)									
KOPĀ apropriācijas — programmas piešķirums	Saistības	=1+3									
	Maksājumi	=2+3									

Daudz gadu finanšu shēmas izdevumu kategorija	7	“Administratīvie izdevumi”. Sanāksmes: TID sadarbības grupas plenārsēdes parasti notiek četras reizes gadā. Komisija sedz 27 dalībvalstu pārstāvju ēdināšanas un ceļa izdevumus (viens pārstāvis no katras DV). Vienas sēdes izmaksas var sasniegt 15 000 EUR. Komandējumi: komandējumi ir saistīti ar TID direktīvas īstenošanas uzraudzību. Piemērs. Vienā gadā (2019. gada maijs–2020. gada jūlijs) bija jāorganizē tā dēvētie “TID valstu apmeklējumi” un jāapmeklē visas 27 DV, lai apspriestu TID direktīvas
--	---	---

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

		īstenošanu ES.
--	--	----------------

Šī iedaļa jāaizpilda, izmantojot administratīva rakstura budžeta datu izklājlapu, kas vispirms jānoformē [Tiesību akta finanšu pārskata pielikumā](#), kas starpdienestu konsultāciju vajadzībām ir augšupielādēts *DECIDE* sistēmā.

Miljonos EUR (līdz 3 zīmēm aiz komata)

		2021	2022	2023	2024	2025	2026	2027	Pēc 2027. g ada	KOPĀ
Cilvēkresursi		1,14	1,14	1,14	1,14	1,14	1,14	1,14		7,98
Citi administratīvie izdevumi		0,09	0,09	0,09	0,09	0,09	0,09	0,09		0,63
KOPĀ — daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS apropriācijas	(Saistību summa = maksājumu summa)	1,23	1,23	1,23	1,23	1,23	1,23	1,23		8,61

Miljonos EUR (līdz 3 zīmēm aiz komata)

		2021	2022	2023	2024	2025	2026	2027	Pēc 2027. g ada	KOPĀ
KOPĀ daudzgadu finanšu shēmas visu IZDEVUMU KATEGORIJU apropriācijas	Saistības									
	Maksājumi									

3.2.2. Paredzamā ietekme uz administratīvajām apropriācijām

- ☐ Priekšlikums/iniciatīva neparedz administratīvo apropriāciju izmantošanu
- ☒ Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādi:

Miljonos EUR (līdz 3 zīmēm aiz komata)

Gads	2021	2022	2023	2024	2025	2026	2027	KOPĀ
------	------	------	------	------	------	------	------	------

Daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJA								
Cilvēkresursi	1,14	1,14	1,14	1,14	1,14	1,14	1,14	7,98
Citi administratīvie izdevumi	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63
Ārpus daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61

Ārpus daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS ⁴⁶								
Cilvēkresursi								
Citi administratīvie izdevumi								
Starpsumma – ārpus daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS								

KOPĀ	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------

Vajadzīgās cilvēkresursu un citu administratīvo izdevumu apropriācijas tiks nodrošinātas no ĢD apropriācijām, kas jau piešķirtas darbības pārvaldībai un/vai pārdalītas attiecīgajā ģenerāldirektorātā, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

⁴⁶

Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās “BA” pozīcijas), netiešā pētniecība, tiešā pētniecība.

3.2.2.1. Paredzamās vajadzības pēc cilvēkresursiem

- ☐ Priekšlikums/iniciatīva neparedz cilvēkresursu izmantošanu.
- ☒ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Aplēse izsakāma ar pilnslodzes ekvivalentu

Gads	2021	2022	2023	2024	2025	2026	2027
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)							
Galvenā mītne un Komisijas pārstāvniecības	6	6	6	6	6	6	6
Delegācijas							
Pētniecība							
• Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu — FTE) — AC, AL, END, INT un JPD⁴⁷							
7. kategorija							
Finansēts no daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS	– galvenajā mītnē	3	3	3	3	3	3
	– delegācijās						
Finansēts no programmas piešķiruma ⁴⁸	– galvenajā mītnē						
	– delegācijās						
Pētniecība							
Cits (konkretizēt)							
KOPĀ		9	9	9	9	9	9

Vajadzīgie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau iesaistīti konkrētās darbības pārvaldībā un/vai pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts

Ierēdņi un pagaidu darbinieki	- Deleģēto aktu sagatavošana saskaņā ar 18. panta 6. punktu, 21. panta 2. punktu, 36. pantu; - Īstenošanas aktu sagatavošana saskaņā ar 12. panta 8. punktu, 18. panta 5. punktu, 20. panta 11. punktu; - sekretariāta nodrošināšana TID sadarbības grupai; - TID sadarbības grupas plenārsēžu un darba straumēšanas sanāksmju organizēšana; - dalībvalstu darba koordinēšana saistībā ar dažādiem dokumentiem (pamatnostādnes, rīkkopas utt.); - sadarbība ar citiem Komisijas dienestiem, ENISA un valsts iestādēm, lai īstenotu TID direktīvu; - ar TID direktīvas īstenošanu saistīto valsts metožu un paraugprakses analīze.
Ārštata darbinieki	Pēc vajadzības sniegt atbalstu visos minētajos uzdevumos

⁴⁷ AC – līgumdarbinieki, AL – vietējie darbinieki, END – valstu norīkotie eksperti, INT – aģentūru darbinieki, JPD – jaunākie speciālisti delegācijās.

⁴⁸ Ārštata darbiniekiem paredzētā maksimālā summa, ko finansē no darbības apropriācijām (kādreizējām “BA” pozīcijām).

3.2.3. Trešo personu iemaksas

Priekšlikums/iniciatīva:

- ☒ neparedz līdzfinansējumu no trešām personām
- ☐ paredz šādu līdzfinansējumu no trešām personām:

Apropriācijas miljonos EUR (līdz 3 zīmēm aiz komata)

Gads	2021	2022	2023	2024	2025	2026	2027	KOPĀ
Norādīt līdzfinansētāju struktūru								
KOPĀ līdzfinansētās apropriācijas								

3.3. Aplēstā ietekme uz ieņēmumiem

- ☒ Priekšlikums/iniciatīva ieņēmumus finansiāli neietekmē.
- ☐ Priekšlikums/iniciatīva finansiāli ietekmē:
 - ☐ pašu resursus
 - ☐ citus ieņēmumus

Norādiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām ☐

Miljonos EUR (līdz 3 zīmēm aiz komata)

Budžeta pozīcija: ieņēmumu	Priekšlikuma/iniciatīvas ietekme ⁴⁹						
	2021	2022	2023	2024	2025	2026	2027
..... pants							

Attiecībā uz piešķirtajiem ieņēmumiem norādīt attiecīgo(-ās) budžeta izdevumu pozīciju(-as).

Citas piezīmes (piemēram, ietekmes uz ieņēmumiem aprēķināšanas metode/formula vai jebkāda cita informācija).

⁴⁹ Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATA **PIELIKUMS**

Priekšlikuma/iniciatīvas nosaukums:

priekšlikums "Direktīva, ar ko pārskata Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā"

1. **PAR VAJADZĪGIEM UZSKATĪTO CILVĒKRESURSU SKAITS un IZMAKSAS**
2. **CITU ADMINISTRATĪVO IZDEVUMU IZMAKSAS**
3. **IZMAKSU APLĒŠANĀ IZMANTOTĀS APRĒĶINU METODES**
 - 3.1. **Cilvēkresursi**
 - 3.2. **Citi administratīvie izdevumi**

Sākot starpdienestu apspriešanos, šis pielikums, kas jāaizpilda katram ģenerāldirektorātam/dienestam, kurš piedalās priekšlikumā/iniciatīvā, jāpievieno tiesību akta priekšlikuma finanšu pārskatam.

Datu tabulas tiek izmantotas par avotu tiesību akta priekšlikuma finanšu pārskatā iekļautajām tabulām. Tās paredzētas tikai un vienīgi Komisijas iekšējai lietošanai.

1. Par vajadzīgiem uzskatīto cilvēkresursu izmaksas

☐ Priekšlikums/iniciatīva neparedz cilvēkresursu izmantošanu

☒ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Miljonos EUR (līdz 3 zīmēm aiz komata)

Daudzgaļu finanšu shēmas 7. IZDEVUMU KATEGORIJA		2021		2022		2023		2024		2025		2026		2027		KOPĀ	
		FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)																	
Galvenā mītne un Komisijas pārstāvniecības	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
Savienības delegācijās	AD																
	AST																
• Ārštata darbinieki ⁵⁰ 0,24																	
Kopējie piešķirumi	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	END																
	INT																
Savienības delegācijās	AC																
	AL																

⁵⁰ AC – līgumdarbinieki, AL – vietējie darbinieki, END – valstu norīkotie eksperti, INT – aģentūru darbinieki, JPD – jaunākie speciālisti delegācijās.

	END																
	INT																
	JPD																
Citas budžeta pozīcijas (norādīt)																	
Starpsumma — daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Vajadzīgie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau iesaistīti konkrētās darbības pārvaldībā un/vai pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

Ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS		2021		2022		2023		2024		2025		2025		2025		KOPĀ	
		FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas	FTE	Apropriācijas
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)																	
Pētniecība	AD																
	AST																
• Ārštata darbinieki ⁵¹																	
Ārštata darbinieki no darbības apropriācijām (kādreizējām BA pozīcijām).	– galvenajā mītnē	AC															
		END															
		INT															
	– Savienības delegācijās	AC															
		AL															
		END															
		INT															
		JPD															
Pētniecība	AC																
	END																
	INT																

⁵¹ AC – līgumdarbinieki, AL – vietējie darbinieki, END – valstu norīkoti eksperti, INT – aģentūru darbinieki, JPD – jaunākie speciālisti delegācijās.

Citas budžeta pozīcijas (norādīt)																	
Starpsumma — ārpus daudzgadu finanšu shēmas																	
7. IZDEVUMU KATEGORIJAS																	

Vajadzīgie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

Paredzamā ietekme uz ENISA cilvēkresursiem

Eiropas Savienības Kiberdrošības aģentūra (ENISA), kam ar Kiberdrošības aktu ir uzticēts jauns pastāvīgs pilnvarojums, palīdzēs dalībvalstīm un Komisijai pārskatītās TID direktīvas īstenošanā.

Pārskatītās TID direktīvas rezultātā no 2022./2023. gada ENISA būs papildu rīcības jomas. Lai gan uz šīm rīcības jomām attieksies ENISA vispārējie uzdevumi atbilstoši tās pilnvarojumam, tās aģentūrai radīs papildu darba slodzi. Konkrētāk, papildus tās pašreizējām rīcības jomām atbilstoši Komisijas priekšlikumam par pārskatītu TID direktīvu ENISA savā darba programmā cita starpā būs arī jāiekļauj šādas darbības: i) izveidot un uzturēt Eiropas neaizsargātības reģistru (priekšlikuma 6. panta 2. punkts), ii) nodrošināt Eiropas Kiberkrīžu sadarbības organizāciju tīklu (CyCLONe) (priekšlikuma 14. pants) un izdot gada ziņojumu par situāciju kiberdrošības jomā ES (priekšlikuma 15. pants), iii) atbalstīt salīdzinošās izvērtēšanas organizēšanu starp dalībvalstīm (priekšlikuma 16. pants), iv) savākt apkopotus incidentu datus no dalībvalstīm un izdot tehniskus norādījumus (priekšlikuma 20. panta 9. punkts), v) izveidot un uzturēt to vienību reģistru, kuras sniedz pārrobežu pakalpojumus (priekšlikuma 25. pants).

Tāpēc no 2022. gada tiks pieprasīti pieci papildu pilnslodzes ekvivalenti (FTE) ar atbilstošo budžetu aptuveni 0,61 miljons gadā, lai finansētu šīs jaunās amata vietas (sk. atsevišķu finanšu pārskatu par aģentūrām).

Tāpēc no 2022. gada tiks pieprasīti pieci papildu pilnslodzes ekvivalenti (FTE) ar atbilstošo budžetu, lai finansētu šīs jaunās amata vietas.

- ☐ Priekšlikums/iniciatīva neprasa izmantot administratīvas apropriācijas
- ☒ Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādi:

Miljonos EUR (līdz 3 zīmēm aiz komata)

	N gads ⁵² 2022	N+1 gads 2023	N+2 gads 2024	N+3 gads 2025	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)	KOPĀ
--	---------------------------------	---------------------	---------------------	---------------------	---	------

Pagaidu darbinieki (AD kategorijas)	0,450	0,450	0,450	0,450	0,450	0,450		2,7
--	-------	-------	-------	-------	-------	-------	--	-----

⁵² N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet “N” ar paredzēto pirmo īstenošanas gadu (piemēram, 2021. gadu). Tas pats attiecas uz turpmākajiem gadiem.

Pagaidu darbinieki (AST kategorijas)								
Līgumdarbinieki	0,160	0,160	0,160	0,160	0,160	0,160		
Norīkotie valsts eksperti								0,96

KOPĀ	0,61	0,61	0,61	0,61	0,61	0,61		3,66
-------------	-------------	-------------	-------------	-------------	-------------	-------------	--	-------------

Personāla vajadzības (FTE):

	N gads⁵³ 2022	N+1 gads 2023	N+2 gads 2024	N+3 gads 2025	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)	KOPĀ
--	---	------------------------------	------------------------------	------------------------------	---	-------------

Pagaidu darbinieki (AD kategorijas)	3	3	3	3	3	3		18
Pagaidu darbinieki (AST kategorijas)								
Līgumdarbinieki	2	2	2	2	2	2		12
Norīkotie valsts eksperti								

⁵³ N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet “N” ar paredzēto pirmo īstenošanas gadu (piemēram, 2021.). Tas pats attiecas uz turpmākajiem gadiem.

KOPĀ	5	5	5	5	5	5		30
------	---	---	---	---	---	---	--	----

2. Citu administratīvo izdevumu izmaksas

☐ Priekšlikums/iniciatīva neparedz administratīvo apropriāciju izmantošanu

X ☐ Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādā veidā:

Miljonos EUR (līdz 3 zīmēm aiz komata)

Daudz gadu finanšu shēmas 7. IZDEVUMU KATEGORIJA	2021	2022	2023	2024	2025	2026	2027	Kopā
<u>Galvenajā mītnē</u>								
Komandējumu un reprezentācijas izmaksas	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,21
Konferenču un sanāksmju izmaksas	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,42
Komitejas ⁵⁴								
Pētījumi un konsultācijas								
Informācijas un vadības sistēmas								
IKT iekārtas un pakalpojumi ⁵⁵								

⁵⁴ Precizēt komitejas veidu un grupu, pie kuras tā pieder.

⁵⁵ IKT: informācijas un sakaru tehnoloģijas; jāapspriežas ar DIGIT.

Pārējās budžeta pozīcijas (<i>vajadzības gadījumā precizēt</i>)								
<u>Savienības delegācijās</u>								
Komandējumu, konferenču un reprezentācijas izdevumi								
Personāla kvalifikācijas celšanas apmācības								
Ēku iegāde, īre un saistītie izdevumi								
Iekārtas, mēbeles, piegādes un pakalpojumi								
Starpsumma — daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63

Miljonos EUR (līdz 3 zīmēm aiz komata)

Ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS	2021	2022	2023	2024	2025	2026	2027	Kopā
Izdevumi tehniskai un administratīvai palīdzībai (neietverot ārštata darbiniekus) no darbības apropriācijām (kādreizējām "BA" pozīcijām)								
– galvenajā mītnē								
– Savienības delegācijās								
Citi pārvaldības izdevumi pētniecībai								
Pārējās budžeta pozīcijas (vajadzības gadījumā precizēt)								
Starpsumma — ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS								

KOPĀ Daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA un ārpus tās	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
--	------	------	------	------	------	------	------	-------------

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

3. Izmantotās izmaksu aprēķināšanas metodes

3.1. Cilvēkresursi

Šajā daļā ir izklāstīta aprēķina metode, ko izmanto nepieciešamo cilvēkresursu aplēšanai (pieņēmumi par darba slodzi, ieskaitot īpašus darbus (Sysper 2 darba profili), darbinieku kategorijas un atbilstīgās vidējās izmaksas)

Daudzgaļu finanšu shēmas 7. IZDEVUMU KATEGORIJA
NB! Galvenās mētnes katras darbinieku kategorijas vidējās izmaksas ir pieejamas BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
- Ierēdņi un pagaidu darbinieki 6 FTE ierēdņi (vidējās izmaksas 0,150) = 0,9 gadā - Deleģēto aktu sagatavošana saskaņā ar 18. panta 6. punktu, 21. panta 2. punktu, 36. pantu; - Īstenošanas aktu sagatavošana saskaņā ar 12. panta 8. punktu, 18. panta 5. punktu, 20. panta 11. punktu; - sekretariāta nodrošināšana TID sadarbības grupai; - TID sadarbības grupas plenārsēžu un darba straumēšanas sanāksmju organizēšana; - dalībvalstu darba koordinēšana saistībā ar dažādiem dokumentiem (pamatnostādnes, rīkkopas utt.); - sadarbība ar citiem Komisijas dienestiem, ENISA un valsts iestādēm, lai īstenotu TID direktīvu; - ar TID direktīvas īstenošanu saistīto valsts metožu un paraugprakses analīze.
Ārštata darbinieki 3 AC (vidējās izmaksas 0,08) = 0,24 gadā - Pēc vajadzības sniegt atbalstu visos minētajos uzdevumos

Ārpus daudzgaļu finanšu shēmas 7. IZDEVUMU KATEGORIJAS
Vienīgi amata vietas, ko finansē no pētniecības budžeta
Ārštata darbinieki

3.2. Citi administratīvie izdevumi

Norādīt aprēķinu metodi, kas izmantota katrai budžeta pozīcijai un īpaši pamatā esošajiem pieņēmumiem (piemēram, sanāksmju skaits gadā, vidējās izmaksas, utt.)

Daudzgažu finanšu shēmas 7. IZDEVUMU KATEGORIJA

Sanāksmes: TID sadarbības grupas plenārsēdes parasti notiek četras reizes gadā. Komisija sēdz 27 dalībvalstu pārstāvju ēdināšanas un ceļa izdevumus (viens pārstāvis no katras DV). Vienas sēdes izmaksas var sasniegt 15 000 EUR, kas veido 60 000 EUR gadā.

Komandējumi: komandējumi ir saistīti ar TID direktīvas īstenošanas uzraudzību. Piemērs. Vienā gadā (2019. gada maijs–2020. gada jūlijs) bija jāorganizē tā dēvētie “TID valstu apmeklējumi” un jāapmeklē visas 27 DV, lai apspriestu

TID direktīvas īstenošanu ES.

Ārpus daudzgažu finanšu shēmas 7. IZDEVUMU KATEGORIJAS
--

7. PIELIKUMS

KOMISIJAS LĒMUMAM,

kas adresēts Komisijas dienestiem, par iekšējiem noteikumiem attiecībā uz Eiropas Savienības vispārējā budžeta (sadaļa “Eiropas Komisija”) izpildi

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS — AĢENTŪRAS

Šis tiesību akta priekšlikuma finanšu pārskats (LFS) attiecas uz pieprasījumu palielināt *ENISA* darbinieku skaitu par 5 FTE no 2022. gada, lai veiktu papildu darbības, kas saistītas ar TID direktīvas īstenošanu. Uz šīm darbībām jau attiecas *ENISA* pilnvarojums.

Satura rādītājs

1.	PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS	17
1.1.	Priekšlikuma/iniciatīvas nosaukums	17
1.2.	Attiecīgā(-as) rīcībpolitikas joma(-as)	17
1.3.	Priekšlikums attiecas uz	17
1.4.	Mērķis(-i)	17
1.4.1.	Vispārīgais(-ie) mērķis(-i).....	17
1.4.2.	Konkrētais(-ie) mērķis(-i)	17
1.4.3.	Paredzamais(-ie) rezultāts(-i) un ietekme	19
1.4.4.	Snieguma rādītāji	19
1.5.	Priekšlikuma/iniciatīvas pamatojums	20
1.5.1.	Īstermiņā vai ilgtermiņā izpildāmās vajadzības, kā arī detalizēts iniciatīvas izvēršanas grafiks	20
1.5.2.	Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka efektivitāte vai papildinājums). Šajā punktā “Savienības iesaistīšanās pievienotā vērtība” ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.	20
1.5.3.	Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas.....	21
1.5.4.	Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem.....	21
1.5.5.	Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums.....	21
1.6.	Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme	22
1.7.	Plānotais(-ie) pārvaldības veids(-i)	22
2.	PĀRVALDĪBAS PASĀKUMI.....	24
2.1.	Pārraudzības un ziņošanas noteikumi	24
2.2.	Pārvaldības un kontroles sistēma(-as).....	24
2.2.1.	Ierosinātā(-o) pārvaldības veida(-u), finansējuma apgūšanas mehānisma, maksāšanas kārtības un kontroles stratēģijas pamatojums	24
2.2.2.	Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto(-ajām) iekšējās kontroles sistēmu(-ām).....	24
2.2.3.	Pārbažu izmaksas un to lietderības pamatojums (attiecība “kontroles izmaksas ÷ attiecīgo pārvaldīto fondu vērtība”), un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas un programmas slēgšanas brīdī)	24
2.3.	Krāpšanas un pārkāpumu novēršanas pasākumi	25
3.	PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME	25

3.1.	Attiecīgā(-ās) daudzgadu finanšu shēmas izdevumu kategorija(-as) un budžeta izdevumu pozīcija(-as).....	25
3.2.	Aplēstā ietekme uz izdevumiem	27
3.2.1.	Kopsavilkums par paredzamo ietekmi uz izdevumiem	27
3.2.2.	Paredzamā ietekme uz [struktūras] apropriācijām	29
3.2.3.	Paredzamā ietekme uz ENISA cilvēkresursiem.....	30
3.2.4.	Saderība ar kārtējo daudzgadu finanšu shēmu	33
3.2.5.	Trešo personu iemaksas	33
3.3.	Aplēstā ietekme uz ieņēmumiem	34

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Priekšlikums “Direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148”.

1.2. Attiecīgā(-as) rīcībpolitikas joma(-as)

Sakaru tīkli, saturs un tehnoloģija

1.3. Priekšlikums attiecas uz

☐ jaunu darbību

☐ jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību⁵⁶

☒ esošas darbības pagarināšanu

☐ vienas vai vairāku darbību apvienošanu ar citu/jaunu darbību

1.4. Mērķis(-i)

1.4.1. Vispārīgais(-ie) mērķis(-i)

Pārskatīšanas mērķis ir paaugstināt kiberneturības līmeni uzņēmumu, kas darbojas Eiropas Savienībā visās attiecīgajās nozarēs, visaptverošam kopumam, mazināt noturības atšķirības visā iekšējā tirgū nozarēs, uz kurām jau attiecas direktīva, un uzlabot kopējās izpratnes par situāciju līmeni un kolektīvo spēju sagatavoties un reaģēt.

1.4.2. Konkrētais(-ie) mērķis(-i)

Lai risinātu problēmu, kas saistīta ar to uzņēmumu zemo kiberneturības līmeni, kuri darbojas Eiropas Savienībā, konkrētais mērķis ir nodrošināt, ka vienībām visās nozarēs, kas ir atkarīgas no tīklu un informācijas sistēmām un kas sniedz pamatpakalpojumus ekonomikai un sabiedrībai kopumā, ir jāveic kiberdrošības pasākumi un jāziņo par incidentiem, lai paaugstinātu vispārējo kiberneturības līmeni visā iekšējā tirgū.

Lai risinātu problēmu, kas saistīta ar neviendabīgu noturību dalībvalstīs un nozarēs, konkrētais mērķis ir nodrošināt, ka visām vienībām, kas darbojas nozarēs, uz kurām attiecas TID tiesiskais regulējums, kas ir līdzīgas to lieluma ziņā un kam ir salīdzināma loma, ir piemērojams vienāds regulatīvais režīms (tās ietilpst vai neietilpst darbības jomā), neatkarīgi no tā, kura jurisdikcija uz tām attiecas ES.

Lai nodrošinātu, ka visām vienībām, kas darbojas nozarēs, uz kurām attiecas TID tiesiskais regulējums, ir jāievēro vienādi pienākumi, pamatojoties uz riska pārvaldības koncepciju, ciktāl runa ir par drošības pasākumiem, un jāziņo par visiem incidentiem, pamatojoties uz vienotu kritēriju kopumu, konkrētie mērķi ir nodrošināt, ka kompetentās iestādes efektīvāk panāk tiesību instrumentā paredzēto noteikumu izpildi, īstenojot saskaņotus uzraudzības un izpildes pasākumus, un nodrošināt dalībvalstīs salīdzināmu līmeni resursiem, ko piešķir kompetentajām iestādēm, lai tās varētu izpildīt TID regulējumā noteiktos pamatuzdevumus.

⁵⁶

Kā minēts Finanšu regulas 58. panta 2. punkta a) vai b) apakšpunktā.

Lai risinātu problēmu, kas saistīta ar vienotu izpratni par situāciju un kopīgas reaģēšanas uz krīzi trūkumu, konkrētais mērķis ir nodrošināt, ka starp dalībvalstīm notiek būtiskas informācijas apmaiņa, ieviešot skaidrus pienākumus kompetentajām iestādēm apmainīties ar informāciju un sadarboties attiecībā uz kibernetiskiem draudiem un incidentiem un attīstot kopējas Savienības operatīvās krīzes reaģēšanas spējas.

1.4.3. *Paredzamais(-ie) rezultāts(-i) un ietekme*

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz labuma guvējiem / mērķgrupām.

Paredzams, ka priekšlikums radīs ievērojamu ieguvumu — aplēses rāda, ka tas var samazināt kibernetikas incidentu izmaksas par 11,3 miljardiem EUR. Nozaru tvērums tiktu ievērojami palielināts atbilstoši TID regulējumam, taču papildus minētajiem ieguvumiem arī slogs, ko var radīt TID prasības, it īpaši no uzraudzības viedokļa, būtu līdzsvarots gan jaunām vienībām, kas jāaptver, gan kompetentajām iestādēm. Proti, ar jauno TID regulējumu tiktu izveidota divslāņu pieeja, koncentrējoties uz lielām un svarīgām vienībām, un uzraudzības režīma diferencēšana, kas ļauj tikai pēc notikušā uzraudzīt lielu skaitu vienību, it īpaši vienības, ko uzskata par “svarīgām”, bet ne “būtiskām”.

Kopumā priekšlikums radītu efektīvus kompromisus un sinerģijas, jo tam ir no visām analizētajām politikas iespējām vislielākais potenciāls nodrošināt uzlabotu un saskaņotu galveno vienību kibernetikas līmeni visā Savienībā, galu galā radot izmaksu ietaupījumus gan uzņēmumiem, gan sabiedrībai.

Priekšlikums arī radīs konkrētas atbilstības un izpildes nodrošināšanas izmaksas attiecīgajām dalībvalstu iestādēm (tika aplēsts kopējais palielinājums par aptuveni 20–30 % no resursiem). Tomēr jaunais regulējums arī radītu ievērojamus ieguvumus, jo uzlabotos priekšstats par galvenajiem uzņēmumiem un mijiedarbība ar tiem, uzlabotos pārrobežu operatīvā sadarbība, kā arī savstarpējā palīdzība un salīdzinošās izvērtēšanas mehānismi. Tas vispārēji palielinātu kibernetikas spējas dalībvalstīs.

Tiek lēsts, ka uzņēmumiem, uz kuriem tiktu attiecināts TID regulējums, to pašreizējie izdevumi IKT drošībai būs jāpalielina par ne vairāk kā 22 % pirmajos gados pēc jaunā TID regulējuma ieviešanas (uzņēmumiem, uz kuriem jau attiecas pašreizējās TID direktīvas darbība joma, tie būtu 12 %). Tomēr šis IKT drošības izdevumu vidējais palielinājums radītu samērīgu ieguvumu no šādiem ieguldījumiem, jo īpaši tādēļ, ka ievērojami samazinātos kibernetikas incidentu izmaksas (tiek lēstas 118 miljardu EUR apmērā desmit gadu laikposmā).

TID regulējums neattiektos uz mazajiem uzņēmumiem un mikrouzņēmumiem. Attiecībā uz vidējiem uzņēmumiem ir gaidāms, ka IKT drošības izdevumu līmenis palielināsies pirmajos gados pēc jaunā TID regulējuma ieviešanas. Tajā pašā laikā kibernetikas prasību līmeņa paaugstināšana šīm vienībām arī stimulētu to kibernetikas spējas un palīdzētu uzlabot to IKT riska pārvaldību.

Būtu ietekme uz valstu budžetiem un valsts pārvaldi — tiek lēsts, ka īstermiņā un vidējā termiņā palielinājums būtu aptuveni 20–30 % no resursiem.

Citāda būtiska negatīva ietekme nav paredzama. Paredzams, ka priekšlikums radīs stabilākas kibernetikas spējas un attiecīgi radīs ievērojamāku mazinošu ietekmi uz incidentu, tostarp datu aizsardzības pārkāpumu, skaitu un smagumu. Tam arī, visticamāk, būs pozitīva ietekme uz vienlīdzīgu konkurences apstākļu nodrošināšanu dalībvalstīs visām vienībām, uz kurām attiecas TID regulējums, un tas mazinās kibernetikas informācijas asimetriju.

1.4.4. *Snieguma rādītāji*

Norādīt, pēc kādiem rādītājiem seko līdzī progresam un sasniegumiem.

Rādītāju novērtējumu veiks Komisija ar ENISA un sadarbības grupas atbalstu, sākot trīs gadus pēc jaunā TID tiesību akta stāšanās spēkā. Daži no uzraudzības rādītājiem, uz kuru pamata tiktu novērtēti TID pārskatīšanas panākumi, ir aprakstīti turpmāk.

- Uzlabota incidentu risināšana. Veicot kibernetikas pasākumus, uzņēmumi uzlabo ne tikai savu spēju pilnībā izvairīties no konkrētiem incidentiem, bet arī savu spēju reaģēt uz incidentiem. Tāpēc panākumu novērtēšanas kritēriji ir i) incidenta atklāšanai vajadzīgā vidējā laika samazināšanās, ii) vidējais laiks, kas organizācijām vajadzīgs, lai atgūtos no incidenta, un iii) incidenta izraisītā kaitējuma vidējās izmaksas.
- Labāka uzņēmumu augstākās vadības izpratne par kibernetikas riskiem. Nosakot uzņēmumiem prasību veikt pasākumus, pārskatīta TID direktīva veicinātu augstākās vadības izpratnes uzlabošanu par riskiem, kas saistīti ar kibernetiku. To var novērtēt, izpētot, ciklā uzņēmumi, uz kuriem attiecas TID regulējums, piešķir prioritāti kibernetikai uzņēmuma iekšējā politikā un procesos, ko apliecina iekšējā dokumentācija, attiecīgas apmācības programmas un izpratnes veicināšanas pasākumi darbiniekiem, un par prioritāti nosaka ar drošību saistītus ieguldījumus IKT. Visu būtisko un svarīgo vienību vadībai būtu arī jāpārzina TID direktīvā paredzētie noteikumi.
- Konkrētu nozaru izdevumu izlīdzināšana. Izdevumi IKT drošībai ievērojami atšķiras starp nozarēm ES. Nosakot uzņēmumiem vairākās nozarēs prasību veikt pasākumus, starp nozarēm un dalībvalstīm būtu jāsamazinās novirze no vidējiem konkrētu nozaru izdevumiem IKT drošībai, tos izsakot procentos no kopējiem izdevumiem IKT.
- Spēcīgākas kompetentās iestādes un palielināta sadarbība. Pārskatīta TID direktīva varētu radīt papildu uzdevumus kompetentajām iestādēm. Tam būtu izmērāma ietekme uz finanšu resursiem un cilvēkresursiem, ko atvēl kibernetikas aģentūrām valstu līmenī, un tam vajadzētu būt arī pozitīvai ietekmei uz kompetento iestāžu spēju proaktīvi sadarboties un tādējādi palielināt to gadījumu skaitu, kad kompetentās iestādes savstarpēji sazinās, lai risinātu pārrobežu incidentus vai veiktu kopīgas uzraudzības darbības.
- Uzlabota informācijas apmaiņa. Pārskatītais TID regulējums arī uzlabotu informācijas apmaiņu starp uzņēmumiem un ar kompetentajām iestādēm. Viens no pārskatīšanas mērķiem varētu būt palielināt to vienību skaitu, kuras piedalās dažādu veidu informācijas apmaiņā.

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, kā arī detalizēts iniciatīvas izvērtēšanas grafiks

Priekšlikuma mērķis ir paaugstināt kibernetikas līmeni uzņēmumu, kas darbojas Eiropas Savienībā visās attiecīgajās nozarēs, visaptverošam kopumam, mazināt noturības atšķirības visā iekšējā tirgū nozarēs, uz kurām jau attiecas direktīva, un uzlabot kopējās izpratnes par situāciju līmeni un kolektīvo spēju sagatavoties un reaģēt. Tas būs balstīts uz to, kas sasniegts saistībā ar Direktīvas (ES) 2016/1148 īstenošanu iepriekšējos četros gados.

1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka efektivitāte vai papildinājums). Šajā punktā "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.

Kibernetikas noturība visā Savienībā nevar būt efektīva, ja attiecībā uz to tiek īstenotas atšķirīgas valstu vai reģionu pieejas. TID direktīva pievērsās šim trūkumam, nosakot satvaru tīklu un informācijas sistēmu drošībai valstu un Savienības līmenī. Tomēr TID direktīvas pirmajā periodiskajā pārskatīšanā tika konstatētas vairākas raksturīgas nepilnības, kas galu galā ir novedušas pie ievērojām atšķirībām starp dalībvalstīm spēju, plānošanas un aizsardzības līmeņa ziņā, kuras tajā pašā laikā ietekmē vienlīdzīgus konkurences apstākļus līdzīgiem uzņēmumiem iekšējā tirgū.

ES iesaistīšanos, kas pārsniedz pašreizējos TID direktīvas pasākumus, pamato galvenokārt šādi faktori: i) problēmas pārrobežu raksturs; ii) iespēja, ka ar ES rīcību tiks uzlabota un veicināta efektīva valstu politika; iii) saskaņotu un sadarbīgu TID politikas darbību ieguldījums efektīvā datu un privātuma aizsardzībā.

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

1.5.3. *Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas*

TID direktīva ir pirmais horizontālais iekšējā tirgus instruments, kura mērķis ir uzlabot tīklu un sistēmu noturību Savienībā pret kiberdrošības riskiem. Kopš tās stāšanās spēkā 2016. gadā tā jau ir ievērojami veicinājusi vispārējā kiberdrošības līmeņa paaugstināšanos dalībvalstīs. Tomēr direktīvas darbības un īstenošanas pārskatīšanā tika konstatētas vairākas nepilnības, kas papildus pieaugošajai digitalizācijai un vajadzībai pēc faktiskajai situācijai atbilstošas reaģēšanas ir jārisina pārskatītā tiesību instrumentā.

1.5.4. *Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem*

Jaunais priekšlikums ir pilnībā saderīgs un saskaņots ar citām saistītām iniciatīvām, piemēram, priekšlikumu regulai par finanšu sektora digitālās darbības noturību ("DORA") un priekšlikumu direktīvai par pamatpakalpojumu kritisko sniedzēju noturību. Tas ir arī saderīgs ar Eiropas Elektronisko sakaru kodeksu, Vispārīgo datu aizsardzības regulu un eIDAS regulu.

Priekšlikums ir ES Drošības savienības stratēģijas būtiska daļa.

1.5.5. *Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums*

Lai ENISA varētu pārvaldīt šos uzdevumus, ir nepieciešami īpaši profili un papildu darba slodze, ko nevar uzņemt, nepalielinot cilvēkresursus.

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

☐ ierobežots ilgums

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

☒ beztermiņa

- Īstenošana ar uzsākšanas periodu no 2022. līdz 2025. gadam,
- pēc kura turpinās normāla darbība.

1.7. Plānotais(-ie) pārvaldības veids(-i)⁵⁷

☒ Komisijas tieša pārvaldība,

ko veic

- ☐ izpildaģentūras

☐ Dalīta pārvaldība kopā ar dalībvalstīm

☐ Netieša pārvaldība, kurā budžeta īstenošanas uzdevumi uzticēti:

- ☐ starptautiskām organizācijām un to aģentūrām (precizēt);
- ☐ EIB un Eiropas Investīciju fondam;
- ☒ Finanšu regulas 70. un 71. pantā minētajām struktūrām;
- ☐ publisko tiesību subjektiem;
- ☐ privāttiesību subjektiem, kas veic sabiedrisko pakalpojumu sniedzēju uzdevumus, tādā mērā, kādā tiem ir pienācīgas finansiālas garantijas;
- ☐ struktūrām, kuru darbību reglamentē dalībvalsts privāttiesības, kurām ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuras sniedz pienācīgas finansiālas garantijas;
- ☐ personām, kurām ir uzticēts veikt īpašas darbības KĀDP saskaņā ar Līguma par Eiropas Savienību V sadaļu un kuras ir noteiktas attiecīgā pamataktā.

Piezīmes

Eiropas Savienības Kiberdrošības aģentūra (ENISA), kam ar Kiberdrošības aktu ir uzticēts jauns pastāvīgs pilnvarojums, palīdzēs dalībvalstīm un Komisijai pārskatītās TID direktīvas īstenošanā.

Pārskatītās TID direktīvas rezultātā no 2022./2023. gada ENISA būs papildu rīcības jomas. Lai gan uz šīm rīcības jomām attieksies ENISA vispārējie uzdevumi atbilstoši tās pilnvarojumam, tās aģentūrai radīs papildu darba slodzi. Konkrētāk, papildus tās pašreizējām rīcības jomām atbilstoši Komisijas priekšlikumam par pārskatītu TID direktīvu ENISA savā darba programmā cita starpā būs arī jāiekļauj šādas darbības: i) izveidot un uzturēt Eiropas neaizsargātības reģistru (priekšlikuma 6. panta 2. punkts), ii) nodrošināt Eiropas Kiberkrīžu sadarbības organizāciju tīklu (CyCLONE) (priekšlikuma 14. pants) un izdot gada ziņojumu par situāciju kiberdrošības jomā ES (priekšlikuma 15. pants), iii) atbalstīt salīdzinošās izvērtēšanas organizēšanu starp dalībvalstīm (priekšlikuma 16. pants), iv) savākt apkopotus incidentu datus no dalībvalstīm un izdot tehniskus norādījumus (priekšlikuma 20. panta

⁵⁷

Skaidrojumus par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt BudgWeb tīmekļa vietnē: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

9. punkts), v) izveidot un uzturēt to vienību reģistru, kuras sniedz pārrobežu pakalpojumus (priekšlikuma 25. pants).

Tāpēc no 2022. gada tiks pieprasīti pieci papildu pilnslodzes ekvivalenti (FTE) ar atbilstošo budžetu aptuveni 0,61 miljons EUR, lai finansētu šīs jaunās amata vietas.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

Norādīt periodiskumu un nosacījumus.

Komisija periodiski pārskatīs direktīvas darbību un ziņos Eiropas Parlamentam un Padomei, pirmo reizi – trīs gadus pēc tās stāšanās spēkā.

Komisija arī novērtēs, vai dalībvalstīs direktīva tiek transponēta pareizi.

Priekšlikuma uzraudzībā un ziņošanā par to tiks ievēroti principi, kas izklāstīti *ENISA* pastāvīgajā pilnvarojumā atbilstoši *REGULAI (ES) 2019/881* (Kiberdrošības aktā).

Datu avoti, ko izmantos plānotajai uzraudzībai, galvenokārt būs *ENISA*, sadarbības grupa, *CSIRT* tīkls un dalībvalstu iestādes. Papildus *ENISA*, sadarbības grupas, *CSIRT* tīkla ziņojumos (arī *ENISA* gada darbības pārskatos) sniegtajiem datiem vajadzības gadījumā var izmantot īpašus datu vākšanas instrumentus (piemēram, valsts iestāžu apsekojumus, Eiroparometru un kiberdrošības mēneša kampaņas un Eiropas mēroga mācību ietvaros sagatavotos pārskatus).

2.2. Pārvaldības un kontroles sistēma(-as)

2.2.1. *Ierosinātā(-o) pārvaldības veida(-u), finansējuma apgūšanas mehānisma, maksāšanas kārtības un kontroles stratēģijas pamatojums*

CNECT ĢD struktūrvienība, kas atbild par attiecīgās politikas jomu, pārvaldīs direktīvas īstenošanu.

Attiecībā uz *ENISA* pārvaldību Kiberdrošības akta 15. pantā ir sniegts sīki izstrādāts *ENISA* Administratīvās padomes kontroles funkciju saraksts.

Saskaņā ar Kiberdrošības akta 31. pantu *ENISA* izpilddirektors atbild par *ENISA* budžeta izpildi un Komisijas iekšējais revidents attiecībā uz *ENISA* īsteno tādas pašas pilnvaras kā attiecībā uz Komisijas dienestiem. *ENISA* Administratīvā padome sniedz atzinumu par *ENISA* galīgajiem pārskatiem.

2.2.2. *Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto(-ajām) iekšējās kontroles sistēmu(-ām)*

Ļoti zems risks, jo TID direktīvas ekosistēma jau pastāv un jau aptver *ENISA*, kam ir pastāvīgas pilnvaras pēc Kiberdrošības akta stāšanās spēkā 2019. gadā.

2.2.3. *Pārbaužu izmaksas un to lietderības pamatojums (attiecība “kontroles izmaksas ÷ attiecīgo pārvaldīto fondu vērtība”), un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas un programmas slēgšanas brīdī)*

Prasītajā budžeta palielinājumā piemēro 1. sadaļu, un tas ir paredzēts, lai finansētu algas. Tas nozīmē ļoti zemu kļūdas risku maksājumu līmenī.

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.

ENISA īstenotie novēršanas un aizsardzības pasākumi tiktu piemēroti šādos gadījumos:

- maksājumus par visiem pieprasītajiem pakalpojumiem vai pētījumiem pirms apmaksas pārbauda aģentūras personāls, ņemot vērā visas līgumsaistības, ekonomikas principus un finanšu vai vadības paraugpraksi. Krāpšanas apkarošanas noteikumus (pārraudzība, prasības par ziņošanu u. c.) iekļaus visos nolīgumos un līgumos, ko noslēdz starp aģentūru un maksājumu saņēmējiem;
- lai apkarotu krāpšanu, korupciju un citas nelikumīgas darbības, bez ierobežojumiem piemēro noteikumus, kas paredzēti Eiropas Parlamenta un Padomes 1999. gada 25. maija Regulā (ES, Euratom) Nr. 883/2013 par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (OLAF);
- saskaņā ar Kiberdrošības akta 33. pantu ENISA līdz 2019. gada 28. decembrim pievienojās Eiropas Parlamenta, Eiropas Savienības Padomes un Eiropas Kopienų Komisijas iestāžu 1999. gada 25. maija nolīgumam par iekšējo izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (OLAF). ENISA nekavējoties izdod attiecīgos noteikumus, kas piemērojami visiem aģentūras darbiniekiem.

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgā(-ās) daudzgadu finanšu shēmas izdevumu kategorija(-as) un budžeta izdevumu pozīcija(-as)

- Esošās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām.

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevum u veids	Iemaksas			
	Numurs	Dif./nedif. 58	no EBTA valstīm ⁵⁹	no kandidātvalstīm ⁶⁰	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē
2	02 10 04	/nedif.	JĀ	NĒ	NĒ	/NĒ

- No jauna veidojamās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām.

Daudzgadu	Budžeta pozīcija	Izdevum	Iemaksas
-----------	------------------	---------	----------

58 Diff. = Dif. — diferencētās apropriācijas / Nedif. — nediferencētās apropriācijas.

59 EBTA – Eiropas Brīvās tirdzniecības asociācija.

60 Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

finanšu shēmas izdevumu kategorija		u veids				
	Numurs	Dif./nedif.	no EBTA valstīm	no kandidātval stīm	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē
	[XX.YY.YY.YY]		JĀ/NĒ	JĀ/NĒ	JĀ/NĒ	JĀ/NĒ

3.2. Aplēstā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

Miljonos EUR (līdz 3 zīmēm aiz komata)

Daudz gadu finanšu shēmas izdevumu kategorija	Numurs	[Pozīcija...2 Vienotais tirgus, inovācija un digitālā ekonomika.....]
---	--------	---

[Struktūra]: <... ENISA....>			N gads ⁶¹ 2022	N+1 gads 2023	N+2 gads 2024	N+3 gads 2025	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu) 2026 2027			KOPĀ
1. sadaļa:	Saistības	1)	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Maksājumi	2)	0,61	0,61	0,61	0,61	0,61	0,61		3,66
2. sadaļa:	Saistības	(1.a)								
	Maksājumi	(2.a)								
3. sadaļa:	Saistības	(3.a)								
	Maksājumi	(3.b)								
KOPĀ apropriācijas [struktūrai] < ENISA.....>	Saistības	=1+1.a +3.a	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Maksājumi	=2+2.a +3.b	0,61	0,61	0,61	0,61	0,61	0,61		3,66

⁶¹ N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet “N” ar paredzēto pirmo īstenošanas gadu (piemēram, 2021.). Tas pats attiecas uz turpmākajiem gadiem.

Daudz gadu finanšu shēmas izdevumu kategorija	5	“Administratīvie izdevumi”
--	----------	----------------------------

Miljonos EUR (līdz 3 zīmēm aiz komata)

		N gads	N+1 gads	N+2 gads	N+3 gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			KOPĀ
ĢD: <.....>									
• Cilvēkresursi									
• Citi administratīvie izdevumi									
KOPĀ ĢD <.....>	Apropriācijas								

KOPĀ — daudz gadu finanšu shēmas 5. IZDEVUMU KATEGORIJAS apropriācijas	(Saistību summa = maksājumu summa)								
---	---------------------------------------	--	--	--	--	--	--	--	--

Miljonos EUR (līdz 3 zīmēm aiz komata)

		N gads⁶² 2022	N+1 gads 2023	N+2 gads 2024	N+3 gads 2025	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu) 2026 2027			KOPĀ
KOPĀ — daudz gadu finanšu shēmas 1.–5. IZDEVUMU KATEGORIJAS apropriācijas	Saistības	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Maksājumi	0,61	0,61	0,61	0,61	0,61	0,61		3,66

⁶² N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet “N” ar paredzēto pirmo īstenošanas gadu (piemēram, 2021.). Tas pats attiecas uz turpmākajiem gadiem.

3.2.2. Paredzamā ietekme uz [struktūras] apropriācijām

- ☐x Priekšlikums/iniciatīva neprasa darbības apropriāciju izmantošanu
- ☐ Priekšlikums/iniciatīva paredz darbības apropriācijas izmantot šādā veidā:

Saistību apropriācijas miljonos EUR (līdz 3 zīmēm aiz komata)

Norādīt mērķus un rezultātus			N gads		N+1 gads		N+2 gads		N+3 gads		Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)						KOPĀ	
	REZULTĀTI																	
	↓	Veids ⁶³	Vidējā s izmak sas	Skaits	Izmak sas	Skaits	Izmak sas	Skaits	Izmak sas	Skaits	Izmak sas	Skaits	Izma ksas	Skaits	Izmak sas	Skaits	Izmak sas	Kopēj ais skaits
KONKRĒTAIS MĒRĶIS Nr. 1 ⁶⁴ ...																		
– Rezultāts																		
– Rezultāts																		
– Rezultāts																		
Starpsumma — konkrētais mērķis Nr. 1																		
KONKRĒTAIS MĒRĶIS Nr. 2 ...																		
– Rezultāts																		
Starpsumma — konkrētais mērķis Nr. 2																		
KOPĒJĀS IZMAKSAS																		

⁶³ Rezultāti ir piegādājamie produkti un pakalpojumi (piemēram, finansēto studentu apmaiņas gadījumu skaits, uzbūvētie ceļi km u. c.).
⁶⁴ Kā aprakstīts 1.4.2. punktā. “Konkrētais(-ie) mērķis(-i)...”

3.2.3. Paredzamā ietekme uz ENISA cilvēkresursiem

3.2.3.1. Kopsavilkums

Pārskatītās TID direktīvas rezultātā no 2022./2023. gada ENISA būs papildu uzdevumi. Lai gan uz šiem uzdevumiem attieksies ENISA pilnvarojums, tie aģentūrai radīs papildu darba slodzi. Tā, saskaņā ar Komisijas priekšlikumu par pārskatītu TID direktīvu ENISA papildus tās pašreizējiem uzdevumiem cita starpā tiks uzticēti šādi uzdevumi: i) izveidot un uzturēt Eiropas neaizsargātības reģistru (6. panta 2. punkts), ii) nodrošināt Eiropas Kiberkrīžu sadarbības organizāciju tīklu (CyCLONe) (14. pants) un izdot gada ziņojumu par situāciju kibernetikas jomā ES (15. pants), iii) atbalstīt salīdzinošās izvērtēšanas organizēšanu starp dalībvalstīm (16. pants), iv) savākt apkopotus incidentu datus no dalībvalstīm un izdot tehniskus norādījumus (20. panta 9. punkts), v) izveidot un uzturēt to vienību reģistru, kuras sniedz pārrobežu pakalpojumus (25. pants).

Tāpēc no 2022. gada tiks pieprasīti pieci papildu pilnslodzes ekvivalenti (FTE) ar atbilstošu budžetu, lai finansētu šīs jaunās amata vietas.

- ☐ Priekšlikums/iniciatīva neprasa izmantot administratīvas apropriācijas
- ☒ Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādi:

Miljonos EUR (līdz 3 zīmēm aiz komata)

	N gads ⁶⁵ 2022	N+1 gads 2023	N+2 gads 2024	N+3 gads 2025	Ierakstīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu) 2026 2027	KOPĀ
--	------------------------------	---------------------	---------------------	---------------------	--	------

Pagaidu darbinieki (AD kategorijas)	0,450	0,450	0,450	0,450	0,450	0,450	2,7
Pagaidu darbinieki (AST kategorijas)							
Līgumdarbinieki	0,160	0,160	0,160	0,160	0,160	0,160	0,96
Norīkoti valsts eksperti							

KOPĀ	0,61	0,61	0,61	0,61	0,61	0,61	3,66
-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------

Personāla vajadzības (FTE):

⁶⁵ N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, 2021.). Tas pats attiecas uz turpmākajiem gadiem.

	N gads ⁶⁶ 2022	N+1 gads 2023	N+2 gads 2024	N+3 gads 2025	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu) 2026 2027			KOPĀ
--	------------------------------	---------------------	---------------------	---------------------	--	--	--	------

Pagaidu darbinieki (AD kategorijas)	3	3	3	3	3	3		18
Pagaidu darbinieki (AST kategorijas)								
Līgumdarbinieki	2	2	2	2	2	2		12
Norīkotie valsts eksperti								

KOPĀ	5	5	5	5	5	5		30
------	---	---	---	---	---	---	--	----

3.2.3.2. Paredzamās cilvēkresursu vajadzības atbilstīgajam ĢD

- ☐ Priekšlikums/iniciatīva neprasa cilvēkresursu izmantošanu.
- ☐ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Paredzamais apmērs izsakāms veselos skaitļos (vai ar ne vairāk kā vienu ciparu aiz komata)

	N gads	N+1 gads	N+2 ga ds	N+3 gads	Ierakstīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)							
XX 01 01 01 (Galvenā mītne un Komisijas pārstāvniecības)							
XX 01 01 02 (Delegācijas)							
XX 01 05 01 (Netiešā pētniecība)							
10 01 05 01 (Tiešā pētniecība)							
• Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu — FTE) ⁶⁷							

⁶⁶ N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, 2021.). Tas pats attiecas uz turpmākajiem gadiem.

⁶⁷ AC – līgumdarbinieki, AL – vietējie darbinieki, END – valstu norīkotie eksperti, INT – aģentūru darbinieki, JPD – jaunākie speciālisti delegācijās.

XX 01 02 01 (AC, END, INT, ko finansē no vispārīgajām apropriācijām)							
XX 01 02 02 (AC, AL, END, INT un JPD delegācijās)							
XX 01 04 yy ⁶⁸	– galvenajā mītnē ⁶⁹						
	– delegācijās						
XX 01 05 02 (AC, END, INT – netiešā pētniecība)							
10 01 05 02 (AC, END, INT – tiešā pētniecība)							
Citas budžeta pozīcijas (precizēt)							
KOPĀ							

XX ir attiecīgā politikas joma vai budžeta sadaļa.

Vajadzīgie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau iesaistīti konkrētās darbības pārvaldībā un/vai pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts

Ierēdņi un pagaidu darbinieki	
Ārštata darbinieki	

FTE vienību izmaksu aprēķins jāiekļauj V pielikuma 3. iedaļā.

⁶⁸ Ārštata darbiniekiem paredzētā maksimālā summa, ko finansē no darbības apropriācijām (kādreizējām “BA” pozīcijām).

⁶⁹ Galvenokārt struktūrfondiem, Eiropas Lauksaimniecības fondam lauku attīstībai (ELFLA) un Eiropas Zivsaimniecības fondam (EZF).

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

- ☒ Priekšlikums/iniciatīva atbilst kārtējai daudzgadu finanšu shēmai
- ☐ Pieņemot priekšlikumu/iniciatīvu, jāpārplāno attiecīgā izdevumu kategorija daudzgadu finanšu shēmā

Aprakstīt, kas jāpārplāno, norādot attiecīgās budžeta pozīcijas un atbilstošās summas.

Priekšlikums ir saderīgs ar DFS 2021./2027. gadam.

Par ENISA cilvēkresursu palielinājuma finansēšanai pieprasītā budžeta summu tajā pašā izdevumu kategorijā tiks samazināts programmas “Digitālā Eiropa” (DEP) budžets.

- ☐ Pieņemot priekšlikumu/iniciatīvu, jāpiemēro elastības instruments vai jāpārskata daudzgadu finanšu shēma⁷⁰.

Aprakstīt, kas jādara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un atbilstošās summas.

3.2.5. Trešo personu iemaksas

- Priekšlikums/iniciatīva neparedz trešo personu līdzfinansējumu
- Priekšlikums/iniciatīva paredz šādu līdzfinansējumu:

Miljonos EUR (līdz 3 zīmēm aiz komata)

	N gads	N+1 gads	N+2 gads	N+3 gads	Ierakstīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			Kopā
Norādīt līdzfinansētāju struktūru								
Līdzfinansētās apropriācijas KOPĀ								

⁷⁰

Sk. Padomes Regulas (ES, Euratom) Nr. 1311/2013, ar ko nosaka daudzgadu finanšu shēmu 2014.–2020. gadam, 11. un 17. pantu.

3.3. Aplēstā ietekme uz ieņēmumiem

- ☐ Priekšlikums/iniciatīva ieņēmumus finansiāli neietekmē.
- ☐ Priekšlikums/iniciatīva finansiāli ietekmē:
 - ☐ pašu resursus
 - ☐ citus ieņēmumus
 - ☐ Norādiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām

Miljonos EUR (līdz 3 zīmēm aiz komata)

Budžeta pozīcija:	ieņēmumu	Kārtējā finanšu gadā pieejamās apropriācijas	Priekšlikuma/iniciatīvas ietekme ⁷¹						
			N gads	N+1 gads	N+2 gads	N+3 gads	Ierakstīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
..... pants									

Dažādiem novirzāmiem ("piešķirtajiem") ieņēmumiem norādīt attiecīgo(-ās) izdevumu pozīciju(-as).

Norādīt, pēc kādas metodes aprēķināta ietekme uz ieņēmumiem.

⁷¹

Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.