DIREKTĪVAS

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA (ES) 2022/2555

(2022. gada 14. decembris),

ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva)

(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 Centrālās bankas atzinumu ([1])

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu ([2]),

pēc apspriešanās ar Reģionu komiteju,

saskaņā ar parasto likumdošanas procedūru ([3]),

tā kā:

(1) Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/1148 ([4]) mērķis bija veidot kiberdrošības spējas Savienībā, mazināt draudus tīklu un informācijas sistēmām, ko izmanto pamatpakalpojumu sniegšanai svarīgās nozarēs, un nodrošināt šādu pakalpojumu nepārtrauktību, saskaroties ar incidentiem, un tādējādi sniedzot ieguldījumu Savienības drošībā un tās ekonomikas un sabiedrības efektīvā darbībā.

(2) Kopš Direktīvas (ES) 2016/1148 stāšanās spēkā Savienības kibernoturības līmeņa paaugstināšanā ir panākts ievērojams progress. Minētās direktīvas pārskatīšana apliecināja, ka tā ir kalpojusi par katalizatoru institucionālajai un regulatīvajai pieejai attiecībā uz kiberdrošību Savienībā, bruģējot ceļu būtiskām domāšanas veida pārmaiņām. Direktīva ir nodrošinājusi, ka tiek pabeigti tīklu un informācijas sistēmu drošības valstu satvari, nosakot valstu tīklu un informācijas sistēmu drošības stratēģijas, veidojot valstu spējas un īstenojot regulatīvus pasākumus, kas aptver būtiskas infrastruktūras un vienības, kuras identificējusi katra dalībvalsts. Direktīva (ES) 2016/1148 ir arī veicinājusi sadarbību Savienības līmenī, izveidojot sadarbības grupu un valstu datordrošības incidentu reaģēšanas vienību tīklu. Neraugoties uz šiem sasniegumiem, Direktīvas (ES) 2016/1148 pārskatīšanas gaitā ir konstatētas tai piemītošas nepilnības, kas liedz tai rezultatīvi risināt pašreizējās un jaunās kiberdrošības problēmas.

(3) Tīklu un informācijas sistēmas ir kļuvušas par būtisku iezīmi ikdienas dzīvē, ko raksturo ātra digitālā pārkārtošanās un sabiedrības savstarpējā savienotība, tai skaitā pārrobežu sakaros. Šīs attīstības rezultātā ir paplašinājusies kiberdraudu aina, rodoties jaunām problēmām, kurām ir vajadzīgi pielāgoti, koordinēti un inovatīvi reaģēšanas pasākumi visās dalībvalstīs. Incidentu skaits, apmērs, sarežģītība, biežums un ietekme pieaug un būtiski apdraud tīklu un informācijas sistēmu darbību. Līdz ar to incidenti var kavēt saimniecisko darbību īstenošanu iekšējā tirgū, radīt finansiālus zaudējumus, apdraudēt lietotāju uzticēšanos un radīt lielu kaitējumu Savienības ekonomikai un

([1]) OV C 233, 16.6.2022., 22. lpp.
([2]) OV C 286, 16.7.2021., 170. lpp.
([3]) Eiropas Parlamenta 2022. gada 10. novembra nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2022. gada 28. novembra lēmums.
([4]) 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, 19.7.2016., 1. lpp.).

sabiedrībai. Tāpēc sagatavotība un rezultativitāte kiberdrošības jomā tagad iekšējā tirgus pienācīgai darbībai ir vēl svarīgāka nekā jebkad iepriekš. Turklāt kiberdrošība daudzās kritiskās nozarēs ir būtisks faktors, kas dod iespēju sekmīgi īstenot digitālo pārkārtošanos un pilnībā izmantot digitalizācijas dotos saimnieciskos, sociālos un ilgtspējīgos ieguvumus.

(4) Direktīvas (ES) 2016/1148 juridiskais pamats bija Līguma par Eiropas Savienības darbību (LESD) 114. pants, kura mērķis ir nodrošināt iekšējā tirgus izveidi un darbību, uzlabojot valstu regulējumu tuvināšanas pasākumus. Kiberdrošības prasības, kas noteiktas vienībām, kuras sniedz pakalpojumus vai veic darbības, kuras ir ekonomiski nozīmīgas, ievērojami atšķiras starp dalībvalstīm prasību veida, detalizācijas līmeņa un uzraudzības metodes ziņā. Minētās atšķirības rada papildu izmaksas un grūtības vienībām, kas piedāvā preces vai pakalpojumus pāri robežām. Prasības, ko nosaka viena dalībvalsts un kas atšķiras no citas dalībvalsts noteiktajām prasībām vai pat ir pretrunā tām, var šādas pārrobežu darbības būtiski ietekmēt. Turklāt iespējai, ka kiberdrošības prasības vienā dalībvalstī nav adekvāti izstrādātas vai netiek adekvāti īstenotas, ļoti iespējams, var būt ietekme uz pārējo dalībvalstu kiberdrošības līmeni, jo īpaši ņemot vērā intensīvos pārrobežu sakarus. 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 deva dalībvalstīm ļoti plašu rīcības brīvību attiecībā uz tajā noteikto drošības un incidentu paziņošanas pienākumu ieviešanu. Tāpēc minētie pienākumi dalībvalstu līmenī tika ieviesti ļoti atšķirīgi. Līdzīgas atšķirības pastāv Direktīvas (ES) 2016/1148 noteikumu par uzraudzību un izpildes panākšanu ieviešanā.

(5) Visas šīs atšķirības sadrumstalo iekšējo tirgu un var prejudiciāli ietekmēt tā darbību, jo īpaši skarot pakalpojumu pārrobežu sniegšanu un kibernoturības līmeni dažādu pasākumu piemērošanas dēļ. Galu galā minētās atšķirības varētu novest pie lielākas dažu dalībvalstu ievainojamības pret kiberdraudiem un potenciālas plašākas ietekmes Savienībā. Šīs direktīvas mērķis ir izbeigt šādas plašas atšķirības starp dalībvalstīm, jo īpaši paredzot minimālos noteikumus par koordinēta tiesiskā regulējuma darbību, nosakot mehānismus rezultatīvai atbildīgo iestāžu sadarbībai katrā dalībvalstī, atjauninot to nozaru un darbību sarakstu, uz kurām attiecas kiberdrošības pienākumi, un paredzot iedarbīgus tiesiskās aizsardzības līdzekļus un izpildes panākšanas pasākumus, kas ir svarīgi rezultatīvai šo pienākumu izpildes panākšanai. Tāpēc Direktīva (ES) 2016/1148 būtu jāatceļ un jāaizstāj ar šo direktīvu.

(6) Līdz ar Direktīvas (ES) 2016/1148 atcelšanu būtu jāpaplašina piemērošanas joma pa nozarēm, aptverot lielāku ekonomikas daļu, lai nodrošinātu tādu nozaru un pakalpojumu pilnīgu aptvērumu, kas ir izšķirīgi svarīgas būtiskām sabiedriskajām un saimnieciskajām darbībām iekšējā tirgū. Šī direktīva jo īpaši tiecas novērst trūkumus, kas saistīti ar pamatpakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju diferenciāciju, kura ir izrādījusies novecojusi, jo neatspoguļo nozaru vai pakalpojumu nozīmīgumu sabiedriskajām un saimnieciskajām darbībām iekšējā tirgū.

(7) Saskaņā ar Direktīvu (ES) 2016/1148 dalībvalstīm bija pienākums identificēt vienības, kuras atbilst kritērijiem, lai tās varētu uzskatīt par pamatpakalpojumu sniedzējiem. Lai šajā ziņā mazinātu lielās atšķirības starp dalībvalstīm un nodrošinātu juridisko noteiktību attiecībā uz kiberdrošība risku pārvaldības pasākumiem un ziņošanas pienākumiem visām attiecīgajām vienībām, būtu jāievieš vienots kritērijs tādu vienību noteikšanai, kuras ietilpst šīs direktīvas darbības jomā. Minētajam kritērijam vajadzētu būt maksimālā lieluma noteikumam, saskaņā ar kuru visas vienības, kas kvalificējas kā vidējie uzņēmumi saskaņā ar Komisijas Ieteikuma 2003/361/EK ([5]) pielikuma 2. pantu vai pārsniedz vidējiem uzņēmumiem noteiktos maksimālos lielumus, kuri paredzēti minētā panta 1. punktā, un kas darbojas šīs direktīvas aptvertajās nozarēs un sniedz tās aptvertos pakalpojumus, vai veic tās aptvertās darbības,

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

ietilpst tās darbības jomā. Dalībvalstīm būtu arī jāparedz, ka šīs direktīvas darbības jomā ietilpst konkrēti mazie uzņēmumi un mikrouzņēmumi, kā definēts minētā pielikuma 2. panta 2. un 3. punktā, kas atbilst konkrētiem kritērijiem, kuri liecina par svarīgu lomu sabiedrībā, ekonomikā vai konkrētās nozarēs vai pakalpojumu veidos.

(8) Valsts pārvaldes vienību izslēgšana no šīs direktīvas darbības jomas būtu jāpiemēro vienībām, kuru darbības galvenokārt tiek veiktas valsts drošības, sabiedriskās drošības, aizsardzības vai tiesībaizsardzības jomā, tostarp noziedzīgu nodarījumu novēršanā, izmeklēšanā, atklāšanā un kriminālvajāšanā par tiem. Tomēr no šīs direktīvas darbības jomas nebūtu jāizslēdz valsts pārvaldes vienības, kuru darbības ir tikai maznozīmīgi saistītas ar minētajām jomām. Šajā direktīvā vienības, kam ir regulatīva kompetence, neuzskata par tādām, kas veic darbības tiesībaizsardzības jomā, un tāpēc tās nav izslēgtas no šīs direktīvas darbības jomas. No šīs direktīvas darbības jomas ir izslēgtas valsts pārvaldes vienības, kas ir izveidotas kopīgi ar trešo valsti saskaņā ar starptautisku nolīgumu. Šo direktīvu nepiemēro dalībvalstu diplomātiskajām un konsulārajām pārstāvniecībām trešās valstīs vai to tīklu un informācijas sistēmām, ciktāl šādas sistēmas atrodas pārstāvniecības telpās vai ir paredzētas lietotājiem trešā valstī.

(9) Dalībvalstīm būtu jāspēj veikt nepieciešamos pasākumus, lai nodrošinātu būtisko valsts drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrisko drošību un lai varētu novērst, izmeklēt un atklāt noziedzīgus nodarījumus un veikt kriminālvajāšanu par tiem. Šajā nolūkā dalībvalstīm būtu jāspēj paredzēt, ka konkrētas vienības, kas veic darbības valsts drošības, sabiedriskās drošības, aizsardzības vai tiesībaizsardzības jomā, tostarp noziedzīgu nodarījumu novēršanā, izmeklēšanā, atklāšanā un kriminālvajāšanā par tiem, ir atbrīvotas no dažiem šajā direktīvā noteiktajiem pienākumiem attiecībā uz minētajām darbībām. Ja vienība sniedz pakalpojumus tikai valsts pārvaldes vienībai, kas ir izslēgta no šīs direktīvas darbības jomas, dalībvalstīm būtu jāspēj atbrīvot minēto vienību no dažiem šajā direktīvā noteiktajiem pienākumiem attiecībā uz minētajiem pakalpojumiem. Turklāt nevajadzētu būt prasībai dalībvalstīm sniegt informāciju, kuras izpaušana būtu pretrunā to būtiskajām valsts drošības, sabiedriskās drošības vai aizsardzības interesēm. Šajā ziņā būtu jāņem vērā Savienības vai valstu noteikumi par klasificētas informācijas aizsardzību, vienošanās par neizpaušanu un neformālas vienošanās par informācijas neizpaušanu, piemēram, gaismas signālu protokols. Gaismas signālu protokols ir jāsaprot kā līdzeklis, ar ko sniegt informāciju par jebkādiem ierobežojumiem attiecībā uz tālāku informācijas izplatīšanu. To izmanto gandrīz visās datordrošības incidentu reaģēšanas vienībās (*CSIRT*) un dažos informācijas analīzes un kopīgošanas centros.

(10) Lai gan šī direktīva attiecas uz vienībām, kas veic darbības elektroenerģijas ražošanā kodolelektrostacijās, dažas no minētajām darbībām var būt saistītas ar valsts drošību. Ja tā ir, dalībvalstij būtu jāspēj pildīt savu pienākumu sargāt valsts drošību attiecībā uz minētajām darbībām, tostarp darbībām kodolenerģijas vērtības ķēdē, saskaņā ar Līgumiem.

(11) Dažas vienības veic darbības valsts drošības, sabiedriskās drošības, aizsardzības vai tiesībaizsardzības jomā, tostarp noziedzīgu nodarījumu novēršanā, izmeklēšanā, atklāšanā un kriminālvajāšanā par tiem, bet vienlaikus sniedz arī uzticamības pakalpojumus. Uzticamības pakalpojumu sniedzējiem, kas ietilpst Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 ([6]) darbības jomā, būtu jāietilpst šīs direktīvas darbības jomā, lai nodrošinātu tādu pašu drošības prasību un uzraudzības līmeni, kāds iepriekš bija noteikts minētajā regulā attiecībā uz uzticamības pakalpojumu sniedzējiem. Atbilstoši dažu konkrētu pakalpojumu izslēgšanai no Regulas (ES) Nr. 910/2014 darbības jomas šo direktīvu nevajadzētu piemērot tādu uzticamības pakalpojumu sniegšanai, kurus izmanto vienīgi slēgtās sistēmās, kas izriet no valsts tiesību aktiem vai nolīgumiem starp noteiktu dalībnieku kopu.

([6]) 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.).

(12) Pasta pakalpojumu sniedzēji, kā tie definēti Eiropas Parlamenta un Padomes Direktīvā 97/67/EK ([7]), tostarp kurjerpiegādes pakalpojumu sniedzēji, šīs direktīvas darbības jomā būtu jāiekļauj tad, ja tie nodrošina vismaz vienu no posmiem pasta piegādes ķēdē, jo īpaši, ja tie sniedz pasta sūtījumu atmuitošanas, šķirošanas, transporta vai sadales pakalpojumus, tostarp savākšanas pakalpojumus, bet vienlaikus būtu jāņem vērā tas, kādā mērā tie ir atkarīgi no tīklu un informācijas sistēmām. Transporta pakalpojumi, kuros neveic saistībā ar kādu no minētajiem posmiem, no pasta pakalpojumu jomas būtu jāizslēdz.

(13) Ņemot vērā kiberdraudu pastiprināšanos un pieaugošo sarežģītību, dalībvalstīm būtu jācenšas nodrošināt, ka vienības, kas ir izslēgtas no šīs direktīvas darbības jomas, sasniedz augstu kiberdrošības līmeni, un atbalstīt tādu līdzvērtīgu kiberdrošības riska pārvaldības pasākumu īstenošanu, kas atbilst minēto vienību sensitīvajam raksturam.

(14) Jebkādai persondatu apstrādei saskaņā ar šo direktīvu piemēro Savienības datu aizsardzības tiesību aktus un Savienības privātuma tiesību aktus. Konkrētāk, šī direktīva neskar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([8]) un Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([9]). Tādēļ šai direktīvai cita starpā nebūtu jāskar tādu iestāžu uzdevumi un pilnvaras, kuras ir kompetentas uzraudzīt atbilstību piemērojamajiem Savienības datu aizsardzības tiesību aktiem un Savienības privātuma tiesību aktiem.

(15) Vienības, kuras ietilpst šīs direktīvas darbības jomā, attiecībā uz atbilstību kiberdrošības risku pārvaldības pasākumiem un ziņošanas pienākumiem būtu jāiedala divās kategorijās, proti, būtiskajās vienībās un svarīgajās vienībās, atspoguļojot to, kādā mērā tās ir kritiski svarīgas to nozares vai sniegto pakalpojumu veida aspektā, kā arī to lielumu. Minētajā sakarā attiecīgā gadījumā būtu pienācīgi jāņem vērā visi attiecīgie nozaru riska novērtējumi vai norādījumi, ko sniegušas kompetentās iestādes. Uzraudzības un izpildes režīmi minētajām divām vienību kategorijām būtu jādiferencē, lai nodrošinātu taisnīgu līdzsvaru starp prasībām un pienākumiem, kas balstīti uz risku, no vienas puses, un administratīvo slogu, kas izriet no atbilstības uzraudzības, no otras puses.

(16) Lai izvairītos no tā, ka vienības, kurām ir partneruzņēmumi vai kuras ir saistīti uzņēmumi, tiek uzskatītas par būtiskām vai svarīgām vienībām, ja tas būtu nesamērīgi, dalībvalstis, piemērojot Ieteikuma 2003/361/EK pielikuma 6. panta 2. punktu, var ņemt vērā vienības neatkarības pakāpi attiecībā pret tās partneri vai saistītajiem uzņēmumiem. Konkrētāk, dalībvalstis var ņemt vērā to, ka vienība ir neatkarīga no sava partnera vai saistītajiem uzņēmumiem to tīklu un informācijas sistēmu ziņā, ko šī vienība izmanto savu pakalpojumu sniegšanā, un tās sniegto pakalpojumu ziņā. Uz šā pamata attiecīgā gadījumā dalībvalstis var uzskatīt, ka šāda vienība nekvalificējas kā vidējs uzņēmums saskaņā ar Ieteikuma 2003/361/EK 2. pantu vai nepārsniedz minētā panta 1. punktā paredzētos maksimālos lielumus vidējiem uzņēmumiem, ja pēc tam, kad ir ņemta vērā šīs vienības neatkarības pakāpe, tiktu uzskatīts, ka šī vienība nekvalificētos kā vidējs uzņēmums vai nepārsniegtu minētos maksimālos lielumus, ja tiktu ņemti vērā tikai tās pašas dati vien. Tas neskar šajā direktīvā noteiktos to partneru un saistīto uzņēmumu pienākumus, kuri ietilpst šīs direktīvas darbības jomā.

(17) Dalībvalstīm būtu jāspēj nolemt, ka vienības, kas pirms šīs direktīvas stāšanās spēkā identificētas kā pamatpakalpojumu sniedzēji saskaņā ar Direktīvu (ES) 2016/1148, ir uzskatāmas par būtiskām vienībām.

([7]) 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.).

([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.).

([9]) 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.).

(18) Lai nodrošinātu skaidru pārskatu par vienībām, kas ir šīs direktīvas darbības jomā, dalībvalstīm būtu jāizveido saraksts ar būtiskajām un svarīgajām vienībām, kā arī vienībām, kuras sniedz domēnu nosaukumu reģistrācijas pakalpojumus. Minētajā nolūkā dalībvalstīm būtu jāprasa, lai vienības kompetentajām iestādēm iesniedz vismaz šādu informāciju: nosaukumu, adresi un atjauninātu kontaktinformāciju, tostarp vienības e-pasta adreses, IP adrešu diapazonus un tālruņa numurus, un attiecīgā gadījumā pielikumos minētās attiecīgās nozares un apakšnozares, kā arī attiecīgā gadījumā to dalībvalstu sarakstu, kurās tās sniedz pakalpojumus, kas ietilpst šīs direktīvas darbības jomā. Šajā nolūkā Komisijai ar Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) palīdzību bez nepamatotas kavēšanās būtu jāsniedz pamatnostādnes un veidnes attiecībā uz pienākumu iesniegt informāciju. Lai atvieglotu būtisko un svarīgo vienību, kā arī vienību, kuras sniedz domēnu nosaukumu reģistrācijas pakalpojumus, saraksta izveidi un atjaunināšanu, dalībvalstīm būtu jāspēj izveidot valsts mehānismus, ko vienības varētu izmantot, lai reģistrētos pašas. Ja pastāv valsts līmeņa reģistri, dalībvalstis var lemt par piemērotiem mehānismiem, kas ļauj identificēt vienības, kuras ietilpst šīs direktīvas darbības jomā.

(19) Dalībvalstīm vajadzētu būt atbildīgām par to, lai Komisijai tiktu iesniegts vismaz to būtisko un svarīgo vienību skaits katrā nozarē un apakšnozarē, kas minētas pielikumos, kā arī relevanta informācija par identificēto vienību skaitu un to no šajā direktīvā paredzētajiem noteikumiem, uz kura pamata tās identificētas, un pakalpojumu veidu, ko tās sniedz. Dalībvalstis tiek mudinātas ar Komisiju apmainīties ar informāciju par būtiskajām un svarīgajām vienībām un – liela mēroga kiberdrošības incidenta gadījumā – ar relevantu informāciju, piemēram, attiecīgās vienības nosaukumu.

(20) Komisijai sadarbībā ar sadarbības grupu un pēc apspriešanās ar attiecīgajām ieinteresētajām personām būtu jāsniedz pamatnostādnes par to, kā īstenot mikrouzņēmumiem un mazajiem uzņēmumiem piemērojamos kritērijus, pēc kuriem novērtēt, vai tie ietilpst šīs direktīvas darbības jomā. Komisijai būtu arī jānodrošina, ka piemēroti norādījumi tiek sniegti mikrouzņēmumiem un mazajiem uzņēmumiem, kuri ietilpst šīs direktīvas darbības jomā. Komisijai ar dalībvalstu palīdzību būtu minētajā nolūkā jādara pieejama informācija mikrouzņēmumiem un mazajiem uzņēmumiem.

(21) Komisija varētu sniegt norādījumus, lai palīdzētu dalībvalstīm īstenot šīs direktīvas noteikumus par darbības jomu un izvērtēt saskaņā ar šo direktīvu veicamo pienākumu proporcionalitāti, jo īpaši attiecībā uz vienībām ar sarežģītiem uzņēmējdarbības modeļiem vai darbības vidēm, kur vienība vienlaikus var atbilst kritērijiem, kas noteikti gan būtiskām, gan svarīgām vienībām, vai vienlaikus veikt darbības, no kurām daļa ietilpst šīs direktīvas darbības jomā, bet citas no tās ir izslēgtas.

(22) Šajā direktīvā ir noteikts pamats kiberdrošības risku pārvaldības pasākumiem un ziņošanas pienākumiem nozarēs, kas ietilpst tās darbības jomā. Lai izvairītos no Savienības tiesību aktos paredzēto kiberdrošības noteikumu sadrumstalotības, ja tiek uzskatīts, ka augsta kiberdrošības līmeņa nodrošināšanai Savienībā ir nepieciešami papildu nozarspecifiski Savienības tiesību akti, kas attiecas uz kiberdrošības risku pārvaldības pasākumiem un ziņošanas pienākumiem, Komisijai būtu jānovērtē, vai šādus papildu noteikumus varētu paredzēt īstenošanas aktā saskaņā ar šo direktīvu. Ja šāds īstenošanas akts minētajam nolūkam nav piemērots, nozarspecifiski Savienības tiesību akti varētu palīdzēt nodrošināt Savienībā augstu kiberdrošības līmeni, vienlaikus pilnībā ņemot vērā attiecīgo nozaru specifiku un sarežģītību. Šajā nolūkā šī direktīva neliedz pieņemt papildu nozarspecifiskus Savienības tiesību aktus, kas pievēršas kiberdrošības risku pārvaldības pasākumiem un ziņošanas pienākumiem un kas pienācīgi ņem vērā nepieciešamību pēc vispusīgas un konsekventas kiberdrošības sistēmas. Šī direktīva neskar pastāvošās īstenošanas pilnvaras, kas Komisijai piešķirtas vairākās nozarēs, tai skaitā transporta un enerģētikas nozarē.

(23) Ja nozarspecifiska Savienības tiesību akta noteikumi prasa būtiskajām vai svarīgajām vienībām pieņemt kiberdrošības risku pārvaldības pasākumus vai ziņot par būtiskiem incidentiem un ja šādas prasības to ietekmes ziņā ir vismaz līdzvērtīgas šajā direktīvā noteiktajiem pienākumiem, minētos noteikumus, tostarp noteikumus par uzraudzību un

izpildes panākšanu, būtu jāpiemēro šādām vienībām. Ja nozarspecifisks Savienības tiesību akts neaptver visas vienības konkrētā nozarē, kas ietilpst šīs direktīvas darbības jomā, attiecīgos šīs direktīvas būtu jāturpina piemērot vienībām, uz kurām minētais akts neattiecas.

(24) Ja nozarspecifiska Savienības tiesību akta noteikumi prasa, lai būtiskās vai svarīgās vienības izpilda ziņošanas prasības, kuras iedarbības ziņā ir vismaz līdzvērtīgas šajā direktīvā noteiktajiem ziņošanas pienākumiem, būtu jānodrošina incidentu paziņojumu apstrādes saskaņotība un rezultativitāte. Minētajā nolūkā nozarspecifiska Savienības tiesību akta noteikumiem saistībā ar incidentu paziņošanu būtu jānodrošina *CSIRT*, kompetentajām iestādēm vai vienotajiem kiberdrošības kontaktpunktiem (vienotie kontaktpunkti), ko paredz šī direktīva, tūlītēja piekļuve paziņojumiem par incidentiem, kas iesniegti saskaņā ar nozarspecifisko Savienības tiesību aktu. Konkrētāk, šādu tūlītēju piekļuvi var nodrošināt, ja incidentu paziņojumi bez nepamatotas kavēšanās tiek nosūtīti *CSIRT*, kompetentajai iestādei vai vienotajam kontaktpunktam, ko paredz šī direktīva. Attiecīgā gadījumā dalībvalstīm būtu jāievieš automātisks un tiešs ziņošanas mehānisms, kas nodrošina sistemātisku un tūlītēju informācijas kopīgošanu ar *CSIRT*, kompetentajām iestādēm vai vienotajiem kontaktpunktiem attiecībā uz šādu incidentu paziņojumu apstrādi. Lai vienkāršotu ziņošanu un ieviestu automātiskās un tiešās ziņošanas mehānismu, dalībvalstis saskaņā ar nozarspecifisko Savienības tiesību aktu varētu izmantot vienotu iesniegšanas punktu.

(25) Nozarspecifiskos Savienības tiesību aktos, kas paredz kiberdrošības risku pārvaldības pasākumus vai ziņošanas pienākumus, kuri iedarbības ziņā ir vismaz līdzvērtīgi tiem, kas noteikti šajā direktīvā, varētu paredzēt, ka kompetentās iestādes, ko paredz šādi akti, savas uzraudzības un izpildes panākšanas pilnvaras attiecībā uz šādiem pasākumiem vai pienākumiem īsteno ar šajā direktīvā minēto kompetento iestāžu palīdzību. Attiecīgās kompetentās iestādes šajā nolūkā varētu izveidot sadarbības mehānismus. Šādos sadarbības mehānismos cita starpā varētu precizēt uzraudzības darbību koordinēšanas procedūras, tostarp izmeklēšanas un uz vietas veicamu inspekciju procedūras saskaņā ar valsts tiesību aktiem, un mehānismu relevantas informācijas apmaiņai starp kompetentajām iestādēm par uzraudzību un izpildes panākšanu, tostarp piekļuvi ar kiberjautājumiem saistītai informācijai, ko pieprasa šajā direktīvā minētās kompetentās iestādes.

(26) Ja nozarspecifiski Savienības tiesību akti prasa vai rada stimulus vienībām paziņot par būtiskiem kiberdraudiem, dalībvalstīm būtu jāmudina informācijā par būtiskiem kiberdraudiem dalīties arī ar šajā direktīvā paredzētajām *CSIRT*, kompetentajām iestādēm vai vienotajiem kontaktpunktiem, lai nodrošinātu minēto struktūru labāku informētību par kiberdraudu ainu un lai tās varētu rezultatīvi un savlaicīgi reaģēt, ja būtiskie kiberdraudi īstenotos.

(27) Turpmākos nozarspecifiskos Savienības tiesību aktos būtu pienācīgi jāņem vērā šajā direktīvā noteiktās definīcijas un uzraudzības un izpildes panākšanas sistēma.

(28) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 ([10]) būtu jāuzskata par nozarspecifisku Savienības tiesību aktu saistībā ar šo direktīvu attiecībā uz finanšu vienībām. Šajā direktīvā izklāstīto noteikumu vietā būtu jāpiemēro Regulas (ES) 2022/2554 noteikumi par informācijas un komunikācijas tehnoloģiju (IKT) risku pārvaldību, ar IKT saistītu incidentu pārvaldību un jo īpaši lielu ar IKT saistītu incidentu paziņošanu, kā arī par digitālās darbības noturības testēšanu, informācijas kopīgošanas mehānismiem un ar trešo personu saistītu IKT risku. Tāpēc dalībvalstīm šīs direktīvas noteikumi par kiberdrošības risku pārvaldību un ziņošanas pienākumiem, kā arī uzraudzību un izpildes panākšanu nebūtu jāpiemēro finanšu vienībām, uz kurām attiecas Regula (ES) 2022/2554. Vienlaikus ir svarīgi uzturēt ciešas attiecības un informācijas apmaiņu ar finanšu sektoru saskaņā ar šo direktīvu. Šajā nolūkā Regula (ES) 2022/2554 Eiropas uzraudzības iestādēm (EUI) un kompetentajām iestādēm saskaņā ar minēto regulu dod iespēju piedalīties sadarbības grupas darbībās un apmainīties ar informāciju un sadarboties ar vienotajiem kontaktpunktiem, kā arī ar *CSIRT* un kompetentajām iestādēm saskaņā ar šo direktīvu. Kompetentajām iestādēm atbilstoši Regulai (ES) 2022/2554 arī būtu jānosūta ziņas par būtiskiem ar IKT saistītiem incidentiem un, attiecīgā gadījumā, par būtiskiem kiberdraudiem *CSIRT*, kompetentajām iestādēm vai vienotajiem kontaktpunktiem,

([10]) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (skatīt šā *Oficiālā Vēstneša* 1.. lpp.).

kas minēti šajā direktīvā. To var panākt, nodrošinot tūlītēju piekļuvi paziņojumiem par incidentiem un tos pārsūtot vai nu tieši, vai izmantojot vienotu iesniegšanas punktu. Turklāt dalībvalstīm arī turpmāk būtu jāiekļauj finanšu sektors savās kiberdrošības stratēģijās, un *CSIRT* savās darbībās var aptvert finanšu sektoru.

(29) Lai izvairītos no aviācijas nozares vienībām piemēroto kiberdrošības pienākumu nepilnībām vai dublēšanās, Eiropas Parlamenta un Padomes Regulā (EK) Nr. 300/2008 ([11]) un Regulā (ES) 2018/1139 paredzētajām ([12]) valsts iestādēm un šajā direktīvā paredzētajām kompetentajām iestādēm būtu jāsadarbojas saistībā ar kiberdrošības risku pārvaldības pasākumu īstenošanu un atbilstības minētajiem pasākumiem uzraudzību valsts līmenī. Šajā direktīvā paredzētās kompetentās iestādes varētu uzskatīt, ka vienības atbilstība drošības prasībām, kuras noteiktas Regulās (EK) Nr. 300/2008 un (ES) 2018/1139 un attiecīgajos deleģētajos un īstenošanas aktos, kas pieņemti, ievērojot minētās regulas, nozīmē atbilstību attiecīgajām šajā direktīvā noteiktajām prasībām.

(30) Ņemot vērā saiknes starp vienību kiberdrošību un fizisko drošību, būtu jānodrošina, ka Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2557 ([13]) un šīs direktīvas pieejas ir saskanīgas. Lai to panāktu, vienības, kas identificētas kā kritiskās vienības saskaņā ar Direktīvu (ES) 2022/2557, būtu jāuzskata par būtiskām vienībām saskaņā ar šo direktīvu. Turklāt katrai dalībvalstij būtu jānodrošina, ka tās valsts kiberdrošības stratēģijā ir paredzēts rīcībpolitikas satvars pastiprinātai koordinācijai minētajā dalībvalstī starp tās kompetentajām iestādēm saskaņā ar šo direktīvu un kompetentajām iestādēm saskaņā ar Direktīvu (ES) 2022/2557 tādas informācijas kopīgošanas kontekstā, kas attiecas uz riskiem, kiberdraudiem un incidentiem, kā arī ar kiberdrošību nesaistītiem riskiem, draudiem un incidentiem un uzraudzības uzdevumu veikšanu. Šajā direktīvā paredzētajām kompetentajām iestādēm un Direktīvā (ES) 2022/2557 paredzētajām kompetentajām iestādēm būtu jāsadarbojas un jāapmainās ar informāciju bez nepamatotas kavēšanās, jo īpaši attiecībā uz kritisko vienību noteikšanu, riskiem, kiberdraudiem un incidentiem, kā arī attiecībā uz ar kiberdrošību nesaistītiem riskiem, draudiem un incidentiem, kas ietekmē kritiskās vienības, tostarp kiberdrošības un fiziskiem pasākumiem, ko veikušas kritiskās vienības, kā arī attiecībā uz šādām vienībām veikto uzraudzības darbību rezultātiem.

Turklāt, lai racionalizētu uzraudzības darbības starp šajā direktīvā paredzētajām kompetentajām iestādēm un Direktīvā (ES) 2022/2557 paredzētajām kompetentajām iestādēm, un lai attiecīgajām vienībām mazinātu administratīvo slogu, minētajām kompetentajām iestādēm būtu jācenšas saskaņot incidentu paziņošanas veidnes un uzraudzības procesus. Attiecīgā gadījumā Direktīvā (ES) 2022/2557 paredzētajām kompetentajām iestādēm būtu jāspēj pieprasīt šajā direktīvā paredzētajām kompetentajām iestādēm īstenot savas uzraudzības un izpildes panākšanas pilnvaras attiecībā uz vienību, kas ir identificēta kā kritiska vienība saskaņā ar Direktīvu (ES) 2022/2557 Šajā nolūkā šajā direktīvā paredzētajām kompetentajām iestādēm un Direktīvā (ES) 2022/2557 paredzētajām kompetentajām iestādēm būtu jāsadarbojas un jāapmainās ar informāciju, ja iespējams – reāllaikā.

(31) Vienības, kas pieder pie digitālās infrastruktūras nozares, būtībā balstās uz tīklu un informācijas sistēmām, un tāpēc ar pienākumiem, kas minētajām vienībām paredzēti šajā direktīvā, būtu visaptveroši jāpievēršas šādu sistēmu fiziskajai drošībai kā daļai no to kiberdrošības risku pārvaldības pasākumiem un ziņošanas pienākumiem. Tā kā šī direktīva aptver minētos jautājumus, Direktīvas (ES) 2022/2557 II, IV un VI nodaļā noteiktos pienākumus šādām vienībām nepiemēro.

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

([12]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1139 (2018. gada 4. jūlijs) par kopīgiem noteikumiem civilās aviācijas jomā un ar ko izveido Eiropas Savienības Aviācijas drošības aģentūru, un ar ko groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 2111/2005, (EK) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 un Direktīvas 2014/30/ES un 2014/53/ES un atceļ Eiropas Parlamenta un Padomes Regulas (EK) Nr. 552/2004 un (EK) Nr. 216/2008 un Padomes Regulu (EEK) Nr. 3922/91 (OV L 212, 22.8.2018., 1. lpp.).

([13]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2557 (2022. gada 14. decembris) par kritisko vienību noturību un ar ko atceļ Padomes Direktīvu 2008/114/EK (skatīt šā *Oficiālā Vēstneša* 164.. lpp.).

(32) Uzticamas, noturīgas un drošas domēnu nosaukumu sistēmas (DNS) veicināšana un saglabāšana ir svarīgs faktors interneta integritātes uzturēšanā un ir svarīga tā nepārtrauktai un stabilai darbībai, no kuras ir atkarīga digitālā ekonomika un sabiedrība. Tāpēc šī direktīva būtu jāpiemēro augstākā līmeņa domēnu (ALD) nosaukumu reģistriem un DNS pakalpojumu sniedzējiem, kas jāsaprot kā vienības, kas sniedz publiski pieejamus interneta galalietotājiem domātus rekursīvu domēnu nosaukumu atrises pakalpojumus vai autoritatīvu domēnu nosaukumu atrises pakalpojumus trešām personām. Šī direktīva nebūtu jāpiemēro saknes nosaukumu serveriem.

(33) Mākoņdatošanas pakalpojumiem būtu jāaptver digitāli pakalpojumi, kas dod iespēju plaši un attālināti piekļūt kopīgojamu datošanas resursu mērogojamam un elastīgam pūlam un pēc pieprasījuma to pārvaldīt, arī tad, ja šādi resursi ir izvietoti vairākās vietās. Datošanas resursi ietver tādus resursus kā tīkli, serveri vai cita infrastruktūra, operētājsistēmas, programmatūra, glabāšana, lietotnes un pakalpojumi. Mākoņdatošanas pakalpojumu modeļi cita starpā ietver infrastruktūru kā pakalpojumu (*IaaS*), platformu kā pakalpojumu (*PaaS*), programmatūru kā pakalpojumu (*SaaS*) un tīklu kā pakalpojumu (*NaaS*). Mākoņdatošanas izvietošanas modeļos būtu jāiekļauj privāts, kopienas, publisks un hibrīds mākonis. Mākoņdatošanas pakalpojumu un izvietošanas modeļu nozīme ir tāda pati kā terminiem "pakalpojums" un "izvietošanas modeļi" standartā ISO/IEC 17788:2014. Mākoņdatošanas lietotāja spēju vienpusēji sev nodrošināt datošanas spējas, piemēram, servera laiku vai glabāšanu tīklā, bez cilvēka mijiedarbības ar mākoņpakalpojumu sniedzēju varētu raksturot kā pārvaldību pēc pieprasījuma.

Termins "plaša un attālināta piekļuve" ir izmantots, lai raksturotu to, ka mākoņdatošanas spējas tiek nodrošinātas visā tīklā un tām piekļūst, izmantojot mehānismus, kas veicina neviendabīgu plāno vai biezo klientiem paredzēto platformu, tai skaitā mobilo tālruņu, planšetdatoru, klēpjdatoru un darbstaciju, izmantošanu. Termins "mērogojams" attiecas uz datošanas resursiem, kurus mākoņpakalpojuma sniedzējs elastīgi piešķir neatkarīgi no resursu ģeogrāfiskās atrašanās vietas, lai risinātu pieprasījuma svārstības. Termins "elastīgs pūls" ir izmantots, lai aprakstītu tos datošanas resursus, kuri tiek nodrošināti un atbrīvoti atbilstoši pieprasījumam, lai pieejamos resursus atkarībā no noslodzes ātri palielinātu vai samazinātu. Termins "kopīgojams" ir izmantots, lai aprakstītu datošanas resursus, kas tiek sniegti daudziem lietotājiem, kuriem ir kopīga piekļuve pakalpojumam, bet apstrāde notiek katram lietotājam atsevišķi, kaut arī pakalpojums tiek sniegts no vienas un tās pašas elektroniskās iekārtas. Termins "sadalīts" ir izmantots, lai aprakstītu datošanas resursus, kas atrodas dažādos tīklotos datoros vai ierīcēs un kas īsteno savstarpēju saziņu un koordināciju, izmantojot ziņojumu sūtīšanu.

(34) Ņemot vērā inovatīvu tehnoloģiju un jaunu darbības modeļu parādīšanos, paredzams, ka, reaģējot uz jaunām klientu vajadzībām, iekšējā tirgū parādīsies jauni mākoņdatošanas pakalpojumu un izvietošanas modeļi. Šajā kontekstā mākoņpakalpojumi var būt sniegti īpaši sadalītā formā, pat tuvāk vietai, kur dati tiek ģenerēti vai savākti, tādējādi pārejot no tradicionālā modeļa uz īpaši sadalītu modeli ("perifērdatošana").

(35) Pakalpojumi, ko piedāvā datu centru pakalpojumu sniedzēji, ne vienmēr tiek sniegti mākoņpakalpojuma veidā. Tas nozīmē, ka datu centri var nebūt daļa no mākoņdatošanas infrastruktūras. Tāpēc, lai pārvaldītu visus riskus tīklu un informācijas sistēmu drošībai, šī direktīva būtu jāattiecina arī uz tādu datu centru pakalpojumu sniedzējiem, kuri nav mākoņpakalpojumi. Šajā direktīvā termins "datu centra pakalpojums" būtu jāattiecina uz tāda pakalpojuma sniegšanu, kas ietver struktūras vai struktūru grupas, kuras paredzētas tāda informācijas tehnoloģiju (IT) 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. Terminam "datu centra pakalpojums" nebūtu jāattiecas uz iekšējiem korporatīviem datu centriem, ko attiecīgā vienība tur īpašumā un ekspluatē savām vajadzībām.

(36) Pētniecības darbībām ir būtiska loma jaunu produktu un procesu izstrādē. Daudzas no minētajām darbībām veic vienības, kas savu pētījumu rezultātus kopīgo, izplata vai izmanto komerciāliem mērķiem. Tāpēc minētās vienības var būt svarīgi vērtības ķēžu dalībnieki, un tas nozīmē, ka to tīklu un informācijas sistēmu drošība ir iekšējā tirgus vispārējās kiberdrošības neatņemama daļa. Pētniecības organizācijas būtu jāsaprot kā citu starpā tādas vienības, kuru darbību būtiskā daļa ir vērsta uz lietišķo pētniecību vai eksperimentālo izstrādi – kā tā saprasta Ekonomiskās

sadarbības un attīstības organizācijas 2015. gada *Frascati* rokasgrāmatā par pētniecības un eksperimentālās izstrādes datu vākšanas un ziņošanas pamatnostādnēm –, lai to rezultātus izmantotu komerciāliem mērķiem, piemēram, produkta ražošanai vai produkta vai procesa izstrādei, vai pakalpojuma sniegšanai, vai to tirdzniecībai.

(37) Pieaugošā savstarpējā atkarība izriet no tā, ka pakalpojumu sniegšanas tīklam aizvien lielākā mērā ir pārrobežu raksturs un piemīt savstarpējā atkarība, proti, tas izmanto pamata infrastruktūras visā Savienībā tādās nozarēs kā enerģētika, transports, digitālā infrastruktūra, dzeramais ūdens un notekūdeņi, veselība, konkrēti valsts pārvaldes aspekti, kā arī kosmoss, ciktāl runa ir par tādu konkrētu pakalpojumu sniegšanu, kuri ir atkarīgi no virszemes infrastruktūrām, ko tur īpašumā, pārvalda vai ekspluatē dalībvalstis vai privātas puses, tādējādi neaptverot infrastruktūras, ko tur īpašumā, pārvalda vai ekspluatē Savienība vai tās vārdā kā daļu no tās kosmosa programmas. Šī savstarpējā atkarība nozīmē, ka jebkuram traucējumam, pat tādam, kas sākotnēji skar tikai vienu vienību vai vienu nozari, var būt plašāka lavīnveida ietekme, kura potenciāli var izraisīt tālejošas un ilgstošas negatīvas sekas pakalpojumu sniegšanā iekšējā tirgū. Kiberuzbrukumu pastiprināšanās Covid-19 pandēmijas laikā ir parādījusi arvien vairāk savstarpēji atkarīgo sabiedrību neaizsargātību pret zemas varbūtības riskiem.

(38) Ņemot vērā atšķirības valstu pārvaldes struktūrās un lai neskartu jau pastāvošos nozaru pasākumus vai Savienības uzraudzības un regulatīvās struktūras, dalībvalstīm būtu jāspēj izraudzīties vai izveidot vienu vai vairākas kompetentās iestādes, kas atbild par kiberdrošību un šajā direktīvā paredzētajiem uzraudzības uzdevumiem.

(39) Lai veicinātu pārrobežu sadarbību un saziņu starp iestādēm un lai varētu efektīvi īstenot šo direktīvu, katrai dalībvalstij jāizraugās vienots kontaktpunkts, kas atbild par to jautājumu koordināciju, kuri saistīti ar tīklu un informācijas sistēmu drošību un pārrobežu sadarbību Savienības līmenī.

(40) Vienotajiem kontaktpunktiem būtu jānodrošina efektīva pārrobežu sadarbība ar citu dalībvalstu attiecīgajām iestādēm un attiecīgā gadījumā ar Komisiju un *ENISA*. Tāpēc vienotajiem kontaktpunktiem būtu jāuzdod nosūtīt paziņojumus par būtiskiem incidentiem ar pārrobežu ietekmi citu skarto dalībvalstu vienotajiem kontaktpunktiem pēc *CSIRT* vai kompetentās iestādes pieprasījuma. Valstu līmenī vienotajiem kontaktpunktiem būtu jādara iespējama raita starpnozaru sadarbība ar citām kompetentajām iestādēm. Vienotie kontaktpunkti varētu arī saņemt relevantu informāciju par incidentiem, kas saistīti ar finanšu vienībām, no kompetentajām iestādēm, kas minētas Regulā (ES) 2022/2554, un tiem būtu jāspēj šo informāciju attiecīgā gadījumā pārsūtīt šajā direktīvā paredzētajām *CSIRT* vai kompetentajām iestādēm.

(41) Dalībvalstīm vajadzētu būt gan tehnisko, gan organizatorisko spēju ziņā adekvāti aprīkotām, lai novērstu un atklātu incidentus un riskus, reaģētu uz tiem un mazinātu to ietekmi. Tāpēc dalībvalstīm būtu jāizveido vai jāizraugās viena vai vairākas *CSIRT* saskaņā ar šo direktīvu un jānodrošina, ka tām ir adekvāti resursi un tehniskās spējas. *CSIRT* būtu jāatbilst šajā direktīvā noteiktajām prasībām, lai garantētu reālas un saderīgas spējas incidentu risināšanai un risku novēršanai un efektīvas sadarbības nodrošināšanai Savienības līmenī. Dalībvalstīm būtu jāspēj par *CSIRT* izraudzīties jau esošas datorapdraudējumu reaģēšanas vienības (*CERT*). Lai uzlabotu uzticības pilnas attiecības starp vienībām un *CSIRT*, gadījumos, kad *CSIRT* ir kompetentās iestādes daļa, dalībvalstīm būtu jāspēj apsvērt funkcionālu nošķirumu starp *CSIRT* veiktajiem operatīvajiem uzdevumiem, jo īpaši attiecībā uz informācijas kopīgošanu un vienībām sniegto palīdzību, un kompetento iestāžu uzraudzības darbībām.

(42) *CSIRT* uzdevums ir risināt incidentus. Tas ietver dažkārt sensitīvu datu apstrādi lielā apjomā. Dalībvalstīm būtu jānodrošina, ka *CSIRT* ir infrastruktūra informācijas kopīgošanai un apstrādei, kā arī labi aprīkots personāls, kas nodrošina to darbību konfidencialitāti un uzticamību. Šajā sakarā *CSIRT* varētu arī pieņemt rīcības kodeksus.

(43) Attiecībā uz persondatiem – *CSIRT*, ja to pieprasa būtiska vai svarīga vienība, būtu jāspēj nodrošināt to pakalpojumu sniegšanai izmantoto tīklu un informācijas sistēmu proaktīvu skenēšanu, ievērojot Regulu (ES) 2016/679. Attiecīgā gadījumā dalībvalstīm būtu jācenšas nodrošināt vienlīdzīgu tehnisko spēju līmeni visām nozaru *CSIRT*. Dalībvalstīm būtu jāspēj lūgt *ENISA* palīdzību savu *CSIRT* izveidē.

(44) *CSIRT* būtu jāspēj pēc būtiskas vai svarīgas vienības pieprasījuma uzraudzīt ar internetu saskarsmē esošos vienības aktīvus gan telpās, gan ārpus tām, nolūkā identificēt, izprast un pārvaldīt vienības vispārējos organizatoriskos riskus attiecībā uz jaunidentificētiem piegādes ķēdes apdraudējumiem vai kritiskām ievainojamībām. Vienība būtu jāpamudina paziņot *CSIRT*, vai tā izmanto priviliģētu pārvaldības saskarni, jo tas varētu ietekmēt mitigācijas darbību veikšanas ātrumu.

(45) 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. Tāpēc, lai veiktu savus uzdevumus, *CSIRT* un kompetentajām iestādēm būtu jāspēj apmainīties ar informāciju, tostarp persondatiem, ar trešo valstu valsts datordrošības incidentu reaģēšanas vienībām vai kompetentajām iestādēm, ar noteikumu, ka ir izpildīti Savienības datu aizsardzības tiesību aktos paredzētie nosacījumi persondatu nosūtīšanai uz trešām valstīm, cita starpā Regulas (ES) 2016/679 49. panta nosacījumi.

(46) Ir būtiski nodrošināt adekvātus resursus, lai sasniegtu šīs direktīvas mērķus un dotu iespēju kompetentajām iestādēm un *CSIRT* veikt tajā noteiktos uzdevumus. Dalībvalstis var valsts līmenī ieviest finansēšanas mehānismu, lai segtu nepieciešamos izdevumus, kas saistīti ar to publisko vienību uzdevumu veikšanu, kuras dalībvalstī saskaņā ar šo direktīvu ir atbildīgas par kiberdrošību. Šādam mehānismam būtu jāatbilst Savienības tiesību aktiem, tam vajadzētu būt samērīgam un nediskriminējošam, un tajā būtu jāņem vērā dažādas pieejas drošu pakalpojumu sniegšanai.

(47) *CSIRT* tīklam būtu jāturpina palīdzēt stiprināt paļāvību un uzticēšanos un veicināt ātru un rezultatīvu operatīvo sadarbību starp dalībvalstīm. Lai uzlabotu operatīvo sadarbību Savienības līmenī, *CSIRT* tīklam būtu jāapsver iespēja aicināt Savienības struktūras un aģentūras, kas iesaistītas kiberdrošības rīcībpolitikā, piemēram, Eiropolu, piedalīties tā darbā.

(48) Lai sasniegtu un uzturētu augstu kiberdrošības līmeni, šajā direktīvā prasītajām valstu kiberdrošības stratēģijām būtu jāsastāv no saskanīgiem satvariem, kas paredz stratēģiskus mērķus un prioritātes kiberdrošības jomā un pārvaldību to sasniegšanai. Minētās stratēģijas var sastāvēt no viena vai vairākiem leģislatīviem vai neleģislatīviem instrumentiem.

(49) Kiberhigiēnas rīcībpolitikas nodrošina pamatu tīklu un informācijas sistēmu infrastruktūru, aparatūras, programmatūras un tiešsaistes lietotņu drošības aizsardzībai, kā arī vienību izmantoto uzņēmumu vai galalietotāju datu aizsardzībai. Kiberhigiēnas rīcībpolitikas, kas veido kopīgu prakšu pamatkopu, tostarp programmatūras un aparatūras atjaunināšanu, paroļu maiņu, jaunu uzstādīto produktu pārvaldību, administratora līmeņa piekļuves kontu ierobežošanu un datu dublējumkopiju izveidi, dara iespējamu proaktīvu gatavības un vispārēja drošumu un drošības sistēmu incidentu vai kiberdraudu gadījumā. *ENISA* būtu jāuzrauga un jāanalizē dalībvalstu kiberhigiēnas rīcībpolitikas.

(50) Izpratne par kiberdrošību un kiberhigiēnu ir būtiska, lai uzlabotu kiberdrošības līmeni Savienībā, jo īpaši ņemot vērā to, ka pieaug tādu savienoto ierīču skaits, kuras arvien vairāk izmanto kiberuzbrukumos. Būtu jācenšas uzlabot vispārējo izpratni par riskiem, kas saistīti ar šādām ierīcēm, savukārt Savienības līmeņa novērtējumi varētu palīdzēt nodrošināt vienotu izpratni par šādiem riskiem iekšējā tirgū.

(51) Dalībvalstīm būtu jāveicina jebkādas tādas inovatīvas tehnoloģijas, tostarp mākslīgā intelekta, izmantošana, kas varētu uzlabot kiberuzbrukumu atklāšanu un novēršanu, dodot iespēju resursus cīņai pret kiberuzbrukumiem novirzīt rezultatīvāk. Tāpēc dalībvalstīm savās valsts kiberdrošības stratēģijās būtu jāveicina pētniecības un izstrādes darbības, lai atvieglotu šādu tehnoloģiju izmantošanu, jo īpaši tādu tehnoloģiju izmantošanu, kas saistītas ar automatizētiem vai pusautomatizētiem kiberdrošības rīkiem, un attiecīgā gadījumā tādu datu kopīgošana, kas vajadzīgi, lai apmācītu šādu tehnoloģiju lietotājus un tās uzlabotu. Jebkuras inovatīvas tehnoloģijas, tostarp mākslīgā intelekta, izmantošanai būtu jāatbilst Savienības datu aizsardzības tiesību aktiem, tostarp datu aizsardzības principiem – datu precizitātei, datu minimizēšanai, taisnīgumam un pārredzamībai un datu drošībai, piemēram, mūsdienīgai šifrēšanai. Būtu pilnībā jāizmanto integrētās datu aizsardzības un datu aizsardzības pēc noklusējuma prasības, ko paredz Regula (ES) 2016/679.

(52) Atvērtā pirmkoda kiberdrošības rīki un lietotnes var paaugstināt atvērtības līmeni un pozitīvi ietekmēt rūpnieciskās inovācijas efektivitāti. Atvērtie standarti veicina drošības rīku sadarbspēju, tādējādi labvēlīgi ietekmējot rūpniecības nozares ieinteresēto personu drošību. Atvērtā pirmkoda kiberdrošības rīki un lietotnes var mobilizēt izstrādātāju kopienu kopumā, darot iespējamu piegādātāju dažādošanu. Atvērtā pirmkoda izmantošana var radīt pārredzamāku ar kiberdrošību saistītu rīku verifikāciju un kopienas virzītu ievainojamības atklāšanu. Tādēļ dalībvalstīm būtu jāspēj veicināt atvērtā pirmkoda programmatūras un atvērto standartu izmantošanu, īstenojot rīcībpolitikas attiecībā uz atvērto datu un atvērtā pirmkoda izmantošanu kā daļu no drošības, ko panāk ar pārredzamību. Rīcībpolitikas, kas veicina atvērtā pirmkoda kiberdrošības rīku ieviešanu un ilgtspējīgu izmantošanu, ir īpaši svarīgas maziem un vidējiem uzņēmumiem, kuri saskaras ar lielām ieviešanas izmaksām, ko varētu minimizēt, samazinot nepieciešamību pēc konkrētām lietotnēm vai rīkiem.

(53) Sabiedriskie pakalpojumi arvien vairāk tiek savienoti ar pilsētu digitālajiem tīkliem, lai uzlabotu pilsētu transporta tīklus, uzlabotu modernizētu ūdensapgādi un atkritumu apglabāšanas kompleksus un palielinātu apgaismojuma un ēku apkures efektivitāti. Minētie digitalizētie sabiedriskie pakalpojumi var tikt pakļauti kiberuzbrukumiem, un veiksmīga kiberuzbrukuma gadījumā savstarpējās savienotības dēļ tie var kaitēt iedzīvotājiem plašā mērogā. Dalībvalstīm savas kiberdrošības stratēģijas ietvaros būtu jāizstrādā rīcībpolitika, kas pievēršas šādu savienotu vai viedu pilsētu izveidei un to iespējamajai ietekmei uz sabiedrību.

(54) Pēdējos gados Savienībā ir strauji palielinājies izspiedējprogrammatūras uzbrukumu skaits, kuros ļaunprogrammatūra šifrē datus un sistēmas un pieprasa izpirkuma maksu par atšifrēšanu. Izspiedējprogrammatūras uzbrukumu pieaugošo biežumu un smagumu var noteikt vairāki faktori, piemēram, dažādi uzbrukuma modeļi, noziedzīgas darbības modeļi, kas saistīti ar "izspiedējprogrammatūru kā pakalpojumu" un kriptovalūtām, izpirkuma maksas pieprasīšana un pieaugoši uzbrukumi piegādes ķēdē. Dalībvalstīm to valsts kiberdrošības stratēģijas ietvaros būtu jāizstrādā rīcībpolitika izspiedējprogrammatūras uzbrukumu pieauguma problēmas risināšanai.

(55) Publiskā un privātā sektora partnerības (PPP) kiberdrošības jomā var nodrošināt pienācīgu sistēmu zināšanu apmaiņai, paraugprakšu kopīgošanai un kopīgas izpratnes gūšanai ieinteresēto personu vidū. Dalībvalstīm būtu jāveicina rīcībpolitikas, kas ir pamatā kiberdrošības PPP izveidei. Minētajās rīcībpolitikās cita starpā būtu jāprecizē tvērums un iesaistītās ieinteresētās personas, pārvaldības modelis, pieejamās finansējuma iespējas un iesaistīto ieinteresēto personu mijiedarbība attiecībā uz PPP. PPP var izmantot privātā sektora vienību specializētās zināšanas, lai palīdzētu kompetentajām iestādēm izstrādāt modernus pakalpojumus un procesus, tostarp informācijas apmaiņu, agrīnus brīdinājumus, kiberdraudu un incidentu jomas mācības, krīzes pārvaldību un noturības plānošanu.

(56) Dalībvalstīm to valsts kiberdrošības stratēģijās būtu jārisina konkrētas mazo un vidējo uzņēmumu kiberdrošības vajadzības. Savienībā mazo un vidējo uzņēmumu īpatsvars rūpniecības un uzņēmējdarbības tirgū ir liels, un bieži vien tiem ir grūtības pielāgoties jaunai uzņēmējdarbības praksei lielākā mērā savienotā pasaulē un digitālā vidē laikā, kad darbinieki strādā no mājām un uzņēmējdarbība arvien biežāk notiek tiešsaistē. Daļai mazo un vidējo uzņēmumu kiberdrošības ziņā ir īpašas grūtības, piemēram, vāja izpratne par kiberdrošību, attālās IT drošības trūkums, augstās kiberdrošības risinājumu izmaksas un augstāks apdraudējuma, piemēram, izspiedējprogrammatūras draudu, līmenis, un šādu problēmu risināšanai tiem būtu jāsaņem padomi un atbalsts. Mazie un vidējie uzņēmumi arvien vairāk kļūst par mērķi uzbrukumos piegādes ķēdēm, jo tiem ir mazāk stingri kiberdrošības risku pārvaldības pasākumi un uzbrukumu pārvaldība, un ierobežoti drošības resursi. Šādi uzbrukumi piegādes ķēdēm neietekmē mazos un vidējos uzņēmumus un to darbību vien: tiem var būt arī lavīneida ietekme uz lielākiem uzbrukumiem vienībām, kurām mazie un vidējie uzņēmumi nodrošina piegādes. Dalībvalstīm ar valsts kiberdrošības stratēģijām būtu jāpalīdz mazajiem un vidējiem uzņēmumiem risināt problēmas to piegādes ķēdēs. Dalībvalstīm vajadzētu būt

valsts vai reģionāla līmeņa kontaktpunktam maziem un vidējiem uzņēmumiem, kurš sniedz norādījumus un palīdzību maziem un vidējiem uzņēmumiem vai nosūta tos pie attiecīgajām struktūrām, lai tie saņemtu norādījumus un palīdzību ar kiberdrošību saistītos jautājumos. Dalībvalstis tiek arī mudinātas piedāvāt tādus pakalpojumus kā tīmekļa vietņu konfigurācija un datu reģistrēšana, kas to darītu iespējamu mikrouzņēmumiem un mazajiem uzņēmumiem, kuriem šādu spēju nav.

(57) Dalībvalstīm valsts kiberdrošības stratēģijās būtu jāpieņem rīcībpolitikas aktīvas kiberaizsardzības veicināšanai plašākas aizsardzības stratēģijas satvarā. Aktīva kiberaizsardzība ir nevis reaģēšana, bet gan aktīva tīkla drošības pārkāpumu nepieļaušana, atklāšana, uzraudzība, analīze un mitigācija apvienojumā ar spēju izmantošanu cietušajā tīklā un ārpus tā. Tās ietvaros dalībvalstis varētu dažām vienībām piedāvāt bezmaksas pakalpojumus vai rīkus, tostarp pašapkalpošanās pārbaudes, atklāšanas rīkus un vietņu bloķēšanas pakalpojumus. Spēja ātri un automātiski kopīgot un izprast informāciju par draudiem un to analīzi, kiberdarbības brīdinājumi un atbildes reakcija ir izšķirīgi svarīga, lai būtu iespējami saskaņoti centieni veiksmīgi nepieļaut, atklāt, risināt un bloķēt uzbrukumus tīklu un informācijas sistēmām. Aktīva kiberaizsardzība ir balstīta uz defensīvu stratēģiju, kas izslēdz ofensīvus pasākumus.

(58) Ņemot vērā to, ka tīklu un informācijas sistēmu ievainojamību izmantošana var izraisīt būtiskus traucējumus un kaitējumu, riska mazināšanā svarīgs faktors ir šādu ievainojamību ātra apzināšana un novēršana. Tāpēc vienībām, kas izstrādā vai pārvalda tīklu un informācijas sistēmas, būtu jāievieš pienācīgas procedūras, kā rīkoties, kad tiek atklāta ievainojamība. Tā kā ievainojamību bieži konstatē un izpauž trešās personas, IKT produktu ražotājam vai IKT pakalpojumu sniedzējam būtu arī jāievieš nepieciešamās procedūras informācijas par ievainojamību saņemšanai no trešām personām. Šajā sakarā norādījumus par rīcību ievainojamības gadījumā un ievainojamības izpaušanu sniedz attiecīgi starptautiskie standarti ISO/IEC 30111 un ISO/IEC 29147. Labāka koordinācija starp ziņotājām fiziskām un juridiskām personām un IKT produktu ražotājiem vai IKT pakalpojumu sniedzējiem ir īpaši svarīga, lai sekmētu brīvprātīgu ievainojamības izpaušanas sistēmu. Koordinēta ievainojamības izpaušana ir strukturēts process, kurā potenciāli ievainojamu IKT produktu ražotājiem vai potenciāli ievainojamu IKT pakalpojumu sniedzējiem par ievainojamību tiek ziņots tā, lai ievainojamību varētu diagnosticēt un izlabot, pirms sīkāka informācija par to tiek izpausta trešām personām vai sabiedrībai. Koordinētā ievainojamības izpaušanā būtu jāietver arī koordinācija starp ziņotāju fizisku vai juridisku personu un potenciāli ievainojamu IKT produktu vai IKT pakalpojumu ražotāju vai sniedzēju attiecībā uz ievainojamības izlabošanas un publiskošanas termiņu.

(59) Komisijai, *ENISA* un dalībvalstīm būtu jāturpina veicināt saskaņotību ar starptautiskajiem standartiem un pastāvošajām nozares paraugpraksēm kiberdrošības risku pārvaldības jomā, piemēram, piegādes ķēdes drošības novērtēšanas, informācijas kopīgošanas un ievainojamības izpaušanas jomā.

(60) Dalībvalstīm sadarbībā ar *ENISA* būtu jāveic pasākumi, lai veicinātu koordinētu ievainojamības izpaušanu, ieviešot atbilstošu valsts rīcībpolitiku. Ar valsts rīcībpolitiku dalībvalstīm būtu jācenšas, cik vien iespējams, risināt problēmas, kas skar ievainojamības pētniekus, tostarp to, ka tiem var tikt noteikta krimināltatbildība saskaņā ar valsts tiesību aktiem. Ņemot vērā, ka fiziskas un juridiskas personas, kas pēta ievainojamību, dažās dalībvalstīs varētu būt pakļautas krimināltatbildībai un civiltiesiskajai atbildībai, dalībvalstis tiek mudinātas pieņemt pamatnostādnes par kriminālvajāšanas neīstenošanu pret pētniekiem informācijas drošības jomā un viņu darbību atbrīvošanu no civiltiesiskās atbildības.

(61) Dalībvalstīm būtu jāizraugās viena no savām *CSIRT* par koordinatori, kas vajadzības gadījumā darbotos kā uzticama starpniece starp ziņotājām fiziskajām un juridiskajām personām un tādu IKT produktu ražotājiem vai IKT pakalpojumu sniedzējiem, ko ievainojamība, visticamāk, skars. Par koordinatori izraudzītās *CSIRT* uzdevumiem būtu jāietver attiecīgo vienību identificēšana un sazināšanās ar tām, palīdzība fiziskajām un juridiskajām personām,

kas ziņo par ievainojamību, sarunas par izpaušanas termiņiem un tādu ievainojamību pārvaldību, kuras ietekmē vairākas vienības (daudzpusējā koordinētā ievainojamības izpaušana). Ja paziņotā ievainojamība varētu būtiski ietekmēt vienības vairāk nekā vienā dalībvalstī, par koordinatorēm izraudzītajām *CSIRT* attiecīgos gadījumos būtu jāsadarbojas *CSIRT* tīklā.

(62) Piekļuve pareizai un savlaicīgai informācijai par ievainojamībām, kas skar IKT produktus un IKT pakalpojumus, veicina labāku kiberdrošības risku pārvaldību. Publiski pieejamas informācijas par ievainojamībām avoti ir svarīgs rīks vienībām un to pakalpojumu lietotājiem, kā arī kompetentajām iestādēm un *CSIRT*. Šā iemesla dēļ *ENISA* būtu jāizveido Eiropas ievainojamību datubāze, kurā vienības, neatkarīgi no tā, vai tās ir šīs direktīvas darbības jomā, un to tīklu un informācijas sistēmu nodrošinātāji, kā arī kompetentās iestādes un *CSIRT* var brīvprātīgi izpaust un reģistrēt publiski zināmas ievainojamības, lai lietotāji varētu veikt pienācīgus mitigācijas pasākumus. Minētās datubāzes mērķis būtu risināt unikālās problēmas, ko draudi rada Savienības vienībām. Turklāt *ENISA* būtu jāizveido pienācīga publiskošanas procesa procedūra, lai dotu vienībām laiku veikt mitigācijas pasākumus attiecībā uz to ievainojamībām, un jāizmanto jaunākie kiberdrošības risku pārvaldības pasākumi, kā arī mašīnlasāmas datu kopas un attiecīgas saskarnes. Lai veicinātu ievainojamību izpaušanas kultūru, atklāšanai nevajadzētu kaitēt ziņotājai fiziskai vai juridiskai personai.

(63) Lai gan līdzīgi ievainojamību reģistri un datubāzes jau pastāv, to mitinātājas un uzturētājas ir vienības, kas nav iedibinātas Savienībā. *ENISA* uzturēta Eiropas ievainojamību datubāze nodrošinātu labāku pārredzamību attiecībā uz publiskošanas procesu, pirms ievainojamība tiek publiski izpausta, un noturību gadījumā, kad notiek traucējumi vai pārtraukums līdzīgu pakalpojumu sniegšanā. Lai pēc iespējas izvairītos no centienu dublēšanās un nodrošinātu komplementaritāti, *ENISA* būtu jāizskata iespēja slēgt strukturētus sadarbības nolīgumus ar līdzīgiem reģistriem vai datubāzēm, kas ir trešo valstu jurisdikcijā. Konkrētāk, *ENISA* būtu jāizskata iespēja cieši sadarboties ar kopējās ievainojamību un eksponētību (*CVE*) sistēmas operatoriem.

(64) Sadarbības grupai būtu jāatbalsta un jāveicina stratēģiskā sadarbība un informācijas apmaiņa, kā arī jāstiprina dalībvalstu savstarpējā uzticēšanās un paļāvība. Sadarbības grupai ik divus gadus būtu jāizstrādā darba programma. Darba programmā būtu jāiekļauj darbības, kas sadarbības grupai jāveic, lai sasniegtu savus mērķus un izpildītus savus uzdevumus. Lai izvairītos no iespējamiem traucējumiem sadarbības grupas darbā, saskaņā ar šo direktīvu pieņemamās pirmās darba programmas izstrādes termiņš būtu jāpielāgo pēdējās saskaņā ar Direktīvu (ES) 2016/1148 izstrādātās darba programmas termiņam.

(65) 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 konkrēti ieteikumi, jo īpaši par to, kā atvieglot saskaņošanu šīs direktīvas transponēšanā dalībvalstīs, kas jāizpilda, labāk īstenojot pastāvošos noteikumus. Sadarbības grupa varētu arī apzināt valstu risinājumus nolūkā veicināt katrā konkrētajā nozarē izmantoto kiberdrošības risinājumu saderību Savienībā. Tas ir īpaši būtiski nozarēm, kurām ir starptautisks vai pārrobežu raksturs.

(66) Sadarbības grupai arī turpmāk vajadzētu būt elastīgam forumam un būtu jāspēj reaģēt uz mainīgām un jaunām rīcībpolitikas prioritātēm un problēmām, vienlaikus ņemot vērā resursu pieejamību. Tā varētu organizēt regulāras kopīgas sanāksmes ar attiecīgajām privātā sektora ieinteresētajām personām no visas Savienības, lai apspriestu sadarbības grupas veiktās darbības un vāktu datus un informāciju par jaunām rīcībpolitiskām problēmām. Papildus tam sadarbības grupai būtu regulāri jānovērtē stāvoklis kiberdraudu vai incidentu, piemēram, izspiedējprogrammatūras, jomā. Lai uzlabotu sadarbību Savienības līmenī, sadarbības grupai būtu jāapsver iespēja pieaicināt

attiecīgās Savienības iestādes, struktūras, birojus un aģentūras, kas iesaistītas kiberdrošības rīcībpolitikā, piemēram, Eiropas Parlamentu, Eiropolu, Eiropas Datu aizsardzības kolēģiju, Eiropas Savienības Aviācijas drošības aģentūru, kura izveidota ar Regulu (ES) 2018/1139, un Eiropas Savienības Kosmosa programmas aģentūru, kura izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/696 ([14]), lai tās piedalītos tās darbā.

(67) Lai uzlabotu sadarbību un stiprinātu dalībvalstu savstarpējo uzticēšanos, kompetentajām iestādēm un *CSIRT* būtu jāspēj piedalīties apmaiņas shēmās, kas paredzētas amatpersonām no citām dalībvalstīm, īpašā sistēmā un attiecīgos gadījumos ar vajadzīgo drošības pārbaudi amatpersonām, kas piedalās šādās apmaiņas shēmās. Kompetentajām iestādēm būtu jāveic pasākumi, kas nepieciešami, lai amatpersonas no citām dalībvalstīm varētu pilnvērtīgi piedalīties uzņēmējas kompetentās iestādes vai uzņēmējas *CSIRT* pasākumos.

(68) Dalībvalstīm būtu jāsniedz ieguldījums Komisijas Ieteikumā (ES) 2017/1584 ([15]) noteiktā ES satvara reaģēšanai kiberdrošības krīzēs izveidošanā, izmantojot pastāvošos sadarbības tīklus, jo īpaši Eiropas Kiberkrīžu sadarbības organizāciju tīklu (*EU-CyCLONe*), *CSIRT* tīklu un sadarbības grupu. *EU-CyCLONe* un *CSIRT* tīklam būtu jāsadarbojas, izmantojot procesuālo kārtību, kas precizē minētās sadarbības detaļas, un jāizvairās no jebkādas uzdevumu dublēšanās. *EU-CyCLONe* reglamentā būtu jāprecizē kārtība, kādā tīklam būtu jādarbojas, cita starpā paredzot tīkla uzdevumus, sadarbības veidus, mijiedarbību ar citiem attiecīgiem rīcībspēkiem un veidnes informācijas kopīgošanai, kā arī saziņas līdzekļus. Attiecībā uz krīžu pārvaldību Savienības līmenī attiecīgajām pusēm būtu jāpaļaujas uz ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem, ko paredz Padomes Īstenošanas lēmums (ES) 2018/1993 ([16]) (*IPCR* mehānismi). Šim nolūkam Komisijai būtu jāizmanto krīzes augstlīmeņa starpnozaru koordinācijas process *ARGUS*. Ja krīzei ir nozīmīgs ārpolitikas vai kopīgās drošības un aizsardzības politikas aspekts, būtu jāiedarbina Eiropas Ārējās darbības dienesta mehānisms reaģēšanai krīzes situācijās.

(69) Saskaņā ar pielikumu Ieteikumam (ES) 2017/1584 plašapmēra kiberdrošības incidents būtu jāsaprot kā incidents, kura radītais traucējuma līmenis pārsniedz dalībvalsts spēju uz to reaģēt vai kuram ir būtiska ietekme uz vismaz divām dalībvalstīm. Atkarībā no cēloņa un ietekmes plašapmēra kiberdrošības incidenti var izvērsties par visaptverošām krīzēm, kas padara neiespējamu iekšējā tirgus pienācīgu darbību vai rada nopietnus sabiedriskās drošības un drošuma riskus vienībām vai iedzīvotājiem vairākās dalībvalstīs vai Savienībai kopumā. Ņemot vērā šādu incidentu plašo tvērumu un to, ka vairākumā gadījumu tiem ir pārrobežu raksturs, dalībvalstīm un attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām būtu jāsadarbojas tehniskā, operatīvā un politiskā līmenī, lai pienācīgi koordinētu reaģēšanu Savienībā.

(70) Krīzēm un plašapmēra kiberdrošības incidentiem Savienības līmenī ir vajadzīga koordinēta rīcība, lai nodrošinātu ātru un rezultatīvu reaģēšanu, jo nozares un dalībvalstis ir lielā mērā savstarpēji atkarīgas. Kibernoturīgu tīklu un informācijas sistēmu pieejamībai un datu pieejamībai, konfidencialitātei un integritātei ir izšķirīga loma Savienības drošībā un tās iedzīvotāju, uzņēmumu un iestāžu aizsardzībā pret incidentiem un kiberdraudiem, kā arī nolūkā vairot indivīdu un organizāciju uzticēšanos Savienības spējai veicināt un aizsargāt globālu, atvērtu, brīvu, stabilu un drošu kibertelpu, kuras pamatā ir cilvēktiesības, pamatbrīvības, demokrātija un tiesiskums.

([14]) Eiropas Parlamenta un Padomes Regula (ES) 2021/696 (2021. gada 28. aprīlis), ar ko izveido Savienības kosmosa programmu un Eiropas Savienības Kosmosa programmas aģentūru un atceļ Regulas (ES) Nr. 912/2010, (ES) Nr. 1285/2013 un (ES) Nr. 377/2014 un Lēmumu Nr. 541/2014/ES (OV L 170, 12.5.2021., 69. lpp.).

([15]) 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.).

([16]) Padomes Īstenošanas lēmums (ES) 2018/1993 (2018. gada 11. decembris) par ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem (OV L 320, 17.12.2018., 28. lpp.).

(71) *EU-CyCLONe* būtu jādarbojas kā starpniekam starp tehnisko un politisko līmeni plašapmēra kiberdrošības incidentu un krīžu laikā, un tam būtu jāuzlabo sadarbība operatīvajā līmenī un jāatbalsta lēmumu pieņemšana politiskajā līmenī. Sadarbībā ar Komisiju, ņemot vērā Komisijas kompetenci krīžu pārvarēšanas jomā, *EU-CyCLONe* būtu jāizmanto *CSIRT* tīkla konstatējumi un savas spējas, lai sagatavotu plašapmēra kiberdrošības incidentu un krīžu ietekmes analīzi.

(72) Kiberuzbrukumiem ir pārrobežu raksturs, un būtisks incidents var traucēt un kaitēt kritiskajām informācijas infrastruktūrām, no kurām ir atkarīga iekšējā tirgus netraucēta darbība. Ieteikums (ES) 2017/1584 pievēršas visu attiecīgo rīcībspēku lomai. Turklāt Komisija ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES ([17]) izveidotā Savienības civilās aizsardzības mehānisma satvarā ir atbildīga par vispārīgām sagatavotības darbībām, tostarp Ārkārtas reaģēšanas koordinēšanas centra un Kopīgās ārkārtējo situāciju sakaru un informācijas sistēmas pārvaldību, situācijas apzināšanās un analīzes spēju uzturēšanu un turpmāku attīstīšanu, kā arī par to, lai izveidotu un attīstītu spēju mobilizēt un nosūtīt ekspertu vienības gadījumā, ja kāda dalībvalsts vai trešā valsts lūdz palīdzību. Komisija ir atbildīga arī par analītisko ziņojumu sniegšanu *IPCR* mehānismiem saskaņā ar Īstenošanas lēmumu (ES) 2018/1993, cita starpā attiecībā uz kiberdrošības situācijas apzināšanos un sagatavotību, kā arī par situācijas apzināšanos un reaģēšanu krīzes situācijās tādās jomās kā lauksaimniecība, nelabvēlīgi laikapstākļi, konfliktu kartēšana un prognozes, agrīnās brīdināšanas sistēmas dabas katastrofu gadījumos, ārkārtas situācijas veselības jomā, infekcijas slimību uzraudzība, augu veselība, ķīmiskie incidenti, pārtikas un barības nekaitīgums, dzīvnieku veselība, migrācija, muita, kodolenerģētiskās un radioloģiskās avārijas un enerģētika.

(73) Attiecīgā gadījumā Savienība saskaņā ar LESD 218. pantu var noslēgt starptautiskus nolīgumus ar trešām valstīm vai starptautiskām organizācijām, kuri ļauj tām piedalīties un organizē to dalību konkrētās sadarbības grupas, *CSIRT* tīkla un *EU-CyCLONe* darbībās. Šādos nolīgumos būtu jānodrošina Savienības intereses un pienācīga datu aizsardzība. Tam nebūtu jāizslēdz dalībvalstu tiesības sadarboties ar trešām valstīm ievainojamību pārvaldībā un kiberdrošības risku pārvaldībā, atvieglojot ziņošanu un vispārēju informācijas apmaiņu saskaņā ar Savienības tiesību aktiem.

(74) Lai veicinātu šīs direktīvas rezultatīvu īstenošanu, piemēram, attiecībā uz ievainojamību pārvaldību, kiberdrošības risku pārvaldības pasākumiem, ziņošanas pienākumiem un kiberdrošības informācijas kopīgošanas mehānismiem, dalībvalstis var sadarboties ar trešām valstīm un veikt darbības, kas tiek uzskatītas par atbilstošām minētajam nolūkam, tostarp apmaiņīties ar informāciju par kiberdraudiem, incidentiem, ievainojamībām, rīkiem un metodēm, taktiku, paņēmieniem un procedūrām, gatavību kiberdrošības krīžu pārvaldībai un mācībām, apmācību, uzticēšanās veidošanu un strukturētus informācijas kopīgošanas mehānismus.

(75) Būtu jāievieš salīdzinošā izvērtēšana, lai palīdzētu mācīties no kopīgas pieredzes, stiprinātu savstarpējo uzticēšanos un panāktu vienādi augstu kiberdrošības līmeni. Salīdzinošā izvērtēšana var dot vērtīgu ieskatu un ieteikumus, kas stiprinātu vispārējās kiberdrošības spējas, radītu vēl vienu funkcionālu ceļu paraugprakses kopīgošanai dalībvalstu starpā un palīdzētu uzlabot dalībvalstu gatavības līmeni kiberdrošības jomā. Turklāt salīdzinošajā izvērtēšanā būtu jāņem vērā līdzīgu mehānismu, piemēram, *CSIRT* tīkla salīdzinošās izvērtēšanas sistēmas, rezultāti, jārada pievienotā vērtība un jāizvairās no dublēšanās. Salīdzinošās izvērtēšanas īstenošanai nevajadzētu skart Savienības vai valstu tiesību aktus par konfidenciālas vai klasificētas informācijas aizsardzību.

(76) Sadarbības grupai būtu jāizveido dalībvalstīm paredzēta pašnovērtējuma metodika, kuras mērķis būtu aptvert tādus faktorus kā kiberdrošības risku pārvaldības pasākumu un ziņošanas pienākumu īstenošanas līmenis, kompetento iestāžu spēju līmenis un uzdevumu izpildes rezultativitāte, *CSIRT* operatīvās spējas, savstarpējās palīdzības īstenošanas līmenis, kiberdrošības informācijas kopīgošanas mehānismu īstenošanas līmenis vai konkrēti pārrobežu vai starpnozaru jautājumi. Dalībvalstis būtu jāmudina pašnovērtējumus veikt regulāri, kā arī iesniegt un apspriest sava pašnovērtējuma rezultātus sadarbības grupā.

([17]) Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu (OV L 347, 20.12.2013., 924. lpp.).

(77) Tīklu un informācijas sistēmas drošības nodrošināšana lielā mērā ir būtisko un svarīgo vienību pienākums. Būtu jāveicina un jāattīsta riska pārvaldības kultūra, kas ietver riska novērtēšanu un faktiskajiem riskiem atbilstošu kiberdrošības risku pārvaldības pasākumu īstenošanu.

(78) Kiberdrošības risku pārvaldības pasākumos būtu jāņem vērā, cik lielā mērā būtiskā vai svarīgā vienība ir atkarīga no tīklu un informācijas sistēmām, un jāietver pasākumi nolūkā identificēt visus incidentu riskus, novērst, atklāt incidentus, reaģēt uz tiem un atgūties no tiem, kā arī mazināt to ietekmi. Tīklu un informācijas sistēmu drošībai būtu jāietver glabāto, pārsūtīto un apstrādāto datu drošība. Kiberdrošības risku pārvaldības pasākumiem būtu jānodrošina sistēmiska analīze, kurā ņemts vērā cilvēkfaktors, lai gūtu pilnīgu priekšstatu par tīklu un informācijas sistēmas drošību.

(79) Tā kā tīklu un informācijas sistēmu drošības apdraudējumiem var būt dažāda izcelsme, kiberdrošības risku pārvaldības pasākumiem vajadzētu būt balstītiem visu apdraudējumu pieejā, kuras mērķis ir aizsargāt tīklu un informācijas sistēmas un minēto sistēmu fizisko vidi pret tādiem notikumiem kā zādzība, ugunsgrēks, plūdi, telesakaru vai elektroapgādes pārtraukumi vai pret tādu neatļautu fizisku piekļuvi un bojājumiem un traucējumiem būtiskās vai svarīgās vienības informācijā un informācijas apstrādes iekārtās, kas varētu apdraudēt glabāto, pārsūtīto vai apstrādāto datu vai pakalpojumu, kurus piedāvā vai kuriem var piekļūt ar tīklu un informācijas sistēmām, pieejamību, autentiskumu, integritāti vai konfidencialitāti. Tāpēc kiberdrošības risku pārvaldības pasākumos būtu jāpievēršas arī tīklu un informācijas sistēmu fiziskajai un vides drošībai, iekļaujot pasākumus šādu sistēmu aizsardzībai pret sistēmas traucējumiem, cilvēka kļūdām, ļaunprātīgām darbībām vai dabas parādībām atbilstoši Eiropas un starptautiskajiem standartiem, piemēram, tiem, kas iekļauti ISO/IEC 27000 sērijā. Šajā ziņā būtiskām vai svarīgām vienībām savu kiberdrošības risku pārvaldības pasākumos būtu jāpievēršas arī cilvēkresursu drošībai un jāievieš atbilstīga piekļuves kontroles rīcībpolitika. Minētajiem pasākumiem būtu jāatbilst Direktīvai (ES) 2022/2557.

(80) Lai pierādītu atbilstību kiberdrošības risku pārvaldības pasākumiem un ja nav piemērotu Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemtas saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 ([18]), dalībvalstīm, apspriežoties ar sadarbības grupu un Eiropas Kiberdrošības sertifikācijas grupu būtu jāveicina attiecīgo Eiropas un starptautiskos standartu izmantošana būtiskajās un svarīgajās vienībās vai arī tās var pieprasīt vienībām izmantot sertificētus IKT produktus, IKT pakalpojumus un IKT procesus.

(81) Lai izvairītos no nesamērīga finansiāla un administratīva sloga radīšanas būtiskajām un svarīgajām vienībām, kiberdrošības risku pārvaldības pasākumiem vajadzētu būt samērīgiem ar riskiem attiecīgajai tīklu un informācijas sistēmai, ņemot vērā jaunākos sasniegumus šādu pasākumu jomā un attiecīgā gadījumā attiecīgos Eiropas un starptautiskos standartus, kā arī to īstenošanas izmaksas.

(82) Kiberdrošības risku pārvaldības pasākumiem vajadzētu būt samērīgiem ar to, cik lielā mērā būtiskā vai svarīgā vienība ir eksponēta riskiem un kāda būtu incidenta sabiedriskā un ekonomiskā ietekme. Nosakot kiberdrošības risku pārvaldības pasākumus, kas pielāgoti būtiskajām un svarīgajām vienībām, būtu pienācīgi jāņem vērā būtisko un svarīgo vienību atšķirīgā eksponētība riskam, piemēram, vienības kritiskums, riski, tostarp sociālie riski, kam tā ir eksponēta, vienības lielums un incidentu rašanās varbūtība un to smagums, tostarp to sabiedrisko un ekonomisko ietekmi.

([18]) 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.).

(83) Būtiskajām un svarīgajām vienībām būtu jānodrošina savās darbībās izmantoto tīklu un informācijas sistēmu drošība. Minētās sistēmas galvenokārt ir privātas tīklu un informācijas sistēmas, kuras pārvalda būtisko un svarīgo vienību iekšējais IT personāls vai kuru drošība tiek nodrošināta ar ārpakalpojumiem. Kiberdrošības risku pārvaldības pasākumi un ziņošanas pienākumi, kas noteikti šajā direktīvā, attiecīgajām būtiskajām un svarīgajām vienībām būtu jāpiemēro neatkarīgi no tā, vai minētās vienības savu tīklu un informācijas sistēmu uzturēšanu veic iekšēji vai šim nolūkam izmanto ārpakalpojumus.

(84) DNS pakalpojumu sniedzējiem, ALD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīklu nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem un uzticamības pakalpojumu sniedzējiem, ņemot vērā to pārrobežu raksturu, būtu jāpieprasa augsta saskaņotības pakāpe Savienības līmenī. Tāpēc attiecībā uz minētajām vienībām kiberdrošības risku pārvaldības pasākumu īstenošana būtu jāveicina ar īstenošanas aktu.

(85) Risināt riskus, kas izriet no vienības piegādes ķēdes un tās attiecībām ar piegādātājiem, piemēram, datu uzglabāšanas un apstrādes pakalpojumu vai pārvaldītu drošības pakalpojumu sniedzējiem un programmatūras redaktoriem, ir īpaši svarīgi, ņemot vērā tādu incidentu izplatību, kuros vienības ir cietušas kiberuzbrukumos un kuros ļaunprātīgi nodarījumu veicēji ir spējuši ietekmēt vienības tīklu un informācijas sistēmu drošību, izmantojot ievainojamības, kas skar trešo personu produktus un pakalpojumus. Tāpēc būtiskām un svarīgām vienībām būtu jānovērtē un jāņem vērā savu piegādātāju un pakalpojumu sniedzēju produktu un pakalpojumu vispārējā kvalitāte un noturība, tajos iegultie kiberdrošības risku pārvaldības pasākumi un kiberdrošības prakses, tai skaitā to drošas izstrādes procedūras. Būtiskās un svarīgās vienības jo īpaši būtu jāmudina iekļaut kiberdrošības risku pārvaldības pasākumus līgumattiecībās ar saviem tiešajiem piegādātājiem un pakalpojumu sniedzējiem. Minētās vienības varētu izsvērt riskus, kas izriet no citiem piegādātāju un pakalpojumu sniedzēju līmeņiem.

(86) Pakalpojumu sniedzēju vidū pārvaldītu drošības pakalpojumu sniedzēji tādās jomās kā reaģēšana uz incidentiem, ielaušanās testēšana, drošības revīzijas un konsultācijas pilda īpaši svarīgu lomu, palīdzēdami vienībām to centienos novērst, atklāt incidentus, reaģēt uz tiem vai atgūties no tiem. Tomēr arī pārvaldītu drošības pakalpojumu sniedzēji paši ir bijuši kiberuzbrukumu mērķis, un tie rada īpašu risku, jo ir cieši iesaistīti vienību darbībās. Tāpēc būtiskām un svarīgām vienībām, izvēloties pārvaldītu drošības pakalpojumu sniedzēju, būtu jāievēro īpaša piesardzība.

(87) Kompetentās iestādes savu uzraudzības uzdevumu kontekstā var izmantot arī tādus kiberdrošības pakalpojumus kā drošības revīzijas, ielaušanās testēšana vai reaģēšana uz incidentiem.

(88) Būtiskām un svarīgām vienībām būtu arī jāizskata riski, kas izriet no to mijiedarbības un attiecībām ar citām ieinteresētajām personām plašākā ekosistēmā, arī attiecībā uz rūpnieciskās spiegošanas apkarošanu un komercnoslēpumu aizsardzību. Konkrētāk, minētajām vienībām būtu jāveic piemēroti pasākumi, lai nodrošinātu, ka to sadarbība ar akadēmiskajām un pētniecības iestādēm notiek atbilstoši to kiberdrošības rīcībpolitikai un ka tiek ievērota laba prakse attiecībā uz drošu piekļuvi un informācijas izplatīšanu kopumā un intelektuālā īpašuma aizsardzību konkrēti. Līdzīgi, ņemot vērā datu nozīmīgumu un vērtību būtisko un svarīgo vienību darbībās, minētajām vienībām, paļaujoties uz trešo personu sniegtiem datu transformēšanas un datu analīzes pakalpojumiem, būtu jāveic visi piemērotie kiberdrošības risku pārvaldības pasākumi.

(89) Būtiskām un svarīgām vienībām būtu jāpieņem dažādas kiberhigiēnas pamatprakses, piemēram, nulles uzticības principi, programmatūras atjauninājumi, ierīču konfigurācija, tīkla segmentēšana, identitātes un piekļuves pārvaldība vai lietotāju informētība, jāorganizē darbinieku apmācība un jāuzlabo izpratne par kiberdraudiem, pikšķerēšanu vai sociālās inženierijas paņēmieniem. Turklāt minētajām vienībām būtu jāizvērtē savas kiberdrošības spējas un attiecīgā gadījumā jāturpina integrēt kiberdrošības uzlabošanas tehnoloģijas, piemēram, mākslīgā intelekta vai mašīnmācīšanās sistēmas, kas stiprina to spējas un tīklu un informācijas sistēmu drošību.

(90) Lai vēl vairāk pievērstos svarīgiem piegādes ķēdes riskiem un palīdzētu būtiskām un svarīgām vienībām, kas darbojas nozarēs, uz kurām šī direktīva attiecas, pienācīgi pārvaldīt ar piegādes ķēdēm un piegādātājiem saistītus riskus, sadarbības grupai sadarbībā ar Komisiju un *ENISA* un attiecīgā gadījumā pēc apspriešanās ar attiecīgajām ieinteresētajām personām, arī no nozares, būtu jāveic koordinēti kritisko piegādes ķēžu riska novērtējumi, kā tas jau tika darīts attiecībā uz 5G tīkliem saskaņā ar Komisijas Ieteikumu (ES) 2019/534 ([19]), lai par katru nozari apzinātu, kuri ir kritiskie IKT pakalpojumi, IKT sistēmas vai IKT produkti, attiecīgie draudi un ievainojamības. Šādos koordinētos drošības riska novērtējumos būtu jāapzina pasākumi, mitigācijas plāni un paraugprakses pret kritiskas atkarības situācijām, potenciāliem kritiskiem atteices punktiem, draudiem, ievainojamībām un citiem riskiem, kas saistīti ar piegādes ķēdi, un būtu jāizpēta, kā vēl vairāk veicināt to plašāku pieņemšanu būtiskās un svarīgās vienībās. Potenciāli netehniski riska faktori, piemēram, nepamatota trešās valsts ietekme uz piegādātājiem un pakalpojumu sniedzējiem, jo īpaši alternatīvu pārvaldības modeļu gadījumā, ietver slēptas ievainojamības vai slepenpiekļuves un potenciālus sistēmiskus piegādes traucējumus, it sevišķi tehnoloģiskās iesīkstes vai atkarības no pakalpojumu sniedzējiem gadījumā.

(91) Koordinētajos piegādes ķēžu drošības riska novērtējumos, ievērojot attiecīgās nozares iezīmes, būtu jāņem vērā gan tehniski, gan attiecīgā gadījumā netehniski faktori, tai skaitā tie, kuri definēti Ieteikumā (ES) 2019/534, ES koordinētajā 5G tīklu kiberdrošības riska novērtējumā un ES 5G kiberdrošības rīkkopā, par ko vienojusies sadarbības grupa. Lai apzinātu piegādes ķēdes, par kurām būtu jāveic koordinēts drošības riska novērtējums, būtu jāņem vērā šādi kritēriji: i) tas, ciktāl būtiskās un svarīgās vienības izmanto konkrētus kritiskus IKT pakalpojumus, IKT sistēmas vai IKT produktus un paļaujas uz tiem; ii) konkrētu kritisku IKT pakalpojumu, IKT sistēmu vai IKT produktu relevance kritisku vai sensitīvu funkciju izpildē, arī persondatu apstrādē; iii) alternatīvu IKT pakalpojumu, IKT sistēmu vai IKT produktu pieejamība; iv) IKT pakalpojumu, IKT sistēmu vai IKT produktu vispārējās piegādes ķēdes noturība visā aprites ciklā pret notikumiem, kas izraisa traucējumus, un v) attiecībā uz jauniem IKT pakalpojumiem, IKT sistēmām vai IKT produktiem – to potenciālais turpmākais nozīmīgums vienību darbībām. Turklāt īpašs uzsvars būtu jāliek uz IKT pakalpojumiem, IKT sistēmām vai IKT produktiem, uz kuriem attiecas konkrētas trešo valstu prasības.

(92) Lai racionalizētu pienākumus, kas tīklu un informācijas sistēmu drošības sakarā noteikti publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem un uzticamības pakalpojumu sniedzējiem, un lai šīs vienības un kompetentās iestādes, kas paredzētas attiecīgi Eiropas Parlamenta un Padomes Direktīvā (ES) 2018/1972 ([20]) un Regulā (ES) Nr. 910/2014, varētu gūt labumu no tiesiskā regulējuma, kas izveidots ar šo direktīvu, tostarp par incidentu risināšanu atbildīgo *CSIRT* izraudzīšanos, attiecīgo kompetento iestāžu piedalīšanos sadarbības grupas un *CSIRT* tīkla darbā, minētās vienības būtu jāiekļauj šīs direktīvas darbības jomā. Tāpēc attiecīgie noteikumi, kas paredzēti Regulā (ES) Nr. 910/2014 un Direktīvā (ES) 2018/1972 un ir saistīti ar drošības un paziņošanas prasību piemērošanu minēto veidu vienībām, būtu jāsvītro. Šajā direktīvā paredzētajiem noteikumiem par ziņošanas pienākumiem nebūtu jāskar Regula (ES) 2016/679 un Direktīva 2002/58/EK.

(93) Šajā direktīvā noteiktie kiberdrošības pienākumi būtu jāuzskata par papildinājumu prasībām, kas uzticamības pakalpojumu sniedzējiem noteiktas ar Regulu (ES) Nr. 910/2014. Būtu jāprasa, lai uzticamības pakalpojumu sniedzēji saskaņā ar šo direktīvu veic visus pienācīgos un samērīgos pasākumus tādu risku pārvaldīšanai, kas tiek radīti to pakalpojumiem, tostarp attiecībā uz klientiem un atkarīgajām trešām pusēm, un ziņo par incidentiem. Šādiem kiberdrošības un ziņošanas pienākumiem būtu jāattiecas arī uz sniegto pakalpojumu fizisko aizsardzību. Regulas (ES) Nr. 910/2014 24. pantā noteiktās prasības kvalificētiem uzticamības pakalpojumu sniedzējiem joprojām ir piemērojamas.

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

([20]) 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.).

(94) Lai nodrošinātu pašreizējās prakses turpināšanu un izmantotu Regulā (ES) Nr. 910/2014 piemērošanā gūtās zināšanas un pieredzi, dalībvalstis var piešķirt kompetento iestāžu lomu uzticamības pakalpojumu jomā uzraudzības iestādēm, kas norādītas minētajā regulā. Šādā gadījumā kompetentajām iestādēm saskaņā ar šo direktīvu būtu laikus un cieši jāsadarbojas ar minētajām uzraudzības iestādēm, apmainoties ar relevanto informāciju, lai nodrošinātu uzticamības pakalpojumu sniedzēju rezultatīvu uzraudzību un atbilstību šajā direktīvā un Regulā (ES) Nr. 910/2014 noteiktajām prasībām. Attiecīgā gadījumā *CSIRT* vai kompetentajai iestādei saskaņā ar šo direktīvu būtu nekavējoties jāinformē Regulā (ES) Nr. 910/2014 paredzētā uzraudzības iestāde par visiem paziņotajiem būtiskajiem kiberdraudiem vai incidentiem, kas ietekmē uzticamības pakalpojumus, kā arī par jebkādu uzticamības pakalpojumu sniedzēja šīs direktīvas pārkāpumu. Dalībvalstis ziņošanas nolūkā var attiecīgā gadījumā izmantot vienoto iesniegšanas punktu, kas izveidots, lai panāktu vienotu un automātisku ziņošanu par incidentiem gan Regulā (ES) Nr. 910/2014 paredzētajai uzraudzības iestādei, gan *CSIRT* vai šajā direktīvā paredzētajai kompetentajai iestādei.

(95) Attiecīgā gadījumā un lai izvairītos no nevajadzīgiem traucējumiem, šīs direktīvas transponēšanā būtu jāņem vērā pastāvošās valsts pamatnostādnes, kas pieņemtas, lai transponētu ar drošības pasākumiem saistītos noteikumus, kuri paredzēti Direktīvas (ES) 2018/1972 40. un 41. pantā, tādējādi izmantojot zināšanas un prasmes, kas attiecībā uz drošības pasākumiem un incidentu ziņošanu jau iegūtas Direktīvas (ES) 2018/1972 kontekstā. *ENISA* var arī izstrādāt norādījumus par drošības prasībām un par ziņošanas pienākumiem publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem, lai atvieglotu saskaņošanu un pāreju un lai līdz minimumam samazinātu traucējumus. Lai nodrošinātu pašreizējās prakses turpināšanu un izmantotu Direktīvas (ES) 2018/1972 īstenošanā gūtās zināšanas un pieredzi, dalībvalstis kompetento iestāžu lomu elektronisko sakaru jomā var piešķirt valsts regulatīvajām iestādēm, kas paredzētas minētajā direktīvā.

(96) Tā kā palielinās numurneatkarīgo starppersonu sakaru pakalpojumu, kā tie definēti Direktīvā (ES) 2018/1972, nozīme, ir jānodrošina, ka uz tiem attiecas arī attiecīgās drošības prasības, ņemot vērā to specifiku un ekonomisko svaru. Tā kā uzbrukumu tvērums joprojām paplašinās, numurneatkarīgie starppersonu sakaru pakalpojumi, piemēram, ziņapmaiņas pakalpojumi, kļūst par tipiskiem uzbrukumu vektoriem. Ļaunprātīgi nodarījumu veicēji izmanto platformas, lai sazinātos ar upuriem un tos mudinātu atvērt kompromitētas tīmekļa lapas, tādējādi palielinot tādu incidentu iespējamību, kuros tiek izmantoti persondati un tālāk arī tiek ietekmēta tīklu un informācijas sistēmu drošība. Numurneatkarīgo starppersonu sakaru pakalpojumu sniedzējiem būtu jānodrošina radītajam riskam atbilstošs tīklu un informācijas sistēmu drošības līmenis. Tā kā numurneatkarīgo starppersonu sakaru pakalpojumu sniedzēji nemēdz faktiski kontrolēt signālu pārraidi tīklos, riskus šādiem pakalpojumiem savā ziņā var uzskatīt par zemākiem nekā tradicionālajiem elektronisko sakaru pakalpojumiem. Tas pats attiecas uz starppersonu sakaru pakalpojumiem, kā tie definēti Direktīvā (ES) 2018/1972, kuros izmanto numurus un kuros netiek īstenota faktiska kontrole pār signālu pārraidi.

(97) Iekšējais tirgus ir vairāk nekā jebkad iepriekš atkarīgs no interneta darbības. Gandrīz visu būtisko un svarīgo vienību pakalpojumi ir atkarīgi no internetā sniegtiem pakalpojumiem. Lai nodrošinātu būtisko un svarīgo vienību pakalpojumu netraucētu sniegšanu, ir svarīgi, lai visiem publisko elektronisko sakaru tīklu nodrošinātājiem būtu ieviesti pienācīgi kiberdrošības risku pārvaldības pasākumi un lai tie ziņotu par saistītajiem būtiskajiem incidentiem. Dalībvalstīm būtu jānodrošina, ka tiek saglabāta publisko elektronisko sakaru tīklu drošība un ka to būtiskās drošības intereses ir aizsargātas pret sabotāžu un spiegošanu. Tā kā starptautiskā savienotība uzlabo un paātrina Savienības un tās ekonomikas konkurētspējīgu digitalizāciju, par incidentiem, kas ietekmē zemūdens sakaru kabeļus, būtu jāziņo *CSIRT* vai attiecīgā gadījumā kompetentajai iestādei. Valsts kiberdrošības stratēģijās attiecīgā gadījumā būtu jāņem vērā zemūdens sakaru kabeļu kiberdrošība un jāietver potenciālo kiberdrošības risku apzināšana un mazināšanas pasākumi, lai nodrošinātu visaugstāko to aizsardzības līmeni.

(98) Lai aizsargātu publisko elektronisko sakaru tīklu un publiski pieejamu elektronisko sakaru pakalpojumu drošību, būtu jāveicina šifrēšanas tehnoloģiju, jo īpaši galšifrēšanas, izmantošana, kā arī uz datiem vērstas drošības koncepcijas, piemēram, kartogrāfija, segmentācija, marķēšana, piekļuves politika un piekļuves pārvaldība, kā arī automatizēti piekļuves lēmumi. Vajadzības gadījumā šifrēšanas, jo īpaši galšifrēšanas, izmantošanai šīs direktīvas nolūkos vajadzētu būt obligātai publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem saskaņā ar tādiem principiem kā drošība un privātums pēc noklusējuma un integrēta drošības un privātuma aizsardzība. Galšifrēšanas izmantošana būtu jāsaskaņo ar dalībvalstu pilnvarām nodrošināt dalībvalstu būtisko drošības interešu un sabiedrības drošības aizsardzību un varēt izmeklēt un atklāt noziedzīgus nodarījumus un par tiem veikt krimināltvajāšanu saskaņā ar Savienības tiesību aktiem. Tomēr tam nevajadzētu vājināt galšifrēšanu, kas ir kritiska tehnoloģija reālai datu un privātuma aizsardzībai un sakaru drošībai.

(99) Lai aizsargātu publisko elektronisko sakaru tīklu un publiski pieejamu elektronisko sakaru pakalpojumu drošību un nepieļautu to ļaunprātīgu izmantošanu un manipulēšanu, būtu jāveicina drošu maršrutēšanas standartu izmantošana, kas nodrošinātu maršrutēšanas funkciju integritāti un stabilitāti interneta piekļuves pakalpojumu sniedzēju ekosistēmā.

(100) Lai aizsargātu interneta funkcionalitāti un integritāti un veicinātu DNS drošību un noturību, attiecīgās ieinteresētās personas, tostarp Savienības privātā sektora vienības, publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji, it sevišķi interneta piekļuves pakalpojumu sniedzēji, un tiešsaistes meklētājprogrammu nodrošinātāji būtu jāmudina pieņemt DNS atrises dažādošanas stratēģiju. Dalībvalstīm būtu arī jāmudina izstrādāt un izmantot publisku un drošu Eiropas DNS atrisinātāja pakalpojumu.

(101) Šī direktīva nosaka vairākposmu pieeju būtisku incidentu paziņošanai, lai panāktu pareizo līdzsvaru starp ātru ziņošanu, kas palīdz mazināt būtisku incidentu potenciālo izplatīšanos un dod būtiskām un svarīgām vienībām iespēju lūgt atbalstu, no vienas puses, un padziļinātu ziņošanu, kurā izdara vērtīgus secinājumus par individuāliem incidentiem un kura laika gaitā uzlabo individuālu vienību un veselu nozaru kibernoturību, no otras puses. Šajā sakarā šajā direktīvā būtu jāiekļauj arī ziņošana par tādiem incidentiem, kuri, spriežot pēc attiecīgās vienības veiktā sākotnējā novērtējuma, varētu minētajai vienībai izraisīt smagus pakalpojumu darbības traucējumus vai finansiālus zaudējumus vai ietekmēt citas fiziskas vai juridiskas personas, radot būtisku materiālu vai nemateriālu kaitējumu. Šādā sākotnējā novērtējumā cita starpā būtu jāņem vērā skartās tīklu un informācijas sistēmas, jo īpaši to nozīmība vienības pakalpojumu sniegšanā, kiberdraudu smagums un tehniskās īpašības, kā arī visas izmantotās pamatā esošās ievainojamības un vienības pieredze ar līdzīgiem incidentiem. To, vai pakalpojuma darbības traucējums ir smags, varētu ļoti palīdzēt noteikt tādi rādītāji kā apmērs, kādā tiek ietekmēta pakalpojuma darbība, incidenta ilgums un skarto pakalpojumu saņēmēju skaits.

(102) Ja būtiskam un svarīgām vienībām kļūst zināms par būtisku incidentu, tām vajadzētu būt pienākumam bez nepamatotas kavēšanās un katrā ziņā 24 stundu laikā sniegt agrīnu brīdinājumu. Pēc minētā agrīnā brīdinājuma būtu jāziņo par incidentu. Attiecīgajām vienībām par incidentu būtu jāziņo bez nepamatotas kavēšanās un katrā ziņā 72 stundu laikā pēc tam, kad tās uzzinājušas par būtisko incidentu, lai it sevišķi atjauninātu informāciju, kas sniegta ar agrīno brīdinājumu, un norādītu būtiskā incidenta sākotnējo novērtējumu, tostarp tā smagumu un ietekmi, kā arī, ja pieejami, aizskāruma rādītājus. Ne vēlāk kā vienu mēnesi pēc incidenta paziņošanas būtu jāsniedz galīgs ziņojums. Agrīnajā brīdinājumā būtu jāiekļauj tikai tāda informācija, kas ir nepieciešama, lai darītu incidentu zināmu *CSIRT* vai attiecīgā gadījumā kompetentajai iestādei un attiecīgā vienība vajadzības gadījumā varētu lūgt palīdzību. Šādā agrīnajā brīdinājumā attiecīgā gadījumā būtu jānorāda, vai ir aizdomas, ka būtisko incidentu ir izraisījušas nelikumīgas vai ļaunprātīgas darbības, un vai tam varētu būt pārrobežu ietekme. Dalībvalstīm būtu

jānodrošina, ka pienākums iesniegt šo agrīno brīdinājumu vai tam sekojošo paziņojumu par incidentu nenovirza paziņotājas vienības resursus no darbībām, kas saistītas ar incidentu risināšanu un kam būtu jāpiešķir prioritāte, lai nepieļautu, ka incidentu ziņošanas pienākumi novirza resursus no reaģēšanas uz būtiskiem incidentiem vai citādi apdraud vienības centienus šajā sakarā. Ja galīgā ziņojuma iesniegšanas laikā incidents turpinās, dalībvalstīm būtu jānodrošina, ka attiecīgās vienības tajā laikā iesniedz progresa ziņojumu un viena mēneša laikā pēc būtiskā incidenta risināšanas – galīgo ziņojumu.

(103) Attiecīgā gadījumā būtiskajām un svarīgajām vienībām bez nepamatotas kavēšanās būtu jāpaziņo saviem pakalpojumu saņēmējiem par visiem pasākumiem vai korektīvajām darbībām, ko var veikt, lai mazinātu riskus, kuri izriet no būtiskiem kiberdraudiem. Minētajām vienībām attiecīgā gadījumā un jo īpaši tad, ja būtiskie kiberdraudi varētu īstenoties, būtu pakalpojumu saņēmēji jāinformē arī par pašiem draudiem. Prasība informēt minētos saņēmējus par būtiskiem kiberdraudiem būtu jāpilda, cik vien iespējams, bet tai nebūtu jāatbrīvo minētās vienības no pienākuma par saviem līdzekļiem veikt pienācīgus un tūlītējus pasākumus, lai novērstu vai izlabotu jebkurus šādus draudus un atjaunotu normālo pakalpojuma drošības līmeni. Šāda informācija par būtiskiem kiberdraudiem būtu jāsniedz pakalpojumu saņēmējiem bez maksas un viegli saprotamā valodā.

(104) Publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem būtu jāievieš integrēta drošība un drošība pēc noklusējuma un jāinformē pakalpojumu saņēmēji par būtiskiem kiberdraudiem un par pasākumiem, ko tie var veikt, lai aizsargātu savu ierīču un sakaru drošību, izmantojot, piemēram, konkrētu veidu programmatūru vai šifrēšanas tehnoloģijas.

(105) Proaktīva pieeja kiberdraudiem ir būtisks kiberdrošības risku pārvaldības pasākumu komponents, kam būtu kompetentajām iestādēm jādod iespēja rezultatīvi novērst kiberdraudu materializēšanos incidentos, kas var radīt ievērojamu materiālo vai nemateriālo kaitējumu. Šajā nolūkā ļoti svarīgi ir ziņot par kiberdraudiem. Tāpēc vienības tiek mudinātas par kiberdraudiem ziņot brīvprātīgi.

(106) Lai vienkāršotu šajā direktīvā prasītās informācijas paziņošanu, kā arī samazinātu administratīvo slogu vienībām, dalībvalstīm relevantās ziņojamās informācijas iesniegšanai būtu jānodrošina tehniskie līdzekļi, piemēram, vienots iesniegšanas punkts, automatizētas sistēmas, tiešsaistes veidlapas, lietotājdraudzīgas saskarnes, veidnes, specializētas platformas vienībām neatkarīgi no tā, vai tās ietilpst šīs direktīvas darbības jomā. Savienības finansējums, kas atbalsta šīs direktīvas īstenošanu, jo īpaši programmā "Digitālā Eiropa", kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/694 ([21]), varētu ietvert atbalstu vienotajiem iesniegšanas punktiem. Turklāt vienības bieži atrodas situācijā, kurā konkrēts incidents tā iezīmju dēļ ir jāpaziņo dažādām iestādēm, jo to paredz paziņošanas pienākumi, kas ietverti dažādos tiesību instrumentos. Šādi gadījumi rada papildu administratīvo slogu un varētu arī izraisīt nenoteiktību attiecībā uz šādu paziņojumu formātu un procedūrām. Ja ir izveidots vienots iesniegšanas punkts, dalībvalstis tiek mudinātas izmantot šo vienoto iesniegšanas punktu arī tādiem paziņojumiem par drošības incidentiem, kas prasīti citos Savienības tiesību aktos, piemēram, Regulā (ES) 2016/679 un Direktīvā 2002/58/EK. Šāda vienota iesniegšanas punkta izmantošanai ziņošanai par drošības incidentiem saskaņā ar Regulu (ES) 2016/679 un Direktīvu 2002/58/EK nevajadzētu ietekmēt Regulas (ES) 2016/679 un Direktīvas 2002/58/EK noteikumu piemērošanu, jo īpaši to noteikumu piemērošanu, kas attiecas uz tajās minēto iestāžu neatkarību. *ENISA* sadarbībā ar sadarbības grupu būtu jāizstrādā vienotas paziņojumu veidnes, pieņemot pamatnostādnes, lai vienkāršotu un racionalizētu ziņojamo informāciju, ko pieprasa Savienības tiesību akti, un mazinātu administratīvo slogu paziņotājām vienībām.

(107) Ja ir aizdomas, ka incidents ir saistīts ar smagām noziedzīgām darbībām, kas noteiktas Savienības vai valsts tiesību aktos, dalībvalstīm būtu jāmudina būtiskās un svarīgās vienības, pamatojoties uz piemērojamiem krimināprocesa noteikumiem atbilstoši Savienības tiesībām, par incidentiem, kam varētu būt smagas noziedzības raksturs, ziņot attiecīgajām tiesībaizsardzības iestādēm. Attiecīgos gadījumos un neskarot persondatu aizsardzības noteikumus, kas piemērojami Eiropolam, vēlams, ka Eiropas Kibernoziedzības apkarošanas centrs (EC3) un *ENISA* veicina koordināciju starp dažādu dalībvalstu kompetentajām iestādēm un tiesībaizsardzības iestādēm.

([21]) Eiropas Parlamenta un Padomes Regula (ES) 2021/694 (2021. gada 29. aprīlis), ar ko izveido programmu "Digitālā Eiropa" un atceļ Lēmumu (ES) 2015/2240 (OV L 166, 11.5.2021., 1. lpp.).

(108) Incidentu dēļ daudzos gadījumos tiek apdraudēti persondati. Šajā kontekstā kompetentajām iestādēm būtu jāsadarbojas un jāapmainās ar informāciju par visiem attiecīgajiem jautājumiem ar iestādēm, kas minētas Regulā (ES) 2016/679 un Direktīvā 2002/58/EK.

(109) Lai nodrošinātu DNS drošību, stabilitāti un noturību, kas savukārt veicina vienādi augsta līmeņa kiberdrošību Savienībā, ir būtiski uzturēt precīzas un pilnīgas datubāzes ar domēnu nosaukumu reģistrācijas datiem (*WHOIS* dati) un nodrošināt likumīgu piekļuvi šādiem datiem. Šajā konkrētajā nolūkā ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jānosaka prasība apstrādāt konkrētus datus, kas vajadzīgi minētā mērķa sasniegšanai. Šādai apstrādei vajadzētu būt juridiskam pienākumam Regulas (ES) 2016/679 6. panta 1. punkta c) apakšpunkta nozīmē. Minētais pienākums neskar iespēju vākt domēnu nosaukumu reģistrācijas datus citiem mērķiem, piemēram, pamatojoties uz līgumattiecībām vai juridiskām prasībām, kas noteiktas citos Savienības vai valsts tiesību aktos. Minētā pienākuma mērķis ir iegūt pilnīgu un precīzu reģistrācijas datu kopumu, un tam nevajadzētu novest pie tā, ka vienus un tos pašus datus vāc vairākas reizes. ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jāsadarbojas, lai izvairītos no minētā uzdevuma izpildes dublēšanās.

(110) Domēna nosaukumu reģistrācijas datu pieejamība un savlaicīga piekļūstamība leģitīmiem piekļuves prasītājiem ir būtiska DNS ļaunprātīgas izmantošanas novēršanai un apkarošanai, kā arī incidentu novēršanai un atklāšanai un reaģēšanai uz tiem. Ar leģitīmiem piekļuves prasītājiem saprot jebkuru fizisku vai juridisku personu, kas iesniedz pieprasījumu, ievērojot Savienības vai valsts tiesību aktus. To vidū var būt iestādes, kas ir kompetentas saskaņā ar šo direktīvu, un iestādes, kas saskaņā ar Savienības vai valsts tiesību aktiem ir kompetentas novērst, izmeklēt, atklāt noziedzīgus nodarījumus vai veikt par tiem kriminālvajāšanu, kā arī *CERT* vai *CSIRT*. ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu arī jānosaka prasība nodrošināt leģitīmiem piekļuves prasītājiem likumīgu piekļuvi konkrētiem domēnu nosaukumu reģistrācijas datiem, kas vajadzīgi prasītās piekļuves mērķiem, saskaņā ar Savienības un valsts tiesību aktiem. Leģitīmu piekļuves prasītāju pieprasījumam būtu jāpievieno pamatojums, pēc kā var novērtēt nepieciešamību piekļūt datiem.

(111) Lai nodrošinātu precīzu un pilnīgu domēnu nosaukumu reģistrācijas datu pieejamību, ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jāvāc domēnu nosaukumu reģistrācijas dati un jāgarantē to integritāte un pieejamība. Konkrētāk, ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jāizstrādā rīcībpolitikas un procedūras precīzu un pilnīgu domēnu nosaukumu reģistrācijas datu vākšanai un uzturēšanai, kā arī neprecīzu reģistrācijas datu novēršanai un izlabošanai saskaņā ar Savienības datu aizsardzības tiesību aktiem. Minētajās rīcībpolitikās un procedūrās pēc iespējas būtu jāņem vērā standarti, ko starptautiskā līmenī izstrādājušas daudzpusējās ieinteresēto personu pārvaldības struktūras. ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jāpieņem un jāīsteno samērīgas domēnu nosaukumu reģistrācijas datu verifikācijas procedūras. Minētajām procedūrām būtu jāatspoguļo nozarē izmantotās paraugprakses un, ciktāl iespējams, elektroniskās identifikācijas jomā panāktais progress. Verifikācijas procedūru piemēri var būt *ex ante* kontroles, ko veic reģistrācijas laikā, un *ex post* kontroles, ko veic pēc reģistrācijas. ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu it īpaši jāverificē vismaz viens no reģistrētāja saziņas līdzekļiem.

(112) ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jānosaka prasība darīt publiski pieejamus domēnu nosaukumu reģistrācijas datus, uz kuriem neattiecas Savienības datu aizsardzības tiesību akti, piemēram, datus, kuri attiecas uz juridiskām personām, saskaņā ar Regulu (ES) 2016/679. Attiecībā uz juridiskām personām ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jādara publiski pieejams vismaz reģistrētāja nosaukums un kontakttālruņa numurs. Būtu jāpublicē arī saziņas e-pasta adrese ar noteikumu, ka tā nesatur persondatus, piemēram, e-pasta pseidonīmu vai funkcionālo kontu gadījumā. ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu arī jānodrošina leģitīmiem piekļuves prasītājiem likumīga piekļuve konkrētiem domēnu nosaukumu reģistrācijas datiem par fiziskām personām saskaņā ar Savienības datu aizsardzības tiesību aktiem. Dalībvalstīm būtu jāprasa, lai ALD nosaukumu reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, bez nepamatotas kavēšanās atbild uz leģitīmo piekļuves prasītāju pieprasījumiem izpaust domēna nosaukumu reģistrācijas datus. ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jāizstrādā rīcībpolitikas un procedūras reģistrācijas datu, tostarp pakalpojumu līmeņa līgumu, publicēšanai un izpaušanai, lai izpildītu leģitīmo piekļuves prasītāju piekļuves pieprasījumus. Minētajās rīcībpolitikās un procedūrās pēc iespējas būtu jāņem vērā jebkādi norādījumi un standarti, ko

starptautiskā līmenī izstrādājušas daudzpusējās ieinteresēto personu pārvaldības struktūras. Piekļuves procedūrā varētu ietvert saskarnes, portāla vai citu tehnisku rīku izmantošanu nolūkā nodrošināt efektīvu sistēmu reģistrācijas datu pieprasīšanai un piekļūšanai tiem. Lai veicinātu saskaņotu praksi visā iekšējā tirgū, Komisija, neskarot Eiropas Datu aizsardzības kolēģijas kompetenci, var sniegt pamantostādnes par šādām procedūrām, kurās, cik iespējams, ņemti vērā standarti, ko starptautiskā līmenī izstrādājušas daudzpusējās ieinteresēto personu pārvaldības struktūras. Dalībvalstīm būtu jānodrošina, ka visu veidu piekļuve personu un nepersonu domēna nosaukumu reģistrācijas datiem ir bez maksas.

(113) Būtu jāuzskata, ka vienības, kuras ietilpst šīs direktīvas darbības jomā, ir tās dalībvalsts jurisdikcijā, kurā tās ir iedibinātas. Tomēr būtu jāuzskata, ka publisko elektronisko sakaru tīklu nodrošinātāji vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji ir tās dalībvalsts jurisdikcijā, kurā tie sniedz savus pakalpojumus. Būtu jāuzskata, ka DNS pakalpojumu sniedzēji, ALD nosaukumu reģistri, vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, mākoņdatošanas pakalpojumu sniedzēji, datu centru pakalpojumu sniedzēji, satura piegādes tīklu nodrošinātāji, pārvaldītu pakalpojumu sniedzēji un pārvaldītu drošības pakalpojumu sniedzēji, kā arī tiešsaistes tirdzniecības vietu nodrošinātāji, tiešsaistes meklētājprogrammu nodrošinātāji un sociālās tīklošanās pakalpojumu platformu nodrošinātāji ir tās dalībvalsts jurisdikcijā, kurā ir to galvenā iedibinājuma vieta Savienībā. Valsts pārvaldes vienībām vajadzētu būt tās dalībvalsts jurisdikcijā, kura tās ir izveidojusi. Ja vienība sniedz pakalpojumus vai ir iedibināta vairāk nekā vienā dalībvalstī, tai vajadzētu būt katras attiecīgās dalībvalsts atsevišķā un vienlaicīgā jurisdikcijā. Šo dalībvalstu kompetentajām iestādēm būtu jāsadarbojas, jāsniedz savstarpēja palīdzība un attiecīgā gadījumā jāveic kopīgas uzraudzības darbības. Ja dalībvalstis īsteno jurisdikciju, tām nebūtu jānosaka izpildes pasākumi vai jāuzliek sodi par vienu un to pašu rīcību vairāk nekā vienu reizi saskaņā ar ne *bis in idem* principu.

(114) Lai ņemtu vērā DNS pakalpojumu sniedzēju, ALD nosaukumu reģistru, vienību, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, mākoņdatošanas pakalpojumu sniedzēju, datu centra pakalpojumu sniedzēju, satura piegādes tīklu nodrošinātāju, pārvaldītu pakalpojumu sniedzēju, pārvaldītu drošības pakalpojumu sniedzēju, kā arī tiešsaistes tirdzniecības vietu nodrošinātāju, tiešsaistes meklētājprogrammu nodrošinātāju un sociālās tīklošanās pakalpojumu platformu nodrošinātāju pakalpojumu un darbību pārrobežu raksturu, tikai vienai dalībvalstij vajadzētu būt jurisdikcijai pār šādām vienībām. Jurisdikcija būtu jāpiešķir tai dalībvalstij, kurā attiecīgajai vienībai ir tās galvenais iedibinājums Savienībā. Iedibinājuma kritērijs šīs direktīvas nolūkos nozīmē darbības reālu īstenošanu ar stabilu veidojumu. Šāda veidojuma juridiskā forma neatkarīgi no tā, vai tā ir filiāle vai meitasuzņēmums ar juridiskas personas statusu, šajā ziņā nav noteicošais faktors. Tam, vai šis kritērijs ir izpildīts, nevajadzētu 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 iedibinājumu un tāpēc nav izšķirīgs kritērijs galvenā iedibinājuma noteikšanai. Būtu jāuzskata, ka galvenais iedibinājums ir tajā dalībvalstī, kur Savienībā tiek pieņemts vairums ar kiberdrošības riska pārvaldības pasākumiem saistīto lēmumu. Parasti tā ir vieta, kur atrodas vienības centrālā administrācija Savienībā. Ja šādu dalībvalsti nevar noteikt vai ja šādus lēmumus nepieņem Savienībā, būtu jāuzskata, ka galvenais iedibinājums ir dalībvalstī, kurā tiek veiktas kiberdrošības darbības. Ja šādu dalībvalsti nevar noteikt, būtu jāuzskata, ka galvenais iedibinājums ir dalībvalstī, kurā vienībai ir iedibinājums ar vislielāko darbinieku skaitu Savienībā. Ja pakalpojumus sniedz uzņēmumu grupa, par uzņēmumu grupas galveno iedibinājumu būtu jāuzskata kontrolējošā uzņēmuma galvenais iedibinājums.

(115) Ja publisko elektronisko sakaru tīklu nodrošinātājs vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējs publiski pieejamu rekursīvu DNS pakalpojumu sniedz tikai kā daļu no interneta piekļuves pakalpojuma, būtu jāuzskata, ka vienība ir visu to dalībvalstu jurisdikcijā, kurās tiek sniegti tās pakalpojumi.

(116) Ja DNS pakalpojumu sniedzējs, ALD nosaukumu reģistrs, vienība, kas sniedz domēna nosaukumu reģistrācijas pakalpojumus, mākoņdatošanas pakalpojumu sniedzējs, datu centra pakalpojumu sniedzējs, satura piegādes tīklu nodrošinātājs, pārvaldītu pakalpojumu sniedzējs, pārvaldītu drošības pakalpojumu sniedzējs vai tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas vai sociālās tīklošanās pakalpojumu platformas nodrošinātājs, kas nav iedibināts Savienībā, piedāvā pakalpojumus Savienībā, tam būtu jāizraugās pārstāvis Savienībā. Lai noteiktu, vai šāda vienība piedāvā pakalpojumus Savienībā, būtu jānoskaidro, vai vienība plāno piedāvāt pakalpojumus personām vienā vai vairākās dalībvalstīs. Būtu jāuzskata, ka, lai noskaidrotu šādu nodomu, nepietiek tikai ar to vien, ka Savienībā ir piekļūstama vienības vai starpnieka tīmekļa vietne, e-pasta adrese vai cita kontaktinformācija vai ka tiek izmantota valoda, ko parasti izmanto trešā valstī, kurā vienība ir iedibināta. Tomēr tādi faktori kā tādas valodas vai valūtas izmantošana, ko parasti izmanto vienā vai vairākās dalībvalstīs, ar iespēju pasūtīt pakalpojumus minētajā valodā vai Savienībā esošu klientu vai lietotāju pieminēšana varētu skaidri liecināt, ka vienība plāno piedāvāt pakalpojumus Savienībā. Pārstāvim būtu jārīkojas vienības vārdā, un kompetentajām iestādēm vai *CSIRT* vajadzētu būt iespējai ar pārstāvi sazināties. Pārstāvis būtu jāizraugās nepārprotami ar vienības rakstisku pilnvarojumu rīkoties tās vārdā attiecībā uz tās pienākumiem, kas noteikti šajā direktīvā, tostarp ziņošanu par incidentiem.

(117) Lai gūtu skaidru pārskatu par DNS pakalpojumu sniedzējiem, ALD nosaukumu reģistriem, vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīklu nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem un pārvaldītu drošības pakalpojumu sniedzējiem, kā arī tiešsaistes tirdzniecības vietu nodrošinātājiem, tiešsaistes meklētājprogrammu nodrošinātājiem un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem, kas sniedz pakalpojumus Savienībā, kuri ietilpst šīs direktīvas darbības jomā, *ENISA* būtu jāizveido un jāuztur šādu vienību reģistrs, kura pamatā būtu informācija, kas saņemta no dalībvalstīm, attiecīgā gadījumā – ar valstu mehānismiem, kas izveidoti, lai vienības reģistrētos. Vienotajiem kontaktpunktiem informācija un jebkādas tās izmaiņas būtu jāpārsūta *ENISA*. Lai nodrošinātu minētajā reģistrā iekļaujamās informācijas precizitāti un pilnīgumu, dalībvalstis var iesniegt *ENISA* valsts reģistros pieejamo informāciju par minētajām vienībām. *ENISA* un dalībvalstīm būtu jāveic šādu reģistru sadarbspējas veicināšanas pasākumi, bet vienlaikus arī jānodrošina konfidenciālas vai klasificētas informācijas aizsardzība. *ENISA* būtu jāizstrādā pienācīgi informācijas klasifikācijas un pārvaldības protokoli, lai nodrošinātu izpaustās informācijas drošību un konfidencialitāti un lai ierobežotu piekļuvi šādai informācijai, tās glabāšanu un pārsūtīšanu paredzētajiem lietotājiem.

(118) Ja notiek apmaiņa ar informāciju, kas saskaņā ar Savienības vai valsts tiesību aktiem ir klasificēta, šāda informācija tiek paziņota vai citādi kopīgota atbilstoši šai direktīvai, būtu jāpiemēro attiecīgie noteikumi par rīcību ar klasificētu informāciju. Turklāt *ENISA* rīcībā vajadzētu būt infrastruktūrai, procedūrām un noteikumiem sensitīvas un klasificētas informācijas apstrādei saskaņā ar piemērojamajiem drošības noteikumiem par ES klasificētas informācijas aizsardzību.

(119) Tā kā kiberdraudi kļūst sarežģītāki un attīstītāki, labi šādu draudu atklāšanas un profilakses pasākumi lielā mērā ir atkarīgi no regulāras apdraudējuma un neaizsargātības izlūkdatu kopīgošanas starp vienībām. Informācijas kopīgošana uzlabo informētību par kiberdraudiem, kas savukārt uzlabo vienību spēju novērst šādu draudu pārtapšanu reālos incidentos un dod tām iespēju labāk ierobežot incidentu ietekmi un efektīvāk no tiem atgūties. Nepastāvot Savienības līmeņa norādījumiem, šādu izlūkdatu apmaiņu, šķiet, ir kavējuši dažādi faktori, jo īpaši nenoteiktība attiecībā uz saderību ar konkurences un atbildības noteikumiem.

(120) Vienības būtu jāmudina ar dalībvalstu atbalstu kolektīvi izmantot savas individuālās zināšanas un praktisko pieredzi stratēģiskajā, taktiskajā un operacionālajā līmenī, lai uzlabotu savas spējas pienācīgi novērst, atklāt incidentus, reaģēt uz tiem vai atgūties no tiem, vai mazināt to sekas. Tāpēc ir nepieciešams pavērt ceļu brīvprātīgiem kiberdrošības informācijas kopīgošanas mehānismiem Savienības līmenī. Šajā nolūkā dalībvalstīm būtu aktīvi jāatbalsta un jāmudina šādos informācijas kopīgošanas mehānismos piedalīties vienības, piemēram, vienības, kas koncentrējas uz kiberdrošības pakalpojumiem un pētījumiem, kā arī attiecīgās vienības, kas nav šīs direktīvas darbības jomā. Minētie pasākumi būtu jāizveido saskaņā ar Savienības konkurences noteikumiem un Savienības datu aizsardzības tiesību aktiem.

(121) Persondatu apstrādi, ciktāl tā ir nepieciešama un samērīga ar nolūku būtiskajām un svarīgajām vienībām nodrošināt tīklu un informācijas sistēmu drošību, varētu uzskatīt par likumīgu, pamatojoties uz to, ka šāda apstrāde atbilst pārzinim uzliktajam juridiskajam pienākumam saskaņā ar Regulas (ES) 2016/679 6. panta 1. punkta c) apakšpunkta un 6. panta 3. punkta prasībām. Persondatu apstrāde varētu būt nepieciešama arī leģitīmām interesēm, kas ir būtiskajām un svarīgajām vienībām, kā arī drošības tehnoloģiju un pakalpojumu sniedzējiem, kuri rīkojas minēto vienību vārdā, saskaņā ar Regulas (ES) 2016/679 6. panta 1. punkta f) apakšpunktu, arī tad, ja šāda apstrāde ir nepieciešama kiberdrošības informācijas kopīgošanas mehānismiem vai brīvprātīgai relevantās informācijas paziņošanai saskaņā ar šo direktīvu. Pasākumiem, kas saistīti ar incidentu novēršanu, atklāšanu, apzināšanu, ierobežošanu, analīzi un reaģēšanu uz tiem, pasākumiem, kas veicina informētību par konkrētiem kiberdraudiem, informācijas apmaiņu ievainojamības izlabošanas un ievainojamības koordinētas izpaušanas kontekstā, brīvprātīgu informācijas apmaiņu par minētajiem incidentiem, kā arī kiberdraudiem un ievainojamībām, aizskāruma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem, varētu būt vajadzīga konkrētu kategoriju persondatu, piemēram, IP adrešu, vienoto resursu vietrāžu (*URL*), domēnu nosaukumu, e-pasta adrešu, un – ja tie atklāj persondatus – laika zīmogu, apstrāde. Persondatu apstrāde, ko veic kompetentās iestādes, vienotie kontaktpunkti un *CSIRT*, varētu būt juridisks pienākums vai varētu tikt uzskatīta par nepieciešamu, lai veiktu uzdevumu sabiedrības interesēs vai īstenotu oficiālās pilnvaras, kas pārzinim piešķirtas saskaņā ar Regulas (ES) 2016/679 6. panta 1. punkta c) vai e) apakšpunktu un 6. panta 3. punktu, vai lai īstenotu minētās regulas 6. panta 1. punkta f) apakšpunktā minēto būtisko un svarīgo vienību leģitīmās intereses. Turklāt valsts tiesību aktos varētu paredzēt noteikumus, kas ļauj kompetentajām iestādēm, vienotajiem kontaktpunktiem un *CSIRT*, ciktāl tas ir nepieciešams un samērīgi ar nolūku nodrošināt būtisko un svarīgo vienību tīklu un informācijas sistēmu drošību, apstrādāt īpašu kategoriju persondatus saskaņā ar Regulas (ES) 2016/679 9. pantu, jo īpaši paredzot piemērotus un konkrētus pasākumus, kā aizsargāt fizisko personu pamattiesības un intereses, tostarp tehniskus ierobežojumus šādu datu atkalizmantošanai un mūsdienīgu drošības un privātuma aizsardzības pasākumu, piemēram, pseidonimizācijas vai šifrēšanas, izmantošanu, ja anonimizācija var būtiski ietekmēt izvirzīto mērķi.

(122) Lai nostiprinātu uzraudzības pilnvaras un pasākumus, kas palīdz nodrošināt reālu atbilstību prasībām, šajā direktīvā būtu jāparedz minimāls to uzraudzības pasākumu un līdzekļu saraksts, ar kuriem kompetentās iestādes var uzraudzīt būtiskās un svarīgās vienības. Turklāt šajā direktīvā būtu jānosaka uzraudzības režīma nošķirums starp būtiskajām un svarīgajām vienībām, lai nodrošinātu taisnīgu pienākumu līdzsvaru minētajām vienībām un kompetentajām iestādēm. Tādēļ būtiskajām vienībām būtu jāpiemēro visaptverošs *ex ante* un *ex post* uzraudzības režīms, savukārt svarīgajām vienībām būtu jāpiemēro viegls un tikai *ex post* uzraudzības režīms. Tāpēc svarīgajām vienībām nebūtu jāpiemēro prasība sistemātiski dokumentēt atbilstību kiberdrošības risku pārvaldības pasākumiem, savukārt kompetentajām iestādēm būtu jāīsteno reaģējoša *ex post* pieeja uzraudzībai, tādēļ tām nevajadzētu būt vispārējam pienākumam uzraudzīt minētās vienības. Svarīgo vienību *ex post* uzraudzību var izraisīt pierādījumi, norādes vai informācija, kas darīta zināma kompetentajām iestādēm un ko šīs iestādes uzskata par tādu, kas liecina par šīs direktīvas iespējamiem pārkāpumiem. Piemēram, tie varētu būt tādi pierādījumi, norādes vai informācija, ko kompetentajām iestādēm sniedz citas iestādes, vienības, iedzīvotāji, mediji vai citi avoti, publiski pieejama informācija vai kas varētu izrietēt no citām darbībām, kuras kompetentās iestādes veic, pildot savus uzdevumus.

(123) Uzraudzības uzdevumu izpildei, ko veic kompetentās iestādes, nevajadzētu lieki kavēt attiecīgās vienības darbu. Ja kompetentās iestādes veic savus uzraudzības uzdevumus attiecībā uz būtiskām vienībām, tostarp veic inspekcijas uz vietas un uzraudzību neklātienē, izmeklē šīs direktīvas pārkāpumus un veic drošības revīzijas vai drošības skenēšanu, tām būtu līdz minimumam jāsamazina ietekme uz attiecīgās vienības darbu.

(124) Veicot *ex ante* uzraudzību, kompetentajām iestādēm būtu jāspēj lemt par prioritāšu noteikšanu attiecībā uz to rīcībā esošo uzraudzības pasākumu un līdzekļu samērīgu izmantošanu. Tas nozīmē, ka kompetentās iestādes var lemt par šādu prioritāšu noteikšanu, pamatojoties uz uzraudzības metodiku, kurā būtu jāievēro uz risku balstīta pieeja. Konkrētāk, šāda metodika varētu ietvert kritērijus vai etalonus būtisko vienību klasificēšanai riska kategorijās un attiecīgus uzraudzības pasākumus un līdzekļus, kas ieteicami katrai riska kategorijai, piemēram, inspekciju uz vietas, mērķorientētu drošības revīziju vai drošības skenēšanas izmantošanu, biežumu vai veidu, pieprasāmās informācijas veidu un minētās informācijas detalizācijas pakāpi. Šādu uzraudzības metodiku varētu papildināt arī ar darba

programmām un regulāri novērtēt un pārskatīt, arī attiecībā uz tādiem aspektiem kā resursu piešķiršana un vajadzības. Attiecībā uz valsts pārvaldes vienībām uzraudzības pilnvaras būtu jāīsteno atbilstoši valsts regulējumam un institucionālajai kārtībai.

(125) Kompetentajām iestādēm būtu jānodrošina, ka to uzraudzības uzdevumus attiecībā uz būtiskajām un svarīgajām vienībām veic apmācīti speciālisti, kuriem vajadzētu būt minēto uzdevumu veikšanai vajadzīgajām prasmēm, jo īpaši attiecībā uz inspekcijām uz vietas un uzraudzību neklātienē, arī attiecībā uz vājo vietu noteikšanu datubāzēs, aparatūrā, ugunsmūros, šifrēšanā un tīklos. Minētās inspekcijas un uzraudzība būtu jāveic objektīvi.

(126) Pienācīgi pamatotos gadījumos, kad kompetentajai iestādei ir zināms par būtiskiem kiberdraudiem vai nenovēršamu risku, tai būtu jāspēj pieņemt tūlītējus izpildes panākšanas lēmumus, lai novērstu incidentu vai reaģētu uz to.

(127) Lai izpildes panākšana būtu rezultatīva, būtu jānosaka minimāls to izpildes panākšanas pilnvaru saraksts, kuras var īstenot par šajā direktīvā paredzēto kiberdrošības risku pārvaldības pasākumu un ziņošanas pienākumu pārkāpumiem, izveidojot Savienībā skaidru un konsekventu satvaru šādai izpildes panākšanai. Būtu pienācīgi jāņem vērā šīs direktīvas pārkāpuma veids, smagums un ilgums, izraisītais materiālais vai nemateriālais kaitējums, tas, vai pārkāpums izdarīts tīši vai nolaidības dēļ, darbības, kas veiktas, lai novērstu vai mazinātu radīto materiālo vai nemateriālo kaitējumu, atbildības pakāpe vai jebkādi attiecīgi iepriekšēji pārkāpumi, sadarbības ar kompetento iestādi pakāpe un jebkādi citi vainu pastiprinoši vai mīkstinoši apstākļi. Izpildes panākšanas pasākumiem, arī administratīvajiem naudas sodiem, vajadzētu būt samērīgiem, un to piemērošanā būtu jāievēro attiecīgās procesuālās garantijas saskaņā ar vispārīgajiem Savienības tiesību principiem un Eiropas Savienības Pamattiesību hartu ("Harta"), tai skaitā tiesībām uz efektīvu tiesību aizsardzību tiesā, nevainīguma prezumpciju un tiesībām uz aizstāvību.

(128) Šī direktīva neprasa dalībvalstīm paredzēt krimināltiesisko atbildību vai civiltiesisko atbildību fiziskām personām, kuru pienākums ir nodrošināt vienības atbilstību šai direktīvai, par kaitējumu, ko šīs direktīvas pārkāpuma dēļ cietušas trešās puses.

(129) Lai nodrošinātu šajā direktīvā noteikto pienākumu rezultatīvas izpildes panākšanu, katrai kompetentajai iestādei vajadzētu būt pilnvarām uzlikt administratīvus naudas sodus vai pieprasīt to uzlikšanu.

(130) Ja administratīvs naudas sods tiek uzlikts būtiskai vai svarīgai vienībai, kas ir uzņēmums, minētajā nolūkā uzņēmums būtu jāsaprot kā uzņēmums saskaņā ar LESD 101. un 102. pantu. Ja administratīvs naudas sods tiek uzlikts personai, kas nav uzņēmums, kompetentajai iestādei, apsverot pienācīgo naudas soda lielumu, būtu jāņem vērā vispārējais ienākumu līmenis dalībvalstī, kā arī attiecīgās personas ekonomiskā situācija. Tas, vai un kādā apmērā administratīvi naudas sodi būtu piemērojami publiskām iestādēm, būtu jānosaka dalībvalstīm. Administratīva naudas soda uzlikšana neskar citu kompetento iestāžu pilnvaru piemērošanu vai citu tādu sodu piemērošanu, kas noteikti valsts tiesību normās, ar kurām transponēta šī direktīva.

(131) Dalībvalstīm būtu jāspēj pieņemt noteikumus par krimināl sodiem, ko piemēro, ja tiek pārkāptas valsts tiesību normas, ar kurām transponēta šī direktīva. Tomēr krimināl sodu piemērošanai par šādu valsts tiesību normu pārkāpumiem un saistītu administratīvu sodu piemērošanai nebūtu jāizraisa ne *bis in idem* principa pārkāpšana, kā to interpretējusi Eiropas Savienības Tiesa.

(132) Situācijām, attiecībā uz kurām šī direktīva administratīvos sodus nesaskaņo vai ja nepieciešams citos gadījumos, piemēram, šīs direktīvas smaga pārkāpuma gadījumā, dalībvalstīm būtu jāievieš sistēma, kas paredz iedarbīgus, samērīgus un atturošus sodus. Šādu sodu raksturs un tas, vai tie ir krimināli vai administratīvi, būtu jānosaka ar valsts tiesību aktiem.

(133) Lai vēl vairāk nostiprinātu par šīs direktīvas pārkāpumiem piemērojamo izpildes panākšanas pasākumu iedarbīgumu un atturošo ietekmi, kompetentajām iestādēm vajadzētu būt pilnvarotām piemērot vai lūgt piemērot sertifikācijas vai atļaujas darbības pagaidu apturēšanu attiecībā uz visiem vai daļu no attiecīgajiem būtiskas vienības sniegtajiem pakalpojumiem vai veiktajām darbībām un pieprasīt noteikt pagaidu aizliegumu jebkādai fiziskai personai pildīt vadības funkcijas izpilddirektora vai juridiskā pārstāvja līmenī. Ņemot vērā šādas pagaidu apturēšanas vai aizlieguma smagumu un ietekmi uz vienību darbībām un galu galā uz lietotājiem, tā būtu jāpiemēro tikai samērīgi ar pārkāpuma smagumu un ņemot vērā katra gadījuma īpašos apstākļus, arī to, vai pārkāpums izdarīts tīši vai nolaidības dēļ, un visas veiktās materiālā vai nemateriālā kaitējuma novēršanas vai mazināšanas darbības. Šāda pagaidu apturēšana vai aizliegums būtu jāpiemēro tikai kā galējs līdzeklis, proti, tikai pēc tam, kad visas citas attiecīgās izpildes panākšanas darbības, kas noteiktas šajā direktīvā, jau ir izsmeltas, un tikai līdz brīdim, kad attiecīgā vienība veic nepieciešamās darbības, lai novērstu trūkumus vai izpildītu kompetentās iestādes prasības, kā sakarā šāda pagaidu apturēšana vai aizliegums piemērots. Šādas pagaidu apturēšanas vai aizlieguma piemērošanā būtu jāievēro attiecīgās procesuālās garantijas saskaņā ar vispārīgajiem Savienības tiesību principiem un Hartu, tai skaitā tiesībām uz efektīvu tiesību aizsardzību un taisnīgu tiesu, nevainīguma prezumpciju un tiesībām uz aizstāvību.

(134) Lai nodrošinātu, ka vienības pilda savus šajā direktīvā noteiktos pienākumus saskaņā ar dalībvalstīm būtu savstarpēji jāsadarbojas un jāpalīdz attiecībā uz uzraudzības un izpildes panākšanas pasākumiem, jo īpaši, ja vienība sniedz pakalpojumus vairāk nekā vienā dalībvalstī vai ja tās tīklu un informācijas sistēmas atrodas dalībvalstī, kas nav tā dalībvalsts, kurā tā sniedz pakalpojumus. Sniedzot palīdzību, pieprasījuma saņēmējai kompetentajai iestādei būtu jāveic uzraudzības vai izpildes panākšanas pasākumi saskaņā ar valsts tiesību aktiem. Lai nodrošinātu šajā direktīvā paredzētās savstarpējās palīdzības raitu darbību, kompetentajām iestādēm sadarbības grupa būtu jāizmanto kā forums, kur apspriest lietas un konkrētus palīdzības pieprasījumus.

(135) Lai nodrošinātu rezultatīvu uzraudzību un izpildes panākšanu, jo īpaši situācijā ar pārrobežu dimensiju, dalībvalstij, kas ir saņēmusi savstarpējas palīdzības lūgumu, minētā lūguma robežās būtu jāveic piemēroti uzraudzības un izpildes panākšanas pasākumi attiecībā uz vienību, uz kuru attiecas minētais lūgums un kas minētās dalībvalsts teritorijā sniedz pakalpojumus vai kam tajā ir tīklu un informācijas sistēma.

(136) Šai direktīvai būtu jānosaka noteikumi par sadarbību starp kompetentajām iestādēm un uzraudzības iestādēm saskaņā ar Regulu (ES) 2016/679, lai vērstos pret šīs direktīvas pārkāpumiem, kas saistīti ar persondatiem.

(137) Šai direktīvai būtu jātiecas nodrošināt augstu atbildības līmeni attiecībā uz kiberdrošības riska pārvaldības pasākumiem un ziņošanas pienākumiem būtisko un svarīgo vienību līmenī. Tāpēc būtisko un svarīgo vienību pārvaldības struktūrām būtu jāapstiprina kiberdrošības risku pārvaldības pasākumi un jāuzrauga to īstenošana.

(138) Lai uz šīs direktīvas pamata Savienībā nodrošinātu vienādi augstu kiberdrošības līmeni, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu attiecībā uz šīs direktīvas papildināšanu, precizējot, kuru kategoriju būtiskajām un svarīgajām vienībām ir jāizmanto konkrēti sertificēti IKT produkti, IKT pakalpojumi un IKT procesi vai jāsaņem sertifikāts Eiropas kiberdrošības sertifikācijas shēmā. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu ([22]). Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu 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.

([22]) OV L 123, 12.5.2016., 1. lpp.

(139) Lai nodrošinātu vienādus nosacījumus šīs direktīvas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai noteikt procesuālo kārtību, kas nepieciešama sadarbības grupas darbībai, un tehniskās un metodiskās, kā arī nozaru prasības attiecībā uz kiberdrošības risku pārvaldības pasākumiem, un sīkāk precizēt informācijas veidu, incidentu, kiberdraudu un gandrīz notikušu incidentu paziņojumu un būtisku kiberdraudu paziņojumu formātu un procedūru, kā arī gadījumus, kad incidents uzskatāms par būtisku. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 ([23]).

(140) Komisijai pēc apspriešanās ar ieinteresētajām personām būtu periodiski jāpārskata šī direktīva, jo īpaši lai noteiktu, vai ir lietderīgi ierosināt grozījumus, ņemot vērā izmaiņas sabiedriskajos, politiskajos, tehnoloģiskajos vai tirgus apstākļos. Īstenojot pārskatīšanu, Komisijai būtu arī jānovērtē attiecīgo vienību lieluma un šīs direktīvas pielikumos minēto nozaru, apakšnozaru un vienību veidu relevance ekonomikas un sabiedrības darbībai kiberdrošības aspektā. Komisijai cita starpā būtu jānovērtē, vai nodrošinātājus, uz kuriem attiecas šīs direktīvas darbības joma un kas izraudzīti kā ļoti lielas tiešsaistes platformas Eiropas Parlamenta un Padomes Regulas (ES) 2022/2065 ([24]) 33. panta nozīmē, varētu identificēt kā būtiskas vienības saskaņā ar šo direktīvu.

(141) Ar šo direktīvu *ENISA* tiek noteikti jauni uzdevumi, tādējādi palielinot tās lomu, un tā rezultātā *ENISA* varētu arī nākties savus Regulā (ES) 2019/881 paredzētos pašreizējos uzdevumus veikt augstākā līmenī nekā iepriekš. Lai nodrošinātu, ka *ENISA* rīcībā ir nepieciešamie finanšu resursi un cilvēkresursi, kas vajadzīgi pastāvošo un jauno uzdevumu veikšanai, kā arī nolūkā minētos no tās lomas palielināšanas izrietošos uzdevumus pildīt augstākā līmenī, būtu attiecīgi jāpalielina tās budžets. Turklāt, lai nodrošinātu resursefektivitāti, *ENISA* būtu jāpiešķir lielāka elastība attiecībā uz to, kā tā var iekšēji sadalīt resursus, lai tā varētu rezultatīvi veikt savus uzdevumus un attaisnot cerības.

(142) Ņemot vērā to, ka šīs direktīvas mērķi, proti, panākt vienādi augstu kiberdrošības līmeni 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.

(143) Šajā direktīvā ir respektētas pamattiesības un ievēroti principi, kas atzīti Hartā, jo īpaši tiesības uz privātās dzīves un saziņas neaizskaramību, tiesības uz persondatu aizsardzību, uzņēmējdarbības brīvība, tiesības uz īpašumu, tiesības uz efektīvu tiesību aizsardzību tiesā un taisnīgu tiesu, nevainīguma prezumpcija un aizstāvības tiesības. Tiesības uz efektīvu tiesību aizsardzību attiecas arī uz būtisko un svarīgo vienību sniegto pakalpojumu saņēmējiem. Šī direktīva būtu jāīsteno saskaņā ar minētajām tiesībām un principiem.

(144) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([25]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2021. gada 11. martā sniedza atzinumu ([26]),

([23]) 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.).

([24]) Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) (OV L 277, 27.10.2022., 1. lpp.).

([25]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

([26]) OV C 183, 11.5.2021., 3. lpp.

IR PIEŅĒMUŠI ŠO DIREKTĪVU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets

1. Šī direktīva paredz pasākumus, kuru mērķis ir Savienībā panākt vienādi augstu kiberdrošības līmeni, lai uzlabotu iekšējā tirgus darbību.

2. Minētajā nolūkā šajā direktīvā ir noteikti:

a) pienākumi, kas dalībvalstīm prasa pieņemt valsts kiberdrošības stratēģijas un izraudzīties vai izveidot kompetentās iestādes, kiberkrīžu pārvaldības iestādes, vienotus kontaktpunktus kiberdrošības jautājumos (vienotie kontaktpunkti) un datordrošības incidentu reaģēšanas vienības (*CSIRT*);

b) kiberdrošības risku pārvaldības pasākumi un ziņošanas pienākumi vienību veidiem, kas minēti I vai II pielikumā, kā arī vienībām, kas identificētas kā kritiskās vienības saskaņā ar Direktīvu (ES) 2022/2557;

c) noteikumi un pienākumi attiecībā uz kiberdrošības informācijas kopīgošanu;

d) uzraudzības un izpildes panākšanas pienākumi dalībvalstīm.

2. pants

Darbības joma

1. Šo direktīvu piemēro to I vai II pielikumā minēto publisko vai privāto vienību veidiem, kas kvalificējas kā vidējie uzņēmumi saskaņā ar Ieteikuma 2003/361/EK pielikuma 2. pantu vai pārsniedz vidējiem uzņēmumiem noteiktos maksimālos lielumus, kuri paredzēti minētā panta 1. punktā, un kas sniedz pakalpojumus vai veic darbības Savienībā.

Minētā ieteikuma pielikuma 3. panta 4. punktu šīs direktīvas nolūkiem nepiemēro.

2. Šo direktīvu I vai II pielikumā minēto vienību veidiem neatkarīgi no to lieluma piemēro arī tad, ja:

a) pakalpojumus sniedz:

   i) publisko elektronisko sakaru tīklu nodrošinātāji vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji;

   ii) uzticamības pakalpojuma sniedzēji;

   iii) augstākā līmeņa domēnu nosaukumu reģistri un domēnu nosaukumu sistēmu pakalpojumu sniedzēji;

b) vienība ir dalībvalstī vienīgā tāda pakalpojuma sniedzēja, kas ir būtisks kritisku sabiedrisku vai ekonomisku darbību nodrošināšanai;

c) vienības sniegtā pakalpojuma traucējumam var būt būtiska ietekme uz sabiedrības aizsardzību, sabiedrisko drošību vai sabiedrības veselību;

d) vienības sniegtā pakalpojuma traucējums varētu izraisīt būtisku sistēmisku risku, jo īpaši nozarēm, kurās šādam traucējumam varētu būt pārrobežu ietekme;

e) vienība ir kritiska tāpēc, ka tā ir īpaši svarīga valsts vai reģionālā līmenī konkrētā veida nozarei vai pakalpojuma veidam vai citām savstarpēji atkarīgām nozarēm dalībvalstī;

f) vienība ir:

i) centrālās valdības valsts pārvaldes vienība, kā definējusi dalībvalsts saskaņā ar valsts tiesību aktiem; vai

ii) valsts pārvaldes vienība reģionālā līmenī, kā definējusi dalībvalsts saskaņā ar valsts tiesību aktiem, un tās sniegto pakalpojumu traucējumi, vadoties pēc uz risku balstīta novērtējuma, varētu būtiski ietekmēt kritiskas sabiedriskās vai ekonomiskās darbības.

3. Neatkarīgi no to lieluma, šo direktīvu piemēro vienībām, kas identificētas kā kritiskas vienības saskaņā ar Direktīvu (ES) 2022/2557.

4. Neatkarīgi no to lieluma, šo direktīvu piemēro vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus.

5. Dalībvalstis var paredzēt, ka šo direktīvu piemēro:

a) valsts pārvaldes vienībām vietējā līmenī;

b) izglītības iestādēm, jo īpaši, ja tās veic kritiskas pētniecības darbības.

6. Šī direktīva neskar dalībvalstu pienākumu sargāt valsts drošību un to pilnvaras aizsargāt citas valsts pamatfunkcijas, tostarp valsts teritoriālās integritātes nodrošināšanu un likumības un kārtības uzturēšanu.

7. Šo direktīvu nepiemēro valsts pārvaldes vienībām, kas veic darbības valsts drošības, sabiedriskās drošības, aizsardzības vai tiesībaizsardzības jomā, tostarp noziedzīgu nodarījumu novēršanā, izmeklēšanā, atklāšanā un kriminālvajāšanā par tiem.

8. Dalībvalstis var atbrīvot konkrētas vienības, kas veic darbības valsts drošības, sabiedriskās drošības, aizsardzības vai tiesībaizsardzības jomā, tostarp noziedzīgu nodarījumu novēršanā, izmeklēšanā, atklāšanā un kriminālvajāšanā par tiem, vai kas sniedz pakalpojumus tikai valsts pārvaldes vienībām, kuras minētas šā panta 7. punktā, attiecībā uz minētajām darbībām vai pakalpojumiem no 21. vai 23. pantā noteikto pienākumu izpildes. Šādos gadījumos minētajām konkrētajām darbībām vai pakalpojumiem nepiemēro VII nodaļā minētos uzraudzības un izpildes panākšanas pasākumus. Ja vienības veic tikai šajā punktā minētās darbības vai sniedz tikai šajā punktā minētos pakalpojumus, dalībvalstis var arī nolemt atbrīvot minētās vienības no 3. un 27. pantā noteiktajiem pienākumiem.

9. Šā panta 7. un 8. punktu nepiemēro, ja vienība darbojas kā uzticamības pakalpojumu sniedzējs.

10. Šo direktīvu nepiemēro vienībām, kuras dalībvalstis ir atbrīvojušas no Regulas (ES) 2022/2554 darbības jomas saskaņā ar minētās regulas 2. panta 4. punktu.

11. Šajā direktīvā noteiktie pienākumi neietver tādas informācijas sniegšanu, kuras izpaušana būtu pretrunā dalībvalstu būtiskajām valsts drošības, sabiedrības drošības vai aizsardzības interesēm.

12. Šo direktīvu piemēro, neskarot Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, Direktīvu 2002/58/EK, Eiropas Parlamenta un Padomes Direktīvas 2011/93/ES ([27]) un 2013/40/ES ([28]) un Direktīvu (ES) 2022/2557.

13. Neskarot LESD 346. pantu, informācijas, kas ir konfidenciāla saskaņā ar Savienības vai valstu tiesību normām, piemēram, normām par uzņēmējdarbības konfidencialitāti, apmaiņa ar Komisiju un citām attiecīgajām iestādēm saskaņā ar šo direktīvu notiek tikai tad, ja šāda apmaiņa ir nepieciešama šīs direktīvas piemērošanai. Ar informāciju apmainās tikai tiktāl, ciktāl tas ir atbilstīgi un samērīgi minētās apmaiņas nolūkam. Informācijas apmaiņā ievēro minētās informācijas konfidencialitāti un aizsargā attiecīgo vienību drošību un komerciālās intereses.

([27]) 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.).

([28]) 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.).

14. Vienības, kompetentās iestādes, vienotie kontaktpunkti un *CSIRT* apstrādā persondatus, ciktāl tas nepieciešams šīs direktīvas mērķiem un saskaņā ar Regulu (ES) 2016/679, un jo īpaši šāda apstrāde balstās uz minētās regulas 6. pantu.

Persondatu apstrādi, ievērojot šo direktīvu, publisko elektronisko sakaru tīklu nodrošinātāji vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji veic saskaņā ar Savienības datu aizsardzības tiesību aktiem un Savienības privātuma tiesību aktiem, jo īpaši Direktīvu 2002/58/EK.

3. pants

Būtiskas un svarīgas vienības

1. Šajā direktīvā par būtiskām vienībām uzskata šādas vienības:

a) I pielikumā minēto veidu vienības, kas pārsniedz Ieteikuma 2003/361/EK pielikuma 2. panta 1. punktā paredzēto maksimālo lielumu vidējiem uzņēmumiem;

b) kvalificētus uzticamības pakalpojumu sniedzējus un augstākā līmeņa domēnu nosaukumu reģistrus, kā arī DNS pakalpojuma sniedzējus neatkarīgi no to lieluma;

c) publisko elektronisko sakaru tīklu nodrošinātājus vai publiski pieejamu elektronisko sakaru pakalpojumu nodrošinātājus, kas kvalificējas kā vidējs uzņēmums saskaņā ar Ieteikuma 2003/361/EK pielikuma 2. pantu;

d) valsts pārvaldes vienības, kas minētas 2. panta 2. punkta f) apakšpunkta i) punktā;

e) jebkuras citas I vai II pielikumā minēto veidu vienības, ko dalībvalsts identificējusi kā būtiskas vienības, ievērojot 2. panta 2. punkta b)–e) apakšpunktu;

f) vienības, kas identificētas kā kritiskās vienības saskaņā ar Direktīvu (ES) 2022/2557, kā minēts šīs direktīvas 2. panta 3. punktā;

g) ja dalībvalsts tā paredzējusi, vienības, ko minētā dalībvalsts pirms 2023. gada 16. janvāra identificējusi par pamatpakalpojumu sniedzējām saskaņā ar Direktīvu (ES) 2016/1148 vai valsts tiesību aktiem.

2. Šajā direktīvā par svarīgām vienībām uzskata tās I vai II pielikumā minēto veidu vienības, kas nav kvalificējamas kā būtiskas vienības, ievērojot šā panta 1. punktu. Tās ir vienības, ko dalībvalsts identificējusi kā svarīgas vienības, ievērojot 2. panta 2. punkta b)–e) apakšpunktu.

3. Līdz 2025. gada 17. aprīlim dalībvalstis izveido sarakstu ar būtiskām un svarīgām vienībām, kā arī vienībām, kuras sniedz domēnu nosaukumu reģistrācijas pakalpojumus. Dalībvalstis minēto sarakstu regulāri un vismaz reizi divos gados pārskata un vajadzības gadījumā atjaunina.

4. Lai izveidotu 3. punktā minēto sarakstu, dalībvalstis pieprasa minētajā punktā norādītajām vienībām iesniegt kompetentajām iestādēm vismaz šādu informāciju:

a) vienības nosaukums;

b) adrese un jaunākā kontaktinformācija, tostarp e-pasta adreses, IP adrešu diapazoni un tālruņa numuri;

c) attiecīgā gadījumā attiecīgā nozare un apakšnozare, kas minēta I vai II pielikumā; un

d) attiecīgā gadījumā to dalībvalstu saraksts, kurās tās sniedz pakalpojumus, kas ietilpst šīs direktīvas darbības jomā.

Šā panta 3. punktā minētās vienības par visām izmaiņām saskaņā ar šā punkta pirmo daļu iesniegtajā informācijā informē bez kavēšanās un katrā ziņā divu nedēļu laikā pēc izmaiņu notikšanas.

Komisija ar Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) palīdzību bez nepamatotas kavēšanās sniedz pamatnostādnes un veidnes attiecībā uz pienākumiem, kas noteikti šajā punktā.

Dalībvalstis var izveidot valsts mehānismus, lai vienības varētu reģistrēties.

5. Līdz 2025. gada 17. aprīlim un pēc tam reizi divos gados kompetentās iestādes paziņo:

a) Komisijai un sadarbības grupai to būtisko un svarīgo vienību skaitu, kuras saskaņā ar 3. punktu iekļautas sarakstā katrā no I vai II pielikumā minētajām nozarēm un apakšnozarēm; un

b) Komisijai relevantu informāciju par to būtisko un svarīgo vienību skaitu, kas identificētas, ievērojot 2. panta 2. punkta b)–e) apakšpunktu, nozari un apakšnozari, kuras minētas I vai II pielikumā un kurās tās darbojas, vienību sniegto pakalpojumu veidu un to no 2. panta 2. punkta b)–e) apakšpunktā paredzētajiem noteikumiem, ievērojot ko tās identificētas.

6. Līdz 2025. gada 17. aprīlim un pēc Komisijas pieprasījuma dalībvalstis var paziņot Komisijai 5. punkta b) apakšpunktā minēto būtisko un svarīgo vienību nosaukumus.

4. pants

Nozarspecifiski Savienības tiesību akti

1. Ja nozarspecifiski Savienības tiesību akti prasa būtiskajām vai svarīgajām vienībām pieņemt kiberdrošības risku pārvaldības pasākumus vai ziņot par būtiskiem incidentiem un ja šādas prasības ietekmes ziņā ir vismaz līdzvērtīgas šajā direktīvā noteiktajiem pienākumiem, attiecīgos šīs direktīvas noteikumus, tostarp VII nodaļas noteikumus par uzraudzību un izpildes panākšanu, šādām vienībām nepiemēro. Ja nozarspecifiski Savienības tiesību akti neattiecas uz visām vienībām konkrētā nozarē, kas ietilpst šīs direktīvas darbības jomā, attiecīgos šīs direktīvas noteikumus turpina piemērot vienībām, uz kurām neattiecas minētie nozarspecifiskie Savienības tiesību akti.

2. Šā panta 1. punktā minētās prasības uzskata par ietekmes ziņā līdzvērtīgām šajā direktīvā noteiktajiem pienākumiem, ja:

a) kiberdrošības risku pārvaldības pasākumi ietekmes ziņā ir vismaz līdzvērtīgi 21. panta 1. un 2. punktā noteiktajiem pasākumiem; vai

b) nozarspecifiskais Savienības tiesību akts paredz *CSIRT* un šajā direktīvā paredzētajām kompetentajām iestādēm vai vienotajiem kontaktpunktiem tūlītēju un attiecīgā gadījumā automātisku un tiešu piekļuvi paziņojumiem par incidentiem un ja prasības paziņot par būtiskiem incidentiem ietekmes ziņā ir vismaz līdzvērtīgas šīs direktīvas 23. panta 1.–6. punktā noteiktajām prasībām.

3. Komisija 2023. gada 17. jūlijam sniedz pamatnostādnes, kurās tā precizē 1. un 2. punkta piemērošanu. Komisija minētās pamatnostādnes regulāri pārskata. Minēto pamatnostādņu sagatavošanā Komisija ņem vērā visus sadarbības grupas un *ENISA* apsvērumus.

5. pants

Minimālā saskaņošana

Šī direktīva neliedz dalībvalstīm ieviest vai saglabāt noteikumus, kas nodrošina augstāku kiberdrošības līmeni, ar noteikumu, ka šādi noteikumi ir saderīgi ar Savienības tiesību aktos noteiktajiem dalībvalstu pienākumiem.

6. pants

Definīcijas

Šajā direktīvā piemēro šādas definīcijas:

1) "tīklu un informācijas sistēma" ir:

   a) elektronisko sakaru tīkls, kā definēts Direktīvas (ES) 2018/1972 2. panta 1) punktā;

b) jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču grupa, no kurām viena vai vairākas ierīces atbilstoši programmai veic digitālu datu automātisku apstrādi; vai

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

2) "tīklu un informācijas sistēmu drošība" ir tīklu un informācijas sistēmu spēja noteiktā uzticamības līmenī pretoties visiem notikumiem, kas var apdraudēt glabāto, pārsūtīto vai apstrādāto datu pieejamību, autentiskumu, integritāti vai konfidencialitāti vai minēto tīklu un informācijas sistēmu piedāvātos vai ar to starpniecību pieejamos pakalpojumus;

3) "kiberdrošība" ir kiberdrošība, kā definēts Regulas (ES) 2019/881 2. panta 1) punktā;

4) "valsts kiberdrošības stratēģija" ir saskaņots dalībvalsts satvars, kas paredz stratēģiskus mērķus un prioritātes kiberdrošības jomā un pārvaldību to sasniegšanai attiecīgajā dalībvalstī;

5) "gandrīz noticis notikums" ir notikums, kas būtu varējis apdraudēt glabātu, pārsūtītu vai apstrādātu datu vai pakalpojumu, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību, pieejamību, autentiskumu, integritāti vai konfidencialitāti, bet kura pilnīga īstenošanās tika sekmīgi novērsta vai tas neīstenojās;

6) "incidents" ir notikums, kas apdraud glabātu, pārsūtītu vai apstrādātu datu vai pakalpojumu, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību, pieejamību, autentiskumu, integritāti vai konfidencialitāti;

7) "plašapmēra kiberdrošības incidents" ir incidents, kas izraisa traucējumu līmeni, kurš pārsniedz dalībvalsts spēju uz to reaģēt, vai kam ir būtiska ietekme uz vismaz divām dalībvalstīm;

8) "incidenta risināšana" ir visas darbības un procedūras, kuru mērķis ir novērst, atklāt, analizēt un ierobežot incidentu vai reaģēt uz to un atgūties no tā;

9) "risks" ir incidenta izraisītu zaudējumu vai traucējumu iespējamība, un to izsaka kā šādu zaudējumu vai traucējumu apjoma un minētā incidenta varbūtības apvienojumu;

10) "kiberdraudi" ir kiberdraudi, kā definēts Regulas (ES) 2019/881 2. panta 8) punktā;

11) "būtiski kiberdraudi" ir tādi kiberdraudi, kurus, ņemot vērā to tehniskās pamatīpašības, var uzskatīt par spējīgiem nopietni ietekmēt kādas vienības tīklu un informācijas sistēmas vai vienības pakalpojumu lietotājus, radot ievērojamu materiālu vai nemateriālu kaitējumu;

12) "IKT produkts" ir IKT produkts, kā definēts Regulas (ES) 2019/881 2. panta 12) punktā;

13) "IKT pakalpojums" ir IKT pakalpojums, kā definēts Regulas (ES) 2019/881 2. panta 13) punktā;

14) "IKT process" ir IKT process, kā definēts Regulas (ES) 2019/881 2. panta 14) punktā;

15) "ievainojamība" ir IKT produktu vai pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnība, ko var izmantot kiberdraudiem;

16) "standarts" ir standarts, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012 ([29]) 2. panta 1) punktā;

17) "tehniskā specifikācija" ir tehniska specifikācija, kā definēts Regulas (ES) Nr. 1025/2012 2. panta 4) punktā;

([29]) 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.).

18) "interneta plūsmu apmaiņas punkts" ir tīkla iekārta, kas ļauj nodrošināt vairāk nekā divu neatkarīgu tīklu (autonomu sistēmu) starpsavienojumu galvenokārt nolūkā atvieglot interneta datplūsmas apmaiņu, kas nodrošina starpsavienojumu tikai autonomām sistēmām un kas nepieprasa, lai interneta datplūsma starp jebkurām divām iesaistītām autonomām sistēmām izietu cauri jebkurai trešai autonomai sistēmai, ne maina vai citādi ietekmē šādu datplūsmu;

19) "domēnu nosaukumu sistēma" jeb "DNS" ir hierarhiska sadalīta nosaukumu sistēma, kas dod iespēju identificēt interneta pakalpojumus un resursus, ļaujot galalietotāju ierīcēm izmantot interneta maršrutēšanas un savienojumu pakalpojumus, lai piekļūtu šiem pakalpojumiem un resursiem;

20) "DNS pakalpojumu sniedzējs" ir vienība, kas sniedz:

a) publiski pieejamus rekursīvus domēnu nosaukumu atrises pakalpojumus interneta galalietotājiem; vai

b) autoritatīvus domēnu nosaukumu atrises pakalpojumus trešo personu lietošanai, izņemot saknes nosaukumu serverus;

21) "augstākā līmeņa domēnu nosaukumu reģistrs" jeb "ALD nosaukumu reģistrs" ir vienība, kam deleģēts īpašs ALD un kas atbild par ALD pārvaldību, to starpā domēnu nosaukumu reģistrāciju kā ALD un ALD tehnisko darbību, kā arī tā nosaukumu serveru darbību, datubāzu uzturēšanu un ALD zonas datņu sadalīšanu starp nosaukumu serveriem, neatkarīgi no tā, vai kādu no minētajām darbībām veic pati vienība vai ārpakalpojumu sniedzējs, bet izņemot situācijas, kad ALD nosaukumus reģistrs izmanto tikai savām vajadzībām;

22) "vienība, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus", ir reģistratūra vai aģents, kas darbojas reģistratūru vārdā, piemēram, privātuma vai pilnvarotās reģistrācijas pakalpojumu sniedzējs vai tālākpārdevējs;

23) "digitāls pakalpojums" ir pakalpojums, kā definēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/1535 ([30]) 1. panta 1. punkta b) apakšpunktā;

24) "uzticamības pakalpojums" ir uzticamības pakalpojums, kā definēts Regulas (ES) Nr. 910/2014 3. panta 16) punktā;

25) "uzticamības pakalpojumu sniedzējs" ir uzticamības pakalpojumu sniedzējs, kā definēts Regulas (ES) Nr. 910/2014 3. panta 19) punktā;

26) "kvalificēts uzticamības pakalpojums" ir kvalificēts uzticamības pakalpojums, kā definēts Regulas (ES) Nr. 910/2014 3. panta 17) punktā;

27) "kvalificēts uzticamības pakalpojumu sniedzējs" ir uzticamības pakalpojumu sniedzējs, kā definēts Regulas (ES) Nr. 910/2014 3. panta 20) punktā;

28) "tiešsaistes tirdzniecības vieta" ir tiešsaistes tirdzniecības vieta, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2005/29/EK ([31]) 2. panta n) punktā;

29) "tiešsaistes meklētājprogramma" ir tiešsaistes meklētājprogramma, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2019/1150 ([32]) 2. panta 5) punktā;

30) "mākoņdatošanas pakalpojums" ir digitāls pakalpojums, kas dod iespēju plaši un attālināti piekļūt kopīgojamu datošanas resursu mērogojamam un elastīgam pūlam un pēc pieprasījuma to pārvaldīt, tostarp, ja šādi resursi ir izvietoti vairākās vietās;

([30]) 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.).

([31]) 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.).

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

31) "datu centra pakalpojums" ir pakalpojums, kas ietver struktūras vai struktūru grupas, kuras paredzētas tāda IT 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;

32) "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;

33) "sociālās tīklošanās pakalpojumu platforma" ir platforma, kurā galalietotāji var pieslēgties, kopīgot saturu, atklāt informāciju un savstarpēji sazināties, izmantojot vairākas ierīces, jo īpaši tērzētavās, ar ziņām, video un ieteikumiem;

34) "pārstāvis" ir fiziska vai juridiska persona, kura ir iedibināta Savienībā un ir skaidri izraudzīta rīkoties, lai pārstāvētu DNS pakalpojumu sniedzēju, ALD nosaukumu reģistru, vienību, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, mākoņpakalpojumu sniedzēju, datu centra pakalpojumu sniedzēju, satura piegādes tīkla nodrošinātāju, pārvaldītu pakalpojumu sniedzēju, pārvaldītu drošības pakalpojumu sniedzēju vai tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas vai sociālās tīklošanās pakalpojumu platformas nodrošinātāju, kas nav iedibināts Savienībā, un pie kuras var vērsties kompetentā iestāde vai *CSIRT* pašas vienības vietā attiecībā uz minētās vienības pienākumiem atbilstoši šai direktīvai;

35) "valsts pārvaldes vienība" ir vienība, kas dalībvalstī par tādu ir atzīta saskaņā ar valsts tiesību aktiem, izņemot tiesu iestādes, parlamentus un centrālās bankas, un kas atbilst šādiem kritērijiem:

   a) tā ir izveidota ar mērķi apmierināt vispārējas vajadzības, un tā nav rūpnieciska vai komerciāla rakstura;

   b) tai ir juridiskas personas statuss vai ar likumu noteiktas tiesības rīkoties citas vienības, kurai ir juridiskas personas statuss, vārdā;

   c) to galvenokārt finansē valsts vai reģionālas iestādes vai citi publisko tiesību subjekti, 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, kuras attiecas uz personu pārrobežu pārvietošanos vai preču, pakalpojumu vai kapitāla pārrobežu apriti;

36) "publisks elektronisko sakaru tīkls" ir publisks elektronisko sakaru tīkls, kā definēts Direktīvas (ES) 2018/1972 2. panta 8) punktā;

37) "elektronisko sakaru pakalpojums" ir elektronisko sakaru pakalpojums, kā definēts Direktīvas (ES) 2018/1972 2. panta 4) punktā;

38) "vienība" ir fiziska vai juridiska persona, kas izveidota un atzīta kā tāda atbilstoši tās iedibinājuma vietas valsts tiesību aktiem un kas var savā vārdā īstenot tiesības un uzņemties pienākumus;

39) "pārvaldītu pakalpojumu sniedzējs" ir vienība, kas sniedz pakalpojumus, kuri saistīti ar IKT produktu, tīklu, infrastruktūras, lietojumprogrammu vai jebkādu citu tīklu un informācijas sistēmu uzstādīšanu, pārvaldību, darbību vai uzturēšanu un kuri izpaužas kā palīdzība vai aktīva administrēšana, ko veic vai nu klientu telpās, vai attālināti;

40) "pārvaldītu drošības pakalpojumu sniedzējs" ir pārvaldītu pakalpojumu sniedzējs, kas veic tādas darbības vai sniedz palīdzību tādām darbībām, kuras saistītas ar kiberdrošības risku pārvaldību;

41) "pētniecības organizācija" ir vienība, kuras galvenais mērķis ir veikt lietišķos pētījumus vai eksperimentālu izstrādi, lai pētījumu rezultātus izmantotu komerciālos nolūkos, bet kas neietver izglītības iestādes.

II NODAĻA

KOORDINĒTI KIBERDROŠĪBAS SATVARI

7. pants

Valsts kiberdrošības stratēģija

1. Katra dalībvalsts pieņem valsts kiberdrošības stratēģiju, kurā nosaka stratēģiskos mērķus, vajadzīgos resursus minēto mērķu sasniegšanai un atbilstīgus rīcībpolitikas un regulatīvus pasākumus, lai sasniegtu un uzturētu augstu kiberdrošības līmeni. Valsts kiberdrošības stratēģijā iekļauj:

a) dalībvalsts kiberdrošības stratēģijas mērķus un prioritātes, kas jo īpaši aptver I un II pielikumā minētās nozares;

b) pārvaldības satvaru šā punkta a) apakšpunktā minēto mērķu un prioritāšu sasniegšanai, tostarp rīcībpolitikas, kas minētas 2. punktā;

c) pārvaldības satvaru, kurā precizēti attiecīgo ieinteresēto personu lomas un pienākumi valsts līmenī, kas ir pamatā sadarbībai un koordinācijai valsts līmenī starp šajā direktīvā minētajām kompetentajām iestādēm, vienotajiem kontaktpunktiem un *CSIRT*, kā arī koordinācijai un sadarbībai starp minētajām struktūrām un kompetentajām iestādēm, kas minētas nozarspecifiskos Savienības tiesību aktos;

d) mehānismu attiecīgo aktīvu identificēšanai un risku novērtējumu konkrētajā dalībvalstī;

e) to pasākumu identifikāciju, kas nodrošina sagatavotību, reaģēšanu un atkopšanos pēc incidentiem, tostarp sadarbību starp publisko un privāto sektoru;

f) valsts kiberdrošības stratēģijas īstenošanā iesaistīto dažādo iestāžu un ieinteresēto personu sarakstu;

g) rīcībpolitikas satvaru pastiprinātai koordinācijai starp kompetentajām iestādēm, kas minētas šajā direktīvā, un kompetentajām iestādēm, kas paredzētas Direktīvā (ES) 2022/2557, tādas informācijas kopīgošanas kontekstā, kura attiecas uz riskiem, kiberdraudiem un incidentiem, kā arī attiecīgā gadījumā ar kiberdrošību nesaistītiem riskiem, draudiem un incidentiem un uzraudzības uzdevumu veikšanu;

h) plānu, tostarp vajadzīgos pasākumus, iedzīvotāju informētības par kiberdrošību vispārējā līmeņa uzlabošanai.

2. Kā valsts kiberdrošības stratēģijas daļu dalībvalstis jo īpaši pieņem rīcībpolitikas:

a) kas vērstas uz kiberdrošību piegādes ķēdē attiecībā uz IKT produktiem un IKT pakalpojumiem, kurus vienības izmanto pakalpojumu sniegšanai;

b) par to, kā publiskajā iepirkumā iekļaut un noteikt ar kiberdrošību saistītas prasības IKT produktiem un IKT pakalpojumiem, tostarp saistībā ar kiberdrošības sertifikāciju, šifrēšanu un atvērtā pirmkoda kiberdrošības produktu izmantošanu;

c) par ievainojamības pārvaldību, ietverot koordinētas ievainojamības izpaušanas veicināšanu un atvieglošanu saskaņā ar 12. panta 1. punktu;

d) saistībā ar atvērtā interneta publiskā kodola vispārējās pieejamības, integritātes un konfidencialitātes uzturēšanu, tostarp attiecīgā gadījumā zemūdens sakaru kabeļu kiberdrošību;

e) kas veicina tādu attiecīgu progresīvu tehnoloģiju izstrādi un integrāciju, kuru mērķis ir īstenot modernus kiberdrošības risku pārvaldības pasākumus;

f) kas veicina un attīsta iedzīvotājiem, ieinteresētajām personām un vienībām paredzētu izglītību un apmācību kiberdrošības, kiberdrošības prasmju, izpratnes veicināšanas un pētniecības un izstrādes iniciatīvu jomā, kā arī norādījumus par labu kiberhigiēnas praksi un kontroli;

g) kas atbalsta akadēmiskās un pētniecības iestādes kiberdrošības rīku un drošas tīklu infrastruktūras attīstīšanā, uzlabošanā un ieviešanas veicināšanā;

h) kas ietver attiecīgas procedūras un atbilstīgus informācijas kopīgošanas rīkus, ar kuriem atbalsta brīvprātīgu kiberdrošības informācijas kopīgošanu starp vienībām saskaņā ar Savienības tiesību aktiem;

i) kas stiprina mazo un vidējo uzņēmumu kibernoturību un kiberhigiēnas pamatlīmeni, jo īpaši tiem, kas ir izslēgti no šīs direktīvas darbības jomas, sniedzot viegli pieejamus norādījumus un palīdzību to īpašajām vajadzībām;

j) kas veicina aktīvu kiberaizsardzību.

3. Dalībvalstis savas kiberdrošības stratēģijas paziņo Komisijai trīs mēnešu laikā pēc to pieņemšanas. Dalībvalstis no šādiem paziņojumiem var izslēgt informāciju, kas attiecas uz to valsts drošību.

4. Dalībvalstis regulāri un vismaz reizi piecos gados novērtē savas kiberdrošības stratēģijas, pamatojoties uz galvenajiem snieguma rādītājiem, un nepieciešamības gadījumā tās atjaunina. *ENISA* pēc dalībvalstu pieprasījuma palīdz tām izstrādāt vai atjaunināt valsts kiberdrošības stratēģiju un galvenos snieguma rādītājus minētās stratēģijas novērtēšanai, lai to saskaņotu ar šajā direktīvā noteiktajām prasībām un pienākumiem.

8. pants

Kompetentās iestādes un vienotie kontaktpunkti

1. Katra dalībvalsts izraugās vai izveido vienu vai vairākas kompetentās iestādes, kas atbild par kiberdrošību un par uzraudzības uzdevumiem, kuri minēti VII nodaļā (kompetentās iestādes).

2. Kompetentās iestādes, kas minētas 1. punktā, uzrauga šīs direktīvas īstenošanu valsts līmenī.

3. Katra dalībvalsts izraugās vai izveido vienoto kontaktpunktu. Ja dalībvalsts, ievērojot 1. punktu, izraugās vai izveido 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 citu dalībvalstu iestādēm un attiecīgā gadījumā ar Komisiju un *ENISA*, kā arī lai nodrošinātu starpnozaru sadarbību ar citām kompetentajām iestādēm savā dalībvalstī.

5. Dalībvalstis nodrošina, ka to kompetentajām iestādēm un vienotajiem kontaktpunktiem ir adekvāti resursi, lai efektīvi un rezultatīvi veiktu tiem uzticētos uzdevumus un tādējādi sasniegtu šīs direktīvas mērķus.

6. Katra dalībvalsts bez nepamatotas kavēšanās paziņo Komisijai 1. punktā minētās kompetentās iestādes un 3. punktā minētā vienotā kontaktpunkta identitāti, minēto iestāžu uzdevumus un visas turpmākās ar tām saistītās izmaiņas. Katra dalībvalsts publisko tās kompetentās iestādes identitāti. Komisija vienoto kontaktpunktu sarakstu dara publiski pieejamu.

9. pants

Valstu kiberkrīžu pārvaldības satvari

1. Katra dalībvalsts izraugās vai izveido vienu vai vairākas kompetentās iestādes, kas atbild par plašapmēra kiberdrošības incidentu un krīžu pārvaldību (kiberkrīžu pārvaldības iestādes). Dalībvalstis nodrošina, ka šīm iestādēm ir pietiekami resursi, lai rezultatīvi un efektīvi veiktu tām uzticētos uzdevumus. Dalībvalstis nodrošina saskaņotību ar esošajiem vispārējas valsts krīžu pārvaldības satvariem.

2. Ja dalībvalsts saskaņā ar 1. punktu izraugās vai izveido vairāk nekā vienu kiberkrīžu pārvaldības iestādi, tā skaidri norāda, kura no minētajām iestādēm darbojas kā koordinatore plašapmēra kiberdrošības incidentu un krīžu pārvaldībā.

3. Katra dalībvalsts nosaka spējas, aktīvus un procedūras, ko var izmantot krīzes gadījumā šīs direktīvas nolūkos.

4. Katra dalībvalsts pieņem valsts plānu reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm, kurā izklāsta plašapmēra kiberdrošības incidentu un krīžu pārvaldības mērķus un kārtību. Minētajā plānā jo īpaši nosaka:

a) valsts sagatavotības pasākumu un darbību mērķus;

b) kiberkrīžu pārvaldības iestāžu uzdevumus un pienākumus;

c) kiberkrīžu pārvaldības procedūras, tostarp to integrēšanu vispārējā valsts krīžu pārvaldības satvarā, un informācijas apmaiņas kanālus;

d) valsts sagatavotības pasākumus, tostarp mācības un apmācību;

e) attiecīgās iesaistītās publiskā un privātā sektora ieinteresētās personas un infrastruktūru;

f) tādas valsts procedūras un vienošanās starp attiecīgajām valsts iestādēm un struktūrām, kuru mērķis ir nodrošināt dalībvalstu efektīvu dalību un atbalstu koordinētā plašapmēra kiberdrošības incidentu un krīžu pārvaldībā Savienības līmenī.

5. Trīs mēnešu laikā pēc tam, kad 1. punktā minētā kiberkrīžu pārvaldības iestāde ir izraudzīta vai izveidota, katra dalībvalsts paziņo Komisijai savas iestādes identitāti un visas turpmākās izmaiņas tajā. Dalībvalstis trīs mēnešu laikā pēc minēto plānu pieņemšanas iesniedz Komisijai un Eiropas Kiberkrīžu koordinācijas organizāciju tīklam (*EU-CyCLONe*) relevantu informāciju saistībā ar 4. punkta prasībām par saviem valsts plāniem reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm. Dalībvalstis var neiekļaut informāciju, ja un ciktāl šāda neiekļaušana ir nepieciešama valsts drošībai.

10. pants

Datordrošības incidentu reaģēšanas vienības (*CSIRT*)

1. Katra dalībvalsts izraugās vai izveido vienu vai vairākas *CSIRT*. *CSIRT* var izraudzīties vai izveidot kādas kompetentās iestādes ietvaros. *CSIRT* atbilst 11. panta 1. punktā noteiktajām prasībām, to darbība attiecas vismaz uz I un II pielikumā minētajām nozarēm, apakšnozarēm vai vienību veidiem, un tās ir atbildīgas par incidentu risināšanu saskaņā ar labi definētu procesu.

2. Dalībvalstis nodrošina, ka katrai *CSIRT* ir pietiekami resursi, lai tā rezultatīvi pildītu savus uzdevumus, kā izklāstīts 11. panta 3. punktā.

3. Dalībvalstis nodrošina, ka katras *CSIRT* rīcībā ir piemērota, droša un noturīga sakaru un informācijas infrastruktūra, izmantojot kuru veikt informācijas apmaiņu ar būtiskajām un svarīgajām vienībām un citām attiecīgajām ieinteresētajām personām. Šajā nolūkā dalībvalstis nodrošina, ka katra *CSIRT* sniedz ieguldījumu drošu informācijas kopīgošanas rīku izmantošanā.

4. *CSIRT* sadarbojas un attiecīgā gadījumā saskaņā ar 29. pantu apmainās ar relevantu informāciju ar būtisko un svarīgo vienību nozaru un starpnozaru kopienām.

5. *CSIRT* piedalās salīdzinošajā izvērtēšanā, ko organizē saskaņā ar 19. pantu.

6. Dalībvalstis nodrošina savu *CSIRT* rezultatīvu, efektīvu un drošu sadarbību *CSIRT* tīklā.

7. *CSIRT* var izveidot sadarbības attiecības ar trešo valstu datordrošības incidentu reaģēšanas vienībām. Šādās sadarbības attiecībās dalībvalstis veicina rezultatīvu, efektīvu un drošu informācijas apmaiņu ar minētajām trešo valstu datordrošības incidentu reaģēšanas vienībām, izmantojot relevantas informācijas kopīgošanas protokolus, tostarp gaismas signālu protokolu. *CSIRT* var apmainīties ar relevantu informāciju ar trešo valstu datordrošības incidentu reaģēšanas vienībām, tostarp ar persondatiem saskaņā ar Savienības datu aizsardzības tiesību aktiem.

8. *CSIRT* var sadarboties ar trešo valstu datordrošības incidentu reaģēšanas vienībām vai līdzvērtīgām trešo valstu struktūrām, jo īpaši, lai tām sniegtu palīdzību kiberdrošības jomā.

9. Katra dalībvalsts bez nepamatotas kavēšanās paziņo Komisijai šā panta 1. punktā minētās *CSIRT* un saskaņā ar 12. panta 1. punktu par koordinatori ieceltās *CSIRT* identitāti, to attiecīgos uzdevumus saistībā ar būtiskām un svarīgām vienībām un visas turpmākās ar tām saistītās izmaiņas.

10. Dalībvalstis var lūgt *ENISA* palīdzību savu *CSIRT* izveidē.

11. pants

Prasības *CSIRT*, to tehniskās spējas un uzdevumi

1. *CSIRT* atbilst šādām prasībām:

a) *CSIRT* nodrošina savu sakaru kanālu augstu pieejamības līmeni, izvairoties no vienotiem atteices punktiem, un tai ir vairāki saziņas līdzekļi, kas jebkurā laikā ļauj ar to sazināties un nodrošina saziņu ar citiem; tās skaidri nosaka saziņas kanālus un dara tos zināmus tiem, kam tās sniedz pakalpojumus, un sadarbības partneriem;

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

c) *CSIRT* ir aprīkotas ar piemērotu sistēmu pieprasījumu pārvaldībai un novirzīšanai, jo īpaši lai atvieglotu efektīvu un lietpratīgu nodošanu;

d) *CSIRT* nodrošina savu darbību konfidencialitāti un uzticamību;

e) *CSIRT* ir pietiekams darbinieku skaits, lai nodrošinātu to pakalpojumu pieejamību jebkurā brīdī, un tās nodrošina, ka to personāls ir pienācīgi apmācīts;

f) *CSIRT* ir nodrošinātas ar rezerves sistēmām un dublēšanas darba telpu, lai nodrošinātu to pakalpojumu nepārtrauktību.

CSIRT var piedalīties starptautiskos sadarbības tīklos.

2. Dalībvalstis nodrošina, ka to *CSIRT* kopīgi ir pietiekamas tehniskās spējas, kas vajadzīgas, lai pildītu 3. punktā minētos uzdevumus. Dalībvalstis nodrošina, ka to *CSIRT* tiek piešķirti pietiekami resursi, lai nodarbinātu pietiekamu skaitu darbinieku, kas *CSIRT* ļautu attīstīt to tehniskās spējas.

3. *CSIRT* ir šādi uzdevumi:

a) kiberdraudu, ievainojamības un incidentu uzraudzība un analīze valsts līmenī un pēc pieprasījuma palīdzības sniegšana attiecīgajām būtiskajām un svarīgajām vienībām saistībā ar to tīklu un informācijas sistēmu uzraudzību reāllaikā vai tuvu reāllaikam;

b) agrīnu brīdinājumu, trauksmju, paziņojumu sniegšana un informācijas izplatīšana attiecīgajām būtiskajām un svarīgajām vienībām, kā arī kompetentajām iestādēm un citām attiecīgām ieinteresētajām personām par kiberdraudiem, ievainojamību un incidentiem, ja iespējams – gandrīz reāllaikā;

c) vajadzības gadījumā reaģēšana uz incidentiem un palīdzības sniegšana attiecīgajām būtiskajām un svarīgajām vienībām;

d) kriminālistikas datu vākšana un analīze un dinamiskas risku un incidentu analīzes un situācijas apzināšanas nodrošināšana attiecībā uz kiberdrošību;

e) pēc būtiskās vai svarīgās vienības pieprasījuma attiecīgās vienības tīklu un informācijas sistēmu proaktīva skenēšana, lai atklātu ievainojamības ar iespējamu būtisku ietekmi;

f) piedalīšanās *CSIRT* tīklā un savstarpējas palīdzības sniegšana atbilstīgi to spējām un kompetencei citiem *CSIRT* tīkla dalībniekiem pēc to lūguma;

g) attiecīgā gadījumā darbošanās kā koordinatorēm koordinētās ievainojamības izpaušanas saskaņā ar 12. panta 1. punktu vajadzībām;

h) līdzdalība drošu informācijas kopīgošanas rīku ieviešanā saskaņā ar 10. panta 3. punktu.

CSIRT var veikt būtisku un svarīgu vienību publiski pieejamu tīklu un informācijas sistēmu proaktīvu neintruzīvu skenēšanu. Skenēšanu veic, lai atklātu ievainojamas vai nedroši konfigurētas tīklu un informācijas sistēmas un informētu attiecīgās vienības. Šādai skenēšanai nav negatīvas ietekmes uz vienību pakalpojumu darbību.

Veicot pirmajā daļā minētos uzdevumus, *CSIRT* var piešķirt prioritāti konkrētiem uzdevumiem, izmantojot uz risku balstītu pieeju.

4. *CSIRT* nodibina sadarbības attiecības ar attiecīgajām ieinteresētajām personām privātajā sektorā, lai labāk sasniegtu šīs direktīvas mērķus.

5. Lai veicinātu 4. punktā minēto sadarbību, *CSIRT* veicina vienotas vai standartizētas prakses, klasifikācijas shēmu un taksonomiju pieņemšanu un izmantošanu attiecībā uz:

a) incidentu risināšanas procedūrām;

b) krīžu pārvaldību; un

c) koordinētu ievainojamības izpaušanu saskaņā ar 12. panta 1. punktu.

12. pants

Koordinēta ievainojamības izpaušana un Eiropas ievainojamību datubāze

1. Katra dalībvalsts izraugās vienu no savām *CSIRT* par koordinatori koordinētas ievainojamības izpaušanas vajadzībām. Par koordinatori izraudzītā *CSIRT* rīkojas kā uzticams starpnieks, nepieciešamības gadījumā pēc kādas no pusēm pieprasījuma veicinot mijiedarbību starp fizisko vai juridisko personu, kas ziņo par ievainojamību, un potenciāli ievainojamu IKT produktu ražotāju vai potenciāli ievainojamu IKT pakalpojumu sniedzēju. *CSIRT*, kas izraudzīta par koordinatori, uzdevumi ietver:

a) attiecīgo vienību identificēšanu un sazināšanos ar tām;

b) palīdzību fiziskām vai juridiskām personām, kas ziņo par ievainojamību; un

c) sarunas par informācijas izpaušanas termiņiem un tādu ievainojamību pārvaldību, kuras ietekmē vairākas vienības.

Dalībvalstis nodrošina, ka fiziskas vai juridiskas personas, ja tās to pieprasa, var anonīmi ziņot par ievainojamību *CSIRT*, kas izraudzīta par koordinatori. *CSIRT*, kas izraudzīta par koordinatori, nodrošina, ka tiek veikta rūpīga pēckontrole attiecībā uz paziņoto ievainojamību, un nodrošina par ievainojamību ziņojušās fiziskās vai juridiskās personas anonimitāti. Ja paziņotā ievainojamība varētu būtiski ietekmēt vienības vairāk nekā vienā dalībvalstī, katras attiecīgās dalībvalsts *CSIRT*, kas izraudzīta par koordinatori, attiecīgos gadījumos sadarbojas *CSIRT* tīklā ar citām *CSIRT*, kas izraudzītas par koordinatorēm.

2. *ENISA* pēc apspriešanās ar sadarbības grupu izstrādā un uztur Eiropas ievainojamību datubāzi. Šajā nolūkā *ENISA* izveido un uztur atbilstīgas informācijas sistēmas, rīcībpolitikas un procedūras un pieņem nepieciešamos tehniskos un organizatoriskos pasākumus Eiropas ievainojamību datubāzes drošības un integritātes nodrošināšanai, jo īpaši lai vienības, neatkarīgi no tā, vai tās ietilpst šīs direktīvas darbības jomā, un to tīklu un informācijas sistēmu piegādātāji varētu brīvprātīgi izpaust un reģistrēt publiski zināmas ievainojamības IKT produktos vai IKT pakalpojumos. Visām ieinteresētajām personām nodrošina piekļuvi Eiropas ievainojamību datubāzē ietvertajai informācijai par ievainojamībām. Minētajā datubāzē iekļauj:

a) informāciju, kas raksturo ievainojamību;

b) ietekmētos IKT produktus vai IKT pakalpojumus un ievainojamības smagumu, raksturojot apstākļus, kādos to var izmantot;

c) informāciju par attiecīgo ielāpu pieejamību un, ja nav pieejamu ielāpu, ievainojamu IKT produktu un IKT pakalpojumu lietotājiem adresētus un kompetento iestāžu vai *CSIRT* sniegtus norādījumus par to, kā var mazināt no izpaustās ievainojamības izrietošos riskus.

13. pants

Sadarbība valsts līmenī

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

2. Dalībvalstis nodrošina, ka *CSIRT* vai attiecīgā gadījumā to kompetentās iestādes saņem paziņojumus par būtiskiem incidentiem saskaņā ar 23. pantu un incidentiem, kiberdraudiem un gandrīz notikušiem notikumiem saskaņā ar 30. pantu.

3. Dalībvalstis nodrošina, ka *CSIRT* vai attiecīgā gadījumā to kompetentās iestādes informē to vienotos kontaktpunktus par paziņojumiem, kas attiecas uz incidentiem, kiberdraudiem un gandrīz notikušiem notikumiem un kas sniegti atbilstoši šai direktīvai.

4. Lai nodrošinātu, ka kompetento iestāžu, vienoto kontaktpunktu un *CSIRT* uzdevumi un pienākumi tiek veikti efektīvi, dalībvalstis pēc iespējas nodrošina pienācīgu sadarbību starp minētajām struktūrām un tiesībaizsardzības iestādēm, datu aizsardzības iestādēm, valstu iestādēm, kas minētas Regulā (EK) Nr. 300/2008 un (ES) 2018/1139, uzraudzības struktūrām, kas minētas Regulā (ES) Nr. 910/2014, kompetentajām iestādēm, kas minētas Regulā (ES) 2022/2554, valsts regulatīvajām iestādēm, kas minētas Direktīvā (ES) 2018/1972, kompetentajām iestādēm, kas minētas Direktīvā (ES) 2022/2557, kā arī kompetentajām iestādēm, kas minētas citos Savienības nozarspecifiskos tiesību aktos, attiecīgajā dalībvalstī.

5. Dalībvalstis nodrošina, ka to kompetentās iestādes, kas minētas šajā direktīvā, un to kompetentās iestādes, kas minētas Direktīvā (ES) 2022/2557, regulāri sadarbojas un apmainās ar informāciju attiecībā uz kritisko vienību identificēšanu, par riskiem, kiberdraudiem un incidentiem, kā arī par riskiem, kuri nav saistīti ar kiberdrošību, draudiem un incidentiem, kas skar būtiskās vienības, kuras identificētas kā kritiskās vienības Direktīvā (ES) 2022/2557., un par pasākumiem, kas veikti, reaģējot uz šādiem riskiem, draudiem un incidentiem. Dalībvalstis arī nodrošina, ka to kompetentās iestādes, kas minētas šajā direktīvā, un to kompetentās iestādes, kas minētas Regulā (ES) Nr. 910/2014, Regulā (ES) 2022/2554 un Direktīvā (ES) 2018/1972, regulāri apmainās ar relevantu informāciju, tostarp par attiecīgajiem incidentiem un kiberdraudiem.

6. Dalībvalstis vienkāršo ziņošanu, izmantojot tehniskos līdzekļus 23. un 30. pantā minētajiem paziņojumiem.

III NODAĻA

SADARBĪBA SAVIENĪBAS UN STARPTAUTISKĀ LĪMENĪ

14. pants

Sadarbības grupa

1. Lai atbalstītu un veicinātu stratēģisku sadarbību un informācijas apmaiņu starp dalībvalstīm, kā arī lai stiprinātu uzticēšanos un paļāvību, izveido sadarbības grupu.

2. Sadarbības grupa veic savus uzdevumus, pamatojoties uz divgadu darba programmām, kas minētas 7. punktā.

3. Sadarbības grupas sastāvā ir pārstāvji no dalībvalstīm, Komisijas un *ENISA*. Sadarbības grupas darbībās kā novērotājs piedalās Eiropas Ārējās darbības dienests. Eiropas uzraudzības iestādes (EUI) un kompetentās iestādes, kas minētas Regulā (ES) 2022/2554, var piedalīties sadarbības grupas darbībās saskaņā ar minētās regulas 47. panta 1. punktu.

Attiecīgā gadījumā sadarbības grupa var uzaicināt tās darbā piedalīties Eiropas Parlamentu un 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) dot norādījumus kompetentajām iestādēm par rīcībpolitiku izstrādi un īstenošanu attiecībā uz koordinētu ievainojamības izpaušanu, kā minēts 7. panta 2. punkta c) apakšpunktā;

c) apmainīties ar paraugpraksi un informāciju saistībā ar šīs direktīvas īstenošanu, arī par kiberdraudiem, incidentiem, ievainojamībām, gandrīz notikušiem notikumiem, izpratnes veicināšanas iniciatīvām, apmācību, mācībām un prasmēm, spēju veidošanu, standartiem un tehniskajām specifikācijām, kā arī būtisku un svarīgu vienību identificēšanu, ievērojot 2. panta 2. punkta b)–e) apakšpunktu;

d) apmainīties ar padomiem un sadarboties ar Komisiju jaunu kiberdrošības rīcībpolitikas iniciatīvu jomā un attiecībā uz vispārējo nozarspecifisko kiberdrošības prasību konsekvenci;

e) apmainīties ar padomiem un sadarboties ar Komisiju saistībā ar deleģēto vai īstenošanas aktu projektiem, ko pieņem, ievērojot šo direktīvu;

f) apmainīties ar paraugpraksi un informāciju ar attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām;

g) apmainīties viedokļiem par tādu nozarspecifisku Savienības tiesību aktu īstenošanu, kuros ietverti noteikumi par kiberdrošību;

h) attiecīgā gadījumā apspriest ziņojumus par salīdzinošo izvērtēšanu, kas minēti 19. panta 9. punktā, un sagatavot secinājumus un ieteikumus;

i) veikt kritisko piegādes ķēžu koordinētus drošības riska novērtējumus saskaņā ar 22. panta 1. punktu;

j) apspriest savstarpējas palīdzības gadījumus, tostarp pieredzi un rezultātus, kas gūti kopīgās pārrobežu uzraudzības darbībās, kā minēts 37. pantā;

k) pēc vienas vai vairāku attiecīgo dalībvalstu lūguma apspriest konkrētus savstarpējas palīdzības pieprasījumus, kā minēts 37. pantā;

l) dot stratēģiskus norādījumus *CSIRT* tīklam un *EU-CyCLONe* par konkrētām jaunām problēmām;

m) apmainīties viedokļiem par rīcībpolitiku attiecībā uz turpmākiem pasākumiem pēc plašapmēra kiberdrošības incidentiem un krīzēm, pamatojoties uz *CSIRT* tīkla un *EU-CyCLONe* gūto pieredzi;

n) sniegt ieguldījumu kiberdrošības spējās visā Savienībā, veicinot valsts amatpersonu apmaiņu ar spēju veidošanas programmu, kurā iesaista darbiniekus no kompetentajām iestādēm vai *CSIRT*;

o) organizēt regulāras kopīgas sanāksmes ar attiecīgajām privātā sektora ieinteresētajām personām no visas Savienības, lai apspriestu sadarbības grupas veiktās darbības un apkopotu informāciju par jaunām rīcībpolitikas problēmām;

p) apspriest darbu, kas veikts saistībā ar kiberdrošības mācībām, tostarp *ENISA* veikto darbu;

q) izstrādāt 19. panta 1. punktā minētās salīdzinošās izvērtēšanas metodiku un organizatoriskos aspektus, kā arī ar Komisijas un *ENISA* palīdzību saskaņā ar 19. panta 5. punktu izstrādāt dalībvalstīm pašnovērtējuma metodiku un sadarbībā ar Komisiju un *ENISA* saskaņā ar 19. panta 6. punktu izstrādāt rīcības kodeksus, kas ir pamatā norīkoto kiberdrošības ekspertu darba metodēm;

r) sagatavot ziņojumus par stratēģiskā līmenī un no salīdzinošās izvērtēšanas gūto pieredzi 40. pantā minētās pārskatīšanas nolūkā;

s) apspriest un regulāri novērtēt pašreizējo stāvokli kiberdraudu vai incidentu, piemēram, izspiedējprogrammatūras, jomā.

Sadarbības grupa pirmās daļas r) apakšpunktā minētos ziņojumus iesniedz Komisijai, Eiropas Parlamentam un Padomei.

5. Dalībvalstis nodrošina to pārstāvju efektīvu, rezultatīvu un drošu sadarbību sadarbības grupā.

6. Sadarbības grupa var pieprasīt no *CSIRT* tīkla tehnisku ziņojumu par izraudzītiem tematiem.

7. Līdz 2024. gada 1. februārim un pēc tam reizi divos gados sadarbības grupa izstrādā darba programmu par pasākumiem, kas jāveic, lai sasniegtu tās mērķus un izpildītu uzdevumus.

8. 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 39. panta 2. punktā.

Komisija saskaņā ar 4. punkta e) apakšpunktu apmainās ar padomiem un sadarbojas ar sadarbības grupu saistībā ar šā punkta pirmajā daļā minētajiem īstenošanas aktu projektiem.

9. Sadarbības grupa regulāri un jebkurā gadījumā vismaz reizi gadā tiekas ar Kritisko vienību noturības grupu, kas izveidota ar Direktīvu (ES) 2022/2557., lai veicinātu un atvieglotu stratēģisko sadarbību un informācijas apmaiņu.

15. pants

CSIRT tīkls

1. Lai palīdzētu attīstīt paļāvību un uzticēšanos un veicinātu ātru un efektīvu operatīvo sadarbību starp dalībvalstīm, tiek izveidots valsts *CSIRT* tīkls.

2. *CSIRT* tīklu veido saskaņā ar 10. pantu izraudzīto vai izveidoto *CSIRT* un Savienības iestāžu, struktūru un aģentūru datorapdraudējumu reaģēšanas vienības (*CERT-EU*) pārstāvji. Komisija piedalās *CSIRT* tīklā novērotāja statusā. *ENISA* nodrošina sekretariātu un aktīvi palīdz sadarbībā starp *CSIRT*.

3. *CSIRT* tīklam ir šādi uzdevumi:

a) apmainīties ar informāciju par *CSIRT* spējām;

b) sekmēt tehnoloģiju un attiecīgo pasākumu, rīcībpolitiku, rīku, procesu, paraugprakšu un satvaru kopīgošanu, pārnesi un apmaiņu *CSIRT* starpā;

c) apmainīties ar relevantu informāciju par incidentiem, gandrīz notikušiem notikumiem, kiberdraudiem, riskiem un ievainojamībām;

d) apmainīties ar informāciju par publikācijām un ieteikumiem kiberdrošības jomā;

e) nodrošināt sadarbspēju attiecībā uz informācijas kopīgošanas specifikācijām un protokoliem;

f) ja to lūdz *CSIRT* tīkla dalībnieks, kuru varētu ietekmēt incidents, – apmainīties ar informāciju par minēto incidentu un apspriest informāciju par to un saistītajiem kiberdraudiem, riskiem un ievainojamībām;

g) pēc *CSIRT* tīkla dalībnieka lūguma apspriest un, ja iespējams, īstenot saskaņotu reaģēšanu uz incidentu, kas ir identificēts attiecīgās dalībvalsts jurisdikcijā;

h) sniegt dalībvalstīm palīdzību pārrobežu incidentu risināšanā atbilstoši šai direktīvai;

i) sadarboties, apmainīties ar paraugpraksi un sniegt palīdzību *CSIRT*, kas izraudzītas par koordinatorēm saskaņā ar 12. panta 1. punktu, attiecībā uz tādas koordinētas ievainojamību izpaušanas pārvaldību, kas varētu būtiski ietekmēt vienības vairāk nekā vienā dalībvalstī;

j) 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 reaģēšanā uz pārrobežu riskiem un incidentiem;

   v) pēc kādas dalībvalsts lūguma – ieguldījumu valsts plānā reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm, kas minēts 9. panta 4. punktā;

k) informēt sadarbības grupu par savām darbībām un par turpmākajiem operatīvās sadarbības veidiem, kas apspriesti, ievērojot j) apakšpunktu, un nepieciešamības gadījumā lūgt norādījumus attiecībā uz tiem;

l) apkopot informāciju no kiberdrošības mācībām, tostarp tām, ko organizē *ENISA*;

m) pēc atsevišķas *CSIRT* pieprasījuma apspriest tās spējas un sagatavotību;

n) sadarboties un apmainīties ar informāciju ar reģionālajiem un Savienības līmeņa drošības operāciju centriem (*SOC*), lai uzlabotu vienotu situācijas izpratni par incidentiem un kiberdraudiem Savienībā;

o) attiecīgā gadījumā apspriest salīdzinošās izvērtēšanas ziņojumus, kas minēti 19. panta 9. punktā;

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

4. Šīs direktīvas 40. pantā minētās pārskatīšanas nolūkā *CSIRT* tīkls līdz 2025. gada 17. janvārim un pēc tam reizi divos gados novērtē operatīvajā sadarbībā gūto progresu un pieņem ziņojumu. Ziņojumā jo īpaši izdara secinājumus un izstrādā ieteikumus, pamatojoties uz rezultātiem, kas gūti 19. pantā minētajā salīdzinošajā izvērtēšanā, kura ir veikta attiecībā uz valstu *CSIRT*. Minēto ziņojumu iesniedz sadarbības grupai.

5. *CSIRT* tīkls pieņem savu reglamentu.

6. *CSIRT* tīkls un *EU-CyCLONe* vienojas par procesuālo kārtību un uz tās pamata sadarbojas.

16. pants

Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*)

1. *EU-CyCLONe* izveido, lai atbalstītu plašapmēra kiberdrošības incidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošinātu regulāru relevantas informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām.

2. *EU-CyCLONe* sastāvā ir pārstāvji no dalībvalstu kiberkrīžu pārvaldības iestādēm, kā arī - gadījumos, kad iespējamam vai notiekošam plašapmēra kiberdrošības incidentam ir vai varētu būt būtiska ietekme uz pakalpojumiem un darbībām, kas ietilpst šīs direktīvas darbības jomā - no Komisijas. Citos gadījumos Komisija *EU-CyCLONe* darbībās piedalās kā novērotāja.

ENISA nodrošina *EU-CyCLONe* sekretariātu un atbalsta drošu informācijas apmaiņu, kā arī nodrošina rīkus, kas vajadzīgi, lai atbalstītu dalībvalstu sadarbību drošas informācijas apmaiņas nodrošināšanā.

Attiecīgā gadījumā *EU-CyCLONe* var aicināt attiecīgo ieinteresēto personu pārstāvjus piedalīties tās darbā novērotāja statusā.

3. *EU-CyCLONe* ir šādi uzdevumi:

a) paaugstināt plašapmēra kiberdrošības incidentu un krīžu pārvaldības sagatavotības līmeni;

b) veidot vienotu situācijas izpratni par plašapmēra kiberdrošības incidentiem un krīzēm;

c) izvērtēt attiecīgo plašapmēra kiberdrošības incidentu un krīžu sekas un ietekmi un ierosināt iespējamos mitigācijas pasākumus;

d) koordinēt plašapmēra kiberdrošības incidentu un krīžu pārvaldību un atbalstīt lēmumu pieņemšanu politiskā līmenī saistībā ar šādiem incidentiem un krīzēm;

e) pēc attiecīgās dalībvalsts pieprasījuma apspriest 9. panta 4. punktā minētos valsts plānus reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm.

4. *EU-CyCLONe* pieņem savu reglamentu.

5. *EU-CyCLONe* regulāri ziņo sadarbības grupai par plašapmēra kiberdrošības incidentu un krīžu pārvaldību, kā arī tendencēm, īpaši pievēršoties to ietekmei uz būtiskajām un svarīgajām vienībām.

6. *EU-CyCLONe* sadarbojas ar *CSIRT* tīklu, pamatojoties uz saskaņotu procesuālo kārtību, kas paredzēta 15. panta 6. punktā.

7. Līdz 2024. gada 17. jūlijam un pēc tam reizi 18 mēnešos *EU-CyCLONe* iesniedz Eiropas Parlamentam un Padomei novērtējuma ziņojumu par savu darbu.

17. pants

Starptautiskā sadarbība

Attiecīgā gadījumā Savienība saskaņā ar LESD 218. pantu var noslēgt starptautiskus nolīgumus ar trešām valstīm vai starptautiskām organizācijām, kuri ļauj tām piedalīties un organizē to dalību sadarbības grupas, *CSIRT* tīkla un *EU-CyCLONe* konkrētās darbībās. Šādi nolīgumi atbilst Savienības datu aizsardzības tiesību aktiem.

18. pants

Ziņojums par situāciju kiberdrošības jomā Savienībā

1. *ENISA*, sadarbojoties ar Komisiju un sadarbības grupu, pieņem divgadu ziņojumu par situāciju kiberdrošības jomā Savienībā un iesniedz minēto ziņojumu Eiropas Parlamentam, kā arī iepazīstina Parlamentu ar to. Ziņojumu cita starpā iesniedz mašīnlasāmu datu veidā, un tajā iekļauj:

a) Savienības līmeņa kiberdrošības risku novērtējumu, kurā ir ņemta vērā kiberapdraudējuma aina;

b) kiberdrošības spēju attīstības novērtējumu publiskajā un privātajā sektorā visā Savienībā;

c) novērtējumu par vispārējo kiberdrošības izpratnes un kiberhigiēnas līmeni iedzīvotāju un vienību, tostarp mazo un vidējo uzņēmumu, vidū;

d) apkopotu novērtējumu par 19. pantā minēto salīdzinošo izvērtēšanu rezultātiem;

e) apkopotu novērtējumu par kiberdrošības spēju un resursu brieduma līmeni visā Savienībā, tostarp nozaru līmenī, kā arī par to, cik lielā mērā dalībvalstu kiberdrošības stratēģijas ir saskaņotas.

2. Ziņojumā iekļauj īpašus rīcībpolitiku ieteikumus trūkumu novēršanai un kiberdrošības līmeņa paaugstināšanai Savienībā un konstatējumu kopsavilkumu par attiecīgo periodu no *ENISA* saskaņā ar Regulas (ES) 2019/881 7. panta 6. punktu sagatavotajiem ES kiberdrošības tehniskās situācijas ziņojumiem par incidentiem un kiberdraudiem.

3. *ENISA* sadarbībā ar Komisiju, sadarbības grupu un *CSIRT* tīklu sagatavo metodiku, tostarp attiecīgos 1. punkta e) apakšpunktā minētā apkopotā novērtējuma mainīgos lielumus, piemēram, kvantitatīvos un kvalitatīvos rādītājus.

19. pants

Salīdzinošā izvērtēšana

1. Sadarbības grupa līdz 2025. gada 17. janvārim ar Komisijas un *ENISA* un attiecīgā gadījumā *CSIRT* tīkla palīdzību izstrādā salīdzinošās izvērtēšanas metodiku un organizatoriskos aspektus, lai mācītos no kopīgas pieredzes, stiprinātu savstarpējo uzticēšanos, panāktu vienādi augstu kiberdrošības līmeni, kā arī uzlabotu dalībvalstu kiberdrošības spējas un rīcībpolitikas, kas vajadzīgas šīs direktīvas īstenošanai. Dalība salīdzinošajā izvērtēšanā ir brīvprātīga. Salīdzinošo izvērtēšanu veic kiberdrošības eksperti. Kiberdrošības ekspertus ieceļ vismaz divas dalībvalstis, kas nav izvērtējamā dalībvalsts.

Salīdzinošās izvērtēšanas ietver vismaz vienu no šiem elementiem:

a) šīs direktīvas 21. un 23. pantā noteikto kiberdrošības risku pārvaldības pasākumu un ziņošanas pienākumu īstenošanas līmenis;

b) spēju līmenis, tostarp pieejamos finansiālos un tehniskos resursus un cilvēkresursus, un kompetento iestāžu uzdevumu izpildes efektivitāte;

c) *CSIRT* operatīvās spējas;

d) 37. pantā minētās savstarpējās palīdzības īstenošanas līmenis;

e) šīs regulas 29. pantā minētā kiberdrošības informācijas kopīgošanas mehānisma īstenošanas līmenis;

f) specifiski pārrobežu vai starpnozaru jautājumi.

2. Metodika, kas minēta 1. punktā, ietver objektīvus, nediskriminējošus, taisnīgus un pārredzamus kritērijus, uz kuru pamata dalībvalstis izraugās kiberdrošības ekspertus, kas ir tiesīgi veikt salīdzinošo izvērtēšanu. Komisija un *ENISA* piedalās salīdzinošajā izvērtēšanā novērotāja statusā.

3. Salīdzinošās izvērtēšanas vajadzībām dalībvalstis var identificēt specifiskus jautājumus, kā minēts 1. punkta f) apakšpunktā.

4. Pirms salīdzinošās izvērtēšanas sākšanas, kā minēts 1. punktā, dalībvalstis paziņo iesaistītajām dalībvalstīm tās tvērumu, tostarp specifiskos jautājumus, kuri identificēti, ievērojot 3. punktu.

5. Pirms salīdzinošās izvērtēšanas sākšanas dalībvalstis var veikt izvērtējamo aspektu pašnovērtējumu un iesniegt minēto pašnovērtējumu izraudzītajiem kiberdrošības ekspertiem. Sadarbības grupa ar Komisijas un *ENISA* palīdzību nosaka dalībvalstu pašnovērtējuma metodiku.

6. Salīdzinošā izvērtēšana ietver fiziskus vai virtuālus apmeklējumus klātienē un informācijas apmaiņu no tālienes. Saskaņā ar labas sadarbības principu dalībvalsts, par kuru veic salīdzinošo izvērtēšanu, izraudzītajiem ekspertiem sniedz izvērtēšanai nepieciešamo informāciju, neskarot valsts vai Savienības tiesību aktus par konfidenciālas vai klasificētas informācijas aizsardzību vai tādu būtisku valsts funkciju saglabāšanu kā valsts drošība. Sadarbības grupa sadarbībā ar Komisiju un *ENISA* izstrādā piemērotus rīcības kodeksus, kuros nosaka izraudzīto kiberdrošības ekspertu darba metodes. Visu salīdzinošās izvērtēšanas laikā iegūto informāciju izmanto tikai minētajam mērķim. Kiberdrošības eksperti, kuri piedalās salīdzinošajā izvērtēšanā, neizpauž trešām personām sensitīvu vai konfidenciālu informāciju, kas iegūta salīdzinošās izvērtēšanas laikā.

7. Pēc salīdzinošās izvērtēšanas par kādu no dalībvalstīm izvērtētos aspektus tajā pašā dalībvalstī nevērtē divus gadus pēc salīdzinošās izvērtēšanas noslēgšanas, ja vien minētā dalībvalsts nav pieprasījusi citādi vai pēc sadarbības grupas priekšlikuma nav panākta citāda vienošanās.

8. Dalībvalstis nodrošina, ka katrs interešu konflikta risks, kas attiecas uz izraudzītajiem kiberdrošības ekspertiem, pirms salīdzinošās izvērtēšanas sākšanas tiek darīts zināms pārējām dalībvalstīm, sadarbības grupai, Komisijai un *ENISA*. Dalībvalsts, par kuru veic salīdzinošo izvērtēšanu, var iebilst pret konkrētu kiberdrošības ekspertu izraudzīšanos, balstoties uz pienācīgi pamatotiem iemesliem, kas paziņoti ekspertus izraugošajai dalībvalstij.

9. Kiberdrošības eksperti, kuri piedalās salīdzinošajā izvērtēšanā, sagatavo ziņojumus par salīdzinošās izvērtēšanas konstatējumiem un secinājumiem. Dalībvalstis, par kurām veic salīdzinošo izvērtēšanu, var sniegt komentārus par tās izvērtējošo ziņojumu projektiem un šādus komentārus pievieno ziņojumiem. Ziņojumos iekļauj ieteikumus, kā panākt uzlabojumus aspektos, uz kuriem attiecas salīdzinošā izvērtēšana. Vajadzības gadījumā ziņojumus iesniedz sadarbības grupai un *CSIRT* tīklam. Dalībvalsts, par kuru veic salīdzinošo izvērtēšanu, var nolemt publiskot tās ziņojumu vai tā versiju ar aizklājumiem.

IV NODAĻA

KIBERDROŠĪBAS RISKU PĀRVALDĪBAS PASĀKUMI UN ZIŅOŠANAS PIENĀKUMI

20. pants

Pārvalde

1. Dalībvalstis nodrošina, ka būtisku un svarīgu vienību pārvaldes struktūras apstiprina kiberdrošības risku pārvaldības pasākumus, ko minētās vienības veikušas, lai izpildītu 21. panta prasības, pārrauga to īstenošanu, un no tām var prasīt atbildību par to, ka vienības ir pārkāpušas minēto pantu.

Šā punkta piemērošana neskar valsts tiesību aktus par atbildības noteikumiem, ko piemēro valsts iestādēm, kā arī par valsts ierēdņu un ievēlētu vai ieceltu amatpersonu atbildību.

2. Dalībvalstis nodrošina, ka būtisko un svarīgo vienību pārvaldības struktūru locekļiem tiek prasīts iziet apmācību, un mudina būtiskās un svarīgās vienības līdzīgu apmācību regulāri piedāvāt saviem darbiniekiem, lai nodrošinātu pietiekamas zināšanas un prasmes, kas tiem ļautu identificēt riskus un novērtēt kiberdrošības risku pārvaldības praksi, kā arī to ietekmi uz vienības sniegtajiem pakalpojumiem.

21. pants

Kiberdrošības risku pārvaldības pasākumi

1. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības veic atbilstīgus un samērīgus tehniskos, operatīvos un organizatoriskos pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmu drošībai, ko tās izmanto savā darbībā vai savu pakalpojumu sniegšanā, un novērstu vai līdz minimumam samazinātu incidentu ietekmi uz pakalpojumu saņēmējiem un uz citiem pakalpojumiem.

Ņemot vērā jaunākos un attiecīgā gadījumā atbilstošos Eiropas un starptautiskos standartus, kā arī īstenošanas izmaksas, pirmajā daļā minētie pasākumi nodrošina radītajiem riskiem atbilstošu tīklu un informācijas sistēmu drošības līmeni. Novērtējot minēto pasākumu samērīgumu, pienācīgi ņem vērā to, kādā mērā vienība ir pakļauta riskiem, vienības lielumu un incidentu iespējamību un smagumu, tostarp sociālo un ekonomisko ietekmi.

2. Pasākumu, kas minēti 1. punktā, pamatā ir visu apdraudējumu pieeja, kuras mērķis ir aizsargāt tīklu un informācijas sistēmas un šo sistēmu fizisko vidi no incidentiem, un tie ietver vismaz:

a) riska analīzes un informācijas sistēmu drošības rīcībpolitikas;

b) incidentu risināšanu;

c) darbības nepārtrauktību, piemēram, dublējuma pārvaldību un negadījuma seku novēršanu, un krīžu pārvaldību;

d) piegādes ķēdes drošību, tostarp ar drošību saistītus aspektus, kas skar attiecības starp katru vienību un tās tiešajiem piegādātājiem vai pakalpojumu sniedzējiem;

e) drošību tīklu un informācijas sistēmu ieguvē, attīstīšanā un uzturēšanā, tostarp rīcību ievainojamības gadījumā un ievainojamības izpaušanu;

f) rīcībpolitikas un procedūras, ar ko novērtē kiberdrošības risku pārvaldības pasākumu efektivitāti;

g) kiberhigiēnas pamatpraksi un apmācību kiberdrošības jomā;

h) rīcībpolitikas un procedūras attiecībā uz kriptogrāfijas un attiecīgā gadījumā šifrēšanas izmantošanu;

i) cilvēkresursu drošību, piekļuves kontroles rīcībpolitikas un aktīvu pārvaldību;

j) attiecīgā gadījumā daudzfaktoru autentifikācijas vai nepārtrauktas autentifikācijas risinājumus, drošu balss, video un teksta sakaru un drošu ārkārtas sakaru sistēmu izmantošanu vienībā.

3. Dalībvalstis nodrošina, ka, apsverot, kuri pasākumi, kas minēti šā panta 2. punkta d) apakšpunktā, ir piemēroti, vienības ņem vērā ievainojamības, kas raksturīgas katram tiešajam piegādātājam un pakalpojumu sniedzējam, un vispārējo savu piegādātāju un pakalpojumu sniedzēju produktu kvalitāti un to kiberdrošības praksi, tostarp to drošās izstrādes procedūras. Dalībvalstis nodrošina arī to, ka, apsverot, kuri minētajā apakšpunktā norādītie pasākumi ir piemēroti, no vienībām tiek prasīts ņemt vērā saskaņā ar 22. panta 1. punktu veikto kritisko piegādes ķēžu koordinēto drošības riska novērtējumu rezultātus.

4. Dalībvalstis nodrošina, ka vienība, kas konstatē, ka tā neievēro 2. punktā paredzētos pasākumus, bez liekas kavēšanās veic visus nepieciešamos, piemērotos un samērīgos korektīvos pasākumus.

5. Līdz 2024. gada 17. oktobrim Komisija pieņem īstenošanas aktus, ar kuriem nosaka 2. punktā minēto pasākumu tehniskās un metodiskās prasības attiecībā uz DNS pakalpojumu sniedzējiem, ALD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem un uzticamības pakalpojumu sniedzējiem.

Komisija var pieņemt īstenošanas aktus, ar kuriem nosaka tehniskās un metodiskās prasības, kā arī vajadzības gadījumā nozaru prasības 2. punktā minētajiem pasākumiem attiecībā uz būtiskām un svarīgām vienībām, kas nav minētas šā punkta pirmajā daļā.

Sagatavojot šā punkta pirmajā un otrajā daļā minētos īstenošanas aktus, Komisija, ciktāl iespējams, ievēro Eiropas un starptautiskos standartus, kā arī attiecīgās tehniskās specifikācijas. Komisija apmainās ar padomiem un sadarbojas ar sadarbības grupu un *ENISA* jautājumos par īstenošanas aktu projektiem saskaņā ar 14. panta 4. punkta e) apakšpunktu.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

22. pants

Savienības līmenī koordinētie kritisko piegādes ķēžu drošības riska novērtējumi

1. Sadarbības grupa kopā ar Komisiju un *ENISA* var veikt konkrētu kritisku IKT pakalpojumu, IKT sistēmu vai IKT 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*, kā arī – vajadzības gadījumā – attiecīgajām ieinteresētajām personām identificē konkrētos kritiskos IKT pakalpojumus, IKT sistēmas vai IKT produktus, par kuriem var veikt 1. punktā minēto koordinēto drošības riska novērtējumu.

23. pants

Ziņošanas pienākumi

1. Katra dalībvalsts nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās paziņo *CSIRT* vai attiecīgā gadījumā savai kompetentajai iestādei saskaņā ar 4. punktu par ikvienu incidentu, kam ir būtiska ietekme uz to pakalpojumu sniegšanu, kā minēts 3. punktā (būtisks incidents). Atbilstošā gadījumā attiecīgās vienības bez nepamatotas kavēšanās informē savus pakalpojumu saņēmējus par būtiskiem incidentiem, kas varētu nelabvēlīgi ietekmēt minēto pakalpojumu sniegšanu. Katra dalībvalsts nodrošina, ka minētās vienības cita starpā paziņo visu informāciju, kas ļauj *CSIRT* vai attiecīgā gadījumā kompetentajai iestādei noteikt incidenta pārrobežu ietekmi. Paziņošanas akts vien neuzliek paziņotājai vienībai lielāku atbildību.

Ja attiecīgās vienības paziņo kompetentajai iestādei par būtisku incidentu saskaņā ar pirmo daļu, dalībvalsts nodrošina, ka minētā kompetentā iestāde pēc paziņojuma saņemšanas to pārsūta arī *CSIRT*.

Pārrobežu vai starpnozaru būtiska incidenta gadījumā dalībvalstis nodrošina, ka to vienotajiem kontaktpunktiem laikus tiek sniegta relevanta informācija, kas paziņota saskaņā ar 4. punktu.

2. Attiecīgā gadījumā dalībvalstis nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās paziņo saviem pakalpojumu saņēmējiem, kurus varētu skart būtiski kiberdraudi, par visiem pasākumiem vai korektīvajiem līdzekļiem, ko minētie saņēmēji var izmantot, reaģējot uz minētajiem draudiem. Attiecīgā gadījumā vienības informē minētos saņēmējus arī par pašiem būtiskajiem kiberdraudiem.

3. Incidentu uzskata par būtisku, ja:

a) tas ir izraisījis vai spēj izraisīt smagus pakalpojumu darbības traucējumus vai finansiālus zaudējumus attiecīgajai vienībai;

b) tas ir ietekmējis vai spēj ietekmēt citas fiziskas vai juridiskas personas, izraisot ievērojamu materiālo vai nemateriālo kaitējumu.

4. Dalībvalstis nodrošina, ka 1. punktā noteiktās paziņošanas nolūkos attiecīgās vienības iesniedz *CSIRT* vai attiecīgā gadījumā kompetentajai iestādei:

a) bez nepamatotas kavēšanās un katrā ziņā 24 stundu laikā no brīža, kad uzzinājušas par būtisku incidentu, – agrīnu brīdinājumu, kurā attiecīgā gadījumā norāda, vai ir aizdomas, ka būtisko incidentu ir izraisījusi nelikumīga vai ļaunprātīga rīcība, un vai tam varētu būt pārrobežu ietekme;

b) bez nepamatotas kavēšanās un jebkurā gadījumā 72 stundu laikā pēc tam, kad uzzinājušas par būtisko incidentu, – paziņojumu par incidentu, kurā attiecīgā gadījumā atjaunina a) apakšpunktā minēto informāciju un norāda būtiskā incidenta sākotnējo novērtējumu, tostarp tā smagumu un ietekmi, kā arī, ja pieejami, aizskāruma rādītājus;

c) pēc *CSIRT* vai attiecīgā gadījumā kompetentās iestādes pieprasījuma – starpposma ziņojumu par attiecīgajiem statusa atjauninājumiem;

d) galīgu ziņojumu ne vēlāk kā mēnesi pēc b) apakšpunktā minētā paziņojuma par incidentu iesniegšanas, tajā iekļaujot:

   i) incidenta, tostarp tā smaguma un ietekmes sīku aprakstu;

   ii) draudu veidu vai pamatcēloni, kas, iespējams, varētu būt izraisījis incidentu;

   iii) piemērotos un notiekošos mitigācijas pasākumus;

   iv) attiecīgā gadījumā informāciju par incidenta pārrobežu ietekmi;

e) ja pēc d) apakšpunktā minētā galīgā ziņojuma iesniegšanas brīža incidents vēl nav beidzies, dalībvalstis nodrošina, ka attiecīgās vienības tajā laikā iesniedz progresa ziņojumu un viena mēneša laikā pēc incidenta risināšanas iesniedz galīgo ziņojumu.

Atkāpjoties no pirmās daļas b) apakšpunkta, uzticamības pakalpojumu sniedzējs par būtiskiem incidentiem, kas ietekmē tā uzticamības pakalpojumu sniegšanu, bez nepamatotas kavēšanās un jebkurā gadījumā 24 stundu laikā pēc uzzināšanas par būtisko incidentu paziņo *CSIRT* vai attiecīgā gadījumā kompetentajai iestādei.

5. *CSIRT* vai kompetentā iestāde bez liekas kavēšanās un, ja iespējams, 24 stundu laikā no 4. punkta a) apakšpunktā minētā agrīnā brīdinājuma saņemšanas sniedz paziņotājai vienībai atbildi, kurā iekļauj sākotnējo komentāru par būtisko incidentu un – pēc vienības pieprasījuma – norādījumus vai praktiskus padomus par iespējamo mitigācijas pasākumu īstenošanu. Ja *CSIRT* nav sākotnējais 1. un 2. punktā minētā paziņojuma saņēmējs, norādījumus sniedz kompetentā iestāde, sadarbojoties ar *CSIRT*. Ja attiecīgā vienība lūdz papildu tehnisko atbalstu, *CSIRT* to sniedz. Ja ir aizdomas, ka būtiskais incidents ir noziedzīgs, *CSIRT* vai kompetentā iestāde arī dod norādījumus par būtiskā incidenta paziņošanu tiesībaizsardzības iestādēm.

6. Attiecīgā gadījumā, īpaši tad, ja 1. punktā minētais būtiskais incidents skar divas vai vairākas dalībvalstis, *CSIRT*, kompetentā iestāde vai vienotais kontaktpunkts bez liekas kavēšanās informē citas skartās dalībvalstis un *ENISA* par būtisko incidentu. Šāda informācija ietver tā veida informāciju, kas saņemta saskaņā ar 4. punktu. To darot, *CSIRT*, kompetentā iestāde vai vienotais kontaktpunkts saskaņā ar Savienības vai valsts tiesību aktiem nodrošina vienības drošību un komerciālās intereses, kā arī sniegtās informācijas konfidencialitāti.

7. Ja ir nepieciešams informēt sabiedrību, lai novērstu būtisku incidentu vai risinātu notiekošu būtisku incidentu, vai būtiska incidenta izpaušana citādi ir sabiedrības interesēs, dalībvalsts *CSIRT* vai attiecīgā gadījumā tās kompetentā iestāde vai vajadzības gadījumā citu iesaistīto dalībvalstu *CSIRT* vai kompetentās iestādes pēc apspriešanās ar attiecīgo vienību var informēt sabiedrību par būtisko incidentu vai pieprasīt, lai to dara vienība.

8. Pēc *CSIRT* vai kompetentās iestādes pieprasījuma vienotais kontaktpunkts nosūta atbilstoši 1. punktam saņemtos paziņojumus citu skarto dalībvalstu vienotajiem kontaktpunktiem.

9. Vienotais kontaktpunkts reizi trijos mēnešos iesniedz *ENISA* kopsavilkuma ziņojumu, kurā iekļauj anonimizētus un apkopotus datus par būtiskiem incidentiem, incidentiem, kiberdraudiem un gandrīz notikušiem notikumiem, par kuriem paziņots saskaņā ar šā panta 1. punktu un 30. pantu. Lai veicinātu salīdzināmas informācijas sniegšanu, *ENISA* var pieņemt tehniskus norādījumus par kopsavilkuma ziņojumā iekļaujamās informācijas parametriem. *ENISA* reizi sešos mēnešos informē sadarbības grupu un *CSIRT* tīklu par saviem konstatējumiem par saņemtajiem paziņojumiem.

10. *CSIRT* vai attiecīgā gadījumā kompetentās iestādes sniedz Direktīvā (ES) 2022/2557 minētajām kompetentajām iestādēm informāciju par būtiskiem incidentiem, incidentiem, kiberdraudiem un gandrīz notikušiem notikumiem, par kuriem vienības, kas identificētas kā kritiskās vienības Direktīvā (ES) 2022/2557, ir paziņojušas saskaņā ar šā panta 1. punktu un 30. pantu.

11. Komisija var pieņemt īstenošanas aktus, kuros sīkāk precizē atbilstoši šā panta 1. punktam un 30. pantam iesniegtajā ziņojumā un atbilstoši šā panta 2. punktam iesniegtajā ziņojumā iekļaujamās informācijas veidu, ziņojuma formātu un paziņošanas procedūru.

Līdz 2024. gada 17. oktobrim Komisija attiecībā uz DNS pakalpojumu sniedzējiem, ALD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, kā arī tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem, pieņem īstenošanas aktus, kuros sīkāk precizē gadījumus, kad incidentu uzskata par būtisku, kā minēts 3. punktā. Komisija var pieņemt šādus īstenošanas aktus attiecībā uz citām būtiskām un svarīgām vienībām.

Komisija apmainās ar padomiem un sadarbojas ar sadarbības grupu saistībā ar šā punkta pirmajā un otrajā daļā minētajiem īstenošanas aktu projektiem saskaņā ar 14. panta 4. punkta e) apakšpunktu.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 39. panta 2. punktā.

24. pants

Eiropas kiberdrošības sertifikācijas shēmu izmantošana

1. Lai pierādītu atbilstību konkrētām 21. panta prasībām, dalībvalstis var pieprasīt būtiskām un svarīgām vienībām izmantot konkrētus IKT produktus, IKT pakalpojumus un IKT procesus, ko būtiskā vai svarīgā vienība ir izstrādājusi vai iepirkusi no trešām pusēm, kuras ir sertificētas atbilstoši Eiropas kiberdrošības sertifikācijas shēmām, kas pieņemtas saskaņā ar Regulas (ES) 2019/881 49. pantu. Dalībvalstis turklāt mudina būtiskās un svarīgās vienības izmantot kvalificētus uzticamības pakalpojumus.

2. Komisija ir pilnvarota pieņemt deleģētus aktus saskaņā ar 38. pantu, lai papildinātu šo direktīvu, nosakot, kurām būtisko un svarīgo vienību kategorijām ir jāizmanto konkrēti sertificēti IKT produkti, IKT pakalpojumi un IKT procesi vai jāsaņem sertifikāts atbilstoši kādai no Eiropas kiberdrošības sertifikācijas shēmām, kas pieņemta saskaņā ar Regulas (ES) 2019/881 49. pantu. Šādus deleģētos aktus pieņem, ja ir konstatēts nepietiekams kiberdrošības līmenis, un tajos iekļauj īstenošanas periodu.

Pirms šādu deleģēto aktu pieņemšanas Komisija veic ietekmes novērtējumu un veic apspriešanos saskaņā ar Regulas (ES) 2019/881 56. pantu.

3. Ja šā panta 2. punkta nolūkiem nav pieejama neviena atbilstīga Eiropas kiberdrošības sertifikācijas shēma, Komisija pēc apspriešanās ar sadarbības grupu un Eiropas Kiberdrošības sertifikācijas grupu pieprasa, lai *ENISA* sagatavo kandidātshēmu atbilstoši Regulas (ES) 2019/881 48. panta 2. punktam.

25. pants

Standartizācija

1. Lai sekmētu 21. panta 1. un 2. punkta konverģentu īstenošanu, dalībvalstis, neliekot izmantot konkrēta veida tehnoloģiju un nediskriminējot par labu tādas izmantošanai, veicina tīklu un informācijas sistēmu drošībai relevantu Eiropas un starptautisko standartu un tehnisko specifikāciju izmantošanu.

2. *ENISA* sadarbībā ar dalībvalstīm un attiecīgā gadījumā pēc apspriešanās ar attiecīgajām ieinteresētajām personām izstrādā padomus un pamatnostādnes par tehniskajām jomām, kas jāapsver saistībā ar 1. punktu, kā arī par jau esošajiem standartiem, tostarp valsts standartiem, kas ļautu aptvert minētās jomas.

V NODAĻA

JURISDIKCIJA UN REĢISTRĀCIJA

26. pants

Jurisdikcija un teritorialitāte

1. Uzskata, ka vienības, kas ietilpst šīs direktīvas darbības jomā, ir tās dalībvalsts jurisdikcijā, kurā tās ir iedibinātas, izņemot:

a) publisko elektronisko sakaru tīklu nodrošinātājus vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējus, kurus uzskata par tādiem, kas ir tās dalībvalsts jurisdikcijā, kur tie sniedz savus pakalpojumus;

b) DNS pakalpojumu sniedzējus, ALD nosaukumu reģistrus, vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, mākoņdatošanas pakalpojumu sniedzējus, datu centru pakalpojumu sniedzējus, satura piegādes tīklu nodrošinātājus, pārvaldītu pakalpojumu sniedzējus, pārvaldītu drošības pakalpojumu sniedzējus, kā arī tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu vai sociālās tīklošanās pakalpojumu platformu nodrošinātājus, kurus uzskata par tādiem, kas ir tās dalībvalsts jurisdikcijā, kurā ir to galvenais iedibinājums Savienībā saskaņā ar 2. punktu.

c) valsts pārvaldes vienības, kuras uzskata par esošām tās dalībvalsts jurisdikcijā, kura tās ir izveidojusi.

2. Šīs direktīvas nolūkos uzskata, ka vienībai, kas minēta 1. punkta b) apakšpunktā, galvenais iedibinājums Savienībā ir tajā dalībvalstī, kurā galvenokārt tiek pieņemti lēmumi saistībā ar kiberdrošības risku pārvaldības pasākumiem. Ja šādu dalībvalsti nevar noteikt vai šādus lēmumus nepieņem Savienībā, uzskata, ka galvenais iedibinājums ir dalībvalstī, kurā tiek veiktas kiberdrošības operācijas. Ja šādu dalībvalsti nevar noteikt, uzskata, ka galvenais iedibinājums ir dalībvalstī, kurā attiecīgajai vienībai ir iedibinājums ar vislielāko darbinieku skaitu Savienībā.

3. Ja 1. punkta b) apakšpunktā minētā vienība nav iedibināta Savienībā, bet tā piedāvā pakalpojumus Savienībā, tā izraugās pārstāvi Savienībā. Minētajam pārstāvim iedibinājums vieta ir vienā no dalībvalstīm, kurās tiek piedāvāti pakalpojumi. Uzskata, ka šāda vienība ir tās dalībvalsts jurisdikcijā, kurā ir pārstāvja iedibinājums. Ja nav izraudzīta pārstāvja Savienībā atbilstoši šim punktam, jebkura dalībvalsts, kurā vienība sniedz pakalpojumus, var veikt tiesiskas darbības pret vienību par šīs direktīvas pārkāpumu.

4. Šā panta 1. punkta b) apakšpunktā minētās vienības veiktā pārstāvja izraudzīšanās neskar tiesiskās darbības, ko var ierosināt pret pašu vienību.

5. Dalībvalstis, kas ir saņēmušas savstarpējas palīdzības lūgumu attiecībā uz 1. punkta b) apakšpunktā minēto vienību, var minētā lūguma robežās veikt pienācīgus uzraudzības un izpildes panākšanas pasākumus attiecībā uz attiecīgo vienību, kas to teritorijā sniedz pakalpojumus vai kam tur ir tīkls un informācijas sistēma.

27. pants

Vienību reģistrs

1. *ENISA* izveido un uztur DNS pakalpojumu sniedzēju, ALD nosaukumu reģistratoru, vienību, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, mākoņdatošanas pakalpojumu sniedzēju, datu centru pakalpojumu sniedzēju, satura piegādes tīklu nodrošinātāju, pārvaldītu pakalpojumu sniedzēju, pārvaldītu drošības pakalpojumu sniedzēju, kā arī tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu vai sociālās tīklošanās pakalpojumu platformu nodrošinātāju reģistru, pamatojoties uz informāciju, kas saņemta no vienotajiem kontaktpunktiem, saskaņā ar 4. punktu. Pēc pieprasījuma *ENISA* atļauj kompetentajām iestādēm piekļūt minētajam reģistram, vienlaikus attiecīgā gadījumā nodrošinot, ka informācijas konfidencialitāte ir aizsargāta.

2. Dalībvalstis pieprasa 1. punktā minētajām vienībām līdz 2025. gada 17. janvārim iesniegt kompetentajām iestādēm šādu informāciju:

a) vienības nosaukums;

b) attiecīgā gadījumā – I vai II pielikumā minētā nozare, apakšnozare un vienības veids;

c) vienības galvenā iedibinājuma adrese un tās citu juridisku iedibinājumu adreses Savienībā vai, ja vienība nav iedibināta Savienībā – ievērojot 26. panta 3. punktu izraudzītā pārstāvja iedibinājuma adrese Savienībā;

d) atjaunināta kontaktinformācija, tostarp vienības un attiecīgā gadījumā tās saskaņā ar 26. panta 3. punktu ieceltā pārstāvja e-pasta adreses un tālruņa numuri;

e) dalībvalstis, kurās vienība sniedz pakalpojumus; un

f) vienības IP adrešu diapazoni.

3. Dalībvalstis nodrošina, ka vienības, kas minētas 1. punktā, par visām izmaiņām informācijā, ko tās iesniegušas atbilstoši 2. punktam, paziņo kompetentajai iestādei nekavējoties un katrā ziņā trīs mēnešu laikā no attiecīgo izmaiņu stāšanās spēkā.

4. Pēc 2. un 3. punktā minētās informācijas, izņemot 2. punkta f) apakšpunktā minētās, saņemšanas attiecīgās dalībvalsts vienotais kontaktpunkts bez liekas kavēšanās pārsūta to *ENISA*.

5. Attiecīgā gadījumā šā panta 2. un 3. punktā minēto informāciju iesniedz, izmantojot valsts mehānismu, kas minēts 3. panta 4. punkta ceturtajā daļā.

28. pants

Domēnu nosaukumu reģistrācijas datubāze

1. Lai veicinātu DNS drošību, stabilitāti un noturību, dalībvalstis pieprasa, lai ALD nosaukumu reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, ar pienācīgu rūpību savāktu un uzturētu precīzus un pilnīgus domēnu nosaukumu reģistrācijas datus īpaši tam paredzētā datubāzē saskaņā ar Savienības datu aizsardzības tiesību aktiem par attiecībā uz datiem, kas ir persondati.

2. Šā panta 1. punkta nolūkos dalībvalstis pieprasa, lai domēnu nosaukumu reģistrācijas datubāzē tiktu ietverta vajadzīgā informācija, kas ļautu identificēt domēnu nosaukumu turētājus un kontaktpunktus, kuri pārvalda ALD nosaukumus, un sazināties ar tiem. Šāda informācija ietver:

a) domēna nosaukumu;

b) reģistrācijas datumu;

c) reģistrētāja vārdu un uzvārdu, e-pasta adresi un tālruņa numuru;

d) tā kontaktpunkta e-pasta adresi un tālruņa numuru, kurš pārvalda domēna nosaukumu, ja tie atšķiras no reģistrētāja e-pasta adreses un tālruņa numura.

3. Dalībvalstis pieprasa ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, ieviest rīcībpolitikas un procedūras, tostarp verifikācijas procedūras, lai nodrošinātu, ka 1. punktā minētajā datubāzē ir iekļauta precīza un pilnīga informācija. Dalībvalstis pieprasa, lai šādas rīcībpolitikas un procedūras tiktu publiskotas.

4. Dalībvalstis pieprasa ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, bez nepamatotas kavēšanās pēc domēna nosaukuma reģistrācijas darīt publiski pieejamus domēnu nosaukumu reģistrācijas datus, kuri nav persondati.

5. Dalībvalstis pieprasa ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, sniegt leģitīmiem piekļuves prasītājiem pēc to likumīgiem un pienācīgi pamatotiem pieprasījumiem piekļuvi konkrētiem domēnu nosaukumu reģistrācijas datiem, ievērojot Savienības datu aizsardzības tiesību aktus. Dalībvalstis pieprasa ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, bez nepamatotas kavēšanās un jebkurā gadījumā 72 stundu laikā pēc jebkādu piekļuves pieprasījumu saņemšanas atbildēt uz tiem. Dalībvalstis pieprasa, lai rīcībpolitikas un procedūras attiecībā uz šādu datu izpaušanu tiktu darītas publiski pieejamas.

6. Šā panta 1.–5. punktā noteikto pienākumu izpilde neizraisa domēnu nosaukumu reģistrācijas datu divkāršu vākšanu. Šajā nolūkā dalībvalstis pieprasa ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus, savstarpēji sadarboties.

VI NODAĻA

INFORMĀCIJAS KOPĪGOŠANA

29. pants

Kiberdrošības informācijas kopīgošanas mehānisms

1. Dalībvalstis nodrošina, ka vienības, kuras ietilpst šīs direktīvas darbības jomā, un attiecīgā gadījumā citas vienības, kuras neietilpst šīs direktīvas darbības jomā, var brīvprātīgi savstarpēji apmainīties ar relevantu kiberdrošības informāciju, tostarp informāciju, kas attiecas uz kiberdraudiem, gandrīz notikušiem notikumiem, ievainojamību, paņēmieniem un procedūrām, aizskāruma rādītājiem, pretinieku taktiku, specifisku informāciju par apdraudējuma aktoru, kiberdrošības brīdinājumiem un ieteikumiem attiecībā uz drošības rīku konfigurācijām kiberuzbrukumu atklāšanai, ja šāda informācijas kopīgošana:

a) ir paredzēta, lai novērstu un atklātu incidentus, reaģētu uz tiem vai atgūtos no tiem, vai mazinātu to ietekmi;

b) uzlabo kiberdrošības līmeni, it īpaši, palielinot informētību par kiberdraudiem, ierobežojot šādu draudu izplatīšanās spējas vai traucējot šādām spējām īstenoties, atbalstot virkni aizsardzības spēju, ievainojamības izlabošanu un izpaušanu, draudu atklāšanas, ierobežošanas un novēršanas metodes, mitigācijas stratēģijas vai reaģēšanas un seku novēršanas posmus vai veicinot publiskā un privātā sektora sadarbību kiberdraudu izpētē.

2. Dalībvalstis nodrošina, ka informācijas apmaiņa notiek būtisko un svarīgo vienību kopienās un attiecīgā gadījumā to piegādātāju un pakalpojumu sniedzēju kopienās. Šādu apmaiņu īsteno, izveidojot kiberdrošības informācijas kopīgošanas mehānismu attiecībā uz nodotās informācijas iespējami sensitīvo raksturu.

3. Dalībvalstis veicina šā panta 2. punktā minēto kiberdrošības informācijas kopīgošanas mehānisma izveidi. Šāds mehānisms var precizēt operatīvos elementus, tostarp speciālu IKT platformu un automatizācijas rīku izmantošanu, saturu un nosacījumus. Detalizētāk aprakstot publisku iestāžu iesaistīšanos šādā mehānismā, dalībvalstis var paredzēt nosacījumus attiecībā uz informāciju, ko dara pieejamu kompetentās iestādes vai *CSIRT*. Dalībvalstis piedāvā palīdzību šāda mehānisma piemērošanā atbilstoši savām rīcībpolitikām, kas minētas 7. panta 2. punkta h) apakšpunktā.

4. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības informē kompetentās iestādes par savu dalību 2. punktā minētajā kiberdrošības informācijas kopīgošanas mehānismā, tiklīdz tās iesaistās šādā mehānismā, vai attiecīgā gadījumā – par izstāšanos no šāda mehānisma, tiklīdz izstāšanās stājas spēkā.

5. *ENISA* palīdz 2. punktā minētā kiberdrošības informācijas kopīgošanas mehānisma izveidē, apmainoties ar paraugpraksi un sniedzot norādījumus.

30. pants

Relevantas informācijas brīvprātīga paziņošana

1. Dalībvalstis nodrošina, ka papildus 23. pantā paredzētajam paziņošanas pienākumam paziņojumus *CSIRT* vai attiecīgā gadījumā kompetentajām iestādēm var brīvprātīgi iesniegt:

a) būtiskās un svarīgās vienības attiecībā uz incidentiem, kiberdraudiem un gandrīz notikušiem notikumiem;

b) vienības, kas nav minētas a) apakšpunktā, neatkarīgi no tā, vai tās ietilpst šīs direktīvas darbības jomā, attiecībā uz būtiskiem incidentiem, kiberdraudiem un gandrīz notikušiem notikumiem.

2. Dalībvalstis šā panta 1. punktā minētos paziņojumus apstrādā saskaņā ar 23. pantā noteikto procedūru. Dalībvalstis obligātos paziņojumus var apstrādāt, nosakot tiem prioritāti pār brīvprātīgajiem paziņojumiem.

Vajadzības gadījumā *CSIRT* un attiecīgā gadījumā kompetentās iestādes sniedz vienotajiem kontaktpunktiem informāciju par paziņojumiem, kas saņemti, ievērojot šo pantu, vienlaikus nodrošinot paziņotājas vienības sniegtās informācijas konfidencialitāti un pienācīgu aizsardzību. Neskarot noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem, brīvprātīgās paziņošanas rezultātā paziņotājai vienībai netiek uzlikti nekādi papildu pienākumi, kādi tai netiktu uzlikti, ja tā nebūtu iesniegusi minēto paziņojumu.

VII NODAĻA

UZRAUDZĪBA UN IZPILDES PANĀKŠANA

31. pants

Vispārīgi uzraudzības un izpildes panākšanas aspekti

1. Dalībvalstis nodrošina, ka to kompetentās iestādes efektīvi uzrauga šīs direktīvas izpildi un veic nepieciešamos pasākumus, lai to nodrošinātu.

2. Dalībvalstis var atļaut to kompetentajām iestādēm uzraudzības uzdevumus prioritizēt. Šādas prioritizēšanas pamatā ir uz risku balstīta pieeja. Šajā nolūkā, pildot šā panta 32. un 33. pantā paredzētos uzraudzības uzdevumus, kompetentās iestādes var izveidot uzraudzības metodiku, kas ļauj noteikt prioritātes attiecībā uz šādiem uzdevumiem, ievērojot uz risku balstītu pieeju.

3. Pievēršoties incidentiem, kuru rezultātā notiek persondatu aizsardzības pārkāpumi, kompetentās iestādes strādā ciešā sadarbībā ar Regulā (ES) 2016/679 minētajām uzraudzības iestādēm, neskarot uzraudzības iestādēm minētajā regulā noteikto kompetenci un uzdevumus.

4. Neskarot valsts tiesisko regulējumu un iestāžu sistēmas, dalībvalstis nodrošina, ka, uzraugot valsts pārvaldes vienību atbilstību šai direktīvai un nosakot izpildes panākšanas pasākumus par šīs direktīvas pārkāpumiem, kompetentajām iestādēm ir atbilstīgas pilnvaras veikt šādus uzdevumus operatīvi neatkarīgi no uzraudzītajām valsts pārvaldes vienībām. Dalībvalstis var lemt par piemērotu, samērīgu un efektīvu uzraudzības un izpildes panākšanas pasākumu noteikšanu attiecībā uz minētajām vienībām saskaņā ar valsts tiesisko regulējumu un iestāžu sistēmu.

32. pants

Uzraudzības un izpildes panākšanas pasākumi attiecībā uz būtiskajām vienībām

1. Dalībvalstis nodrošina, ka uzraudzības vai izpildes panākšanas 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 vismaz:

a) inspekcijas uz vietas un attālinātu uzraudzību, arī izlases veida pārbaudes, ko veic apmācīti speciālisti;

b) regulāras un mērķtiecīgas drošības revīzijas, ko veic neatkarīga struktūra vai kompetenta iestāde;

c) *ad hoc* revīzijas, tostarp, kad to pamato būtisks incidents vai būtiskās vienības šīs direktīvas pārkāpums;

d) drošības skenēšanu, pamatojoties uz objektīviem, nediskriminējošiem, taisnīgiem un pārredzamiem riska novērtēšanas kritērijiem, vajadzības gadījumā sadarbībā ar attiecīgo vienību;

e) tādas informācijas pieprasījumus, kas nepieciešama, lai novērtētu attiecīgās vienības pieņemtos kiberdrošības risku pārvaldības pasākumus, tostarp dokumentētas kiberdrošības rīcībpolitikas, kā arī atbilstību pienākumam iesniegt informāciju kompetentajām iestādēm atbilstīgi 27. pantam;

f) pieprasījumus piekļūt datiem, dokumentiem un informācijai, kas nepieciešama to uzraudzības uzdevumu izpildei;

g) pieprasījumus par pierādījumiem, ka tiek īstenotas kiberdrošības rīcībpolitikas, piemēram, kvalificēta revidenta veikto drošības revīziju rezultātiem un attiecīgajiem pamatā esošajiem pierādījumiem.

Šā punkta pirmās daļas b) apakšpunktā minēto mērķtiecīgo drošības revīziju pamatā ir riska novērtējumi, ko veic kompetentā iestāde vai revidētā vienība, vai cita ar risku saistīta pieejamā informācija.

Ikvienas mērķtiecīgās drošības revīzijas rezultātus dara pieejamus kompetentajai iestādei. Šādas neatkarīgas struktūras veiktas mērķtiecīgas drošības revīzijas izmaksas sedz revidētā vienība, izņemot pienācīgi pamatotus gadījumus, kad kompetentā iestāde nolemj citādi.

3. Īstenojot savas pilnvaras saskaņā ar 2. punkta e), f) vai g) apakšpunktu, kompetentās iestādes norāda pieprasījuma mērķi un precizē prasīto informāciju.

4. Dalībvalstis nodrošina, ka to kompetentajām iestādēm, īstenojot izpildes panākšanas pilnvaras attiecībā uz būtiskajām vienībām, ir pilnvaras vismaz:

a) izdot brīdinājumus par attiecīgo vienību šīs direktīvas pārkāpumiem;

b) pieņemt saistošus norādījumus, tostarp par pasākumiem, kas vajadzīgi, lai novērstu vai atrisinātu incidentu, kā arī šādu pasākumu īstenošanas termiņus un termiņus, kādā jāziņo par to īstenošanu, vai rīkojumu, ar kuru pieprasa, lai attiecīgās vienības novērš konstatētos trūkumus vai šīs direktīvas pārkāpumus;

c) uzdot attiecīgajām iestādēm izbeigt rīcību, ar ko pārkāpj šo direktīvu, un atturēties no tādas rīcības atkārtošanas;

d) uzdot attiecīgajām vienībām konkrētā veidā un konkrētā laikposmā nodrošināt savu kiberdrošības risku pārvaldības pasākumu atbilstību 21. pantam vai izpildīt ziņošanas pienākumu, kas noteikts 23. pantā;

e) uzdot attiecīgajām vienībām informēt fiziskās vai juridiskās personas, attiecībā uz kurām tās sniedz pakalpojumus vai veic darbības, kuras var ietekmēt būtiski kiberdraudi, par apdraudējuma raksturu, kā arī par visiem iespējamajiem aizsardzības vai korektīviem pasākumiem, ko attiecīgās fiziskās vai juridiskās personas var veikt, reaģējot uz šādiem draudiem;

f) uzdot attiecīgajām vienībām saprātīgā termiņā īstenot ieteikumus, kas sniegti drošības revīzijas rezultātā;

g) norīkot uzraudzības speciālistu, kam ir precīzi definēti uzdevumi, noteiktā laikposmā pārraudzīt, vai attiecīgās vienības ievēro 21. un 23. pantu;

h) uzdot attiecīgajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos vērojama šīs direktīvas pārkāpšana;

i) piemērot vai pieprasīt, lai attiecīgās struktūras, tiesas vai tribunāli saskaņā ar valsts tiesību aktiem piemēro administratīvu naudas sodu atbilstoši 34. pantam papildus pasākumiem, kas minēti šā punkta a)–h) apakšpunktā.

5. Ja izrādās, ka izpildes panākšanas pasākumi, kas pieņemti atbilstoši 4. punkta a)–d) un f) apakšpunktam, ir neefektīvi, dalībvalstis nodrošina, ka to kompetentajām iestādēm ir pilnvaras noteikt termiņu, līdz kuram būtiskajai vienībai ir jāveic nepieciešamā rīcība, lai novērstu trūkumus vai izpildītu minēto iestāžu prasības. Ja pieprasītā darbība netiek veikta noteiktajā termiņā, dalībvalstis nodrošina, ka kompetentajām iestādēm ir šādas pilnvaras:

a) uz laiku apturēt vai pieprasīt sertifikācijas vai apstiprināšanas struktūrai vai tiesai vai tribunālam saskaņā ar valsts tiesību aktiem uz laiku apturēt sertifikāciju vai atļauju attiecībā uz visiem būtiskās vienības sniegtajiem attiecīgajiem pakalpojumiem vai veiktajām darbībām vai to daļu;

b) pieprasīt, lai attiecīgās struktūras, tiesas vai tribunāli saskaņā ar valsts tiesību aktiem uz laiku aizliegtu jebkurai fiziskai personai, kas ir atbildīga par vadības pienākumu veikšanu galvenās izpildpersonas vai juridiskā pārstāvja līmenī būtiskajā vienībā, veikt vadības funkcijas šajā vienībā.

Pagaidu apturēšanu vai aizliegumu, kas noteikti saskaņā ar šo punktu, piemēro tikai līdz brīdim, kad attiecīgā vienība veic nepieciešamo darbību, lai novērstu trūkumus vai izpildītu kompetentās iestādes prasības, attiecībā uz kurām šāds izpildes panākšanas pasākums piemērots. Šādas pagaidu apturēšanas vai aizlieguma piemērošanā ievēro attiecīgas procesuālās garantijas saskaņā ar vispārīgajiem Savienības tiesību principiem un Hartu, tai skaitā tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, nevainīguma prezumpciju un tiesības uz aizstāvību.

Šajā punktā paredzētos izpildes panākšanas pasākumus nepiemēro valsts pārvaldes vienībām, uz kurām attiecas šī direktīva.

6. Dalībvalstis nodrošina, ka jebkurai fiziskai personai, kura atbild par būtisko vienību vai rīkojas kā būtiskās vienības juridiskā pārstāve, pamatojoties uz pilnvarām to pārstāvēt, pilnvarām pieņemt lēmumus tās vārdā vai pilnvarām īstenot kontroli pār to, ir pilnvaras nodrošināt, ka vienība ievēro šo direktīvu. Dalībvalstis nodrošina, ka šādas fiziskās personas var tikt sauktas pie atbildības, ja viņas pārkāpj savus pienākumus nodrošināt atbilstību šai direktīvai.

Attiecībā uz valsts pārvaldes vienībām šis punkts neskar valstu tiesību aktus par valsts ierēdņu un ievēlētu vai ieceltu amatpersonu atbildību.

7. Veicot jebkuru no izpildes panākšanas pasākumiem, kas minēti 4. vai 5. punktā, kompetentās iestādes ievēro aizstāvības tiesības un ņem vērā katra atsevišķā gadījuma apstākļus, un vismaz pienācīgi ņem vērā:

a) pārkāpuma smagumu un pārkāpto noteikumu nozīmi, ņemot vērā, ka smags pārkāpums cita starpā jebkurā gadījumā ir:

   i) atkārtoti pārkāpumi;

   ii) būtisku incidentu nepaziņošana vai neatrisināšana;

   iii) trūkumu nenovēršana pretēji kompetento iestāžu saistošiem norādījumiem;

   iv) šķēršļu likšana revīzijām vai uzraudzības darbībām, ko uzdevusi kompetentā iestāde pēc pārkāpuma konstatēšanas;

   v) nepatiesas vai ļoti neprecīzas informācijas sniegšana saistībā ar kiberdrošības risku pārvaldības pasākumiem vai ziņošanas pienākumiem, kas noteikti 21. un 23. pantā;

b) pārkāpuma ilgumu;

c) jebkādus relevantus attiecīgās vienības iepriekšējus pārkāpumus;

d) jebkādu izraisīto materiālo vai nemateriālo kaitējumu, tostarp jebkādu finansiālo vai ekonomisko zaudējumu, ietekmi uz citiem pakalpojumiem un skarto lietotāju skaitu;

e) pārkāpuma izdarītāja nodomu vai nolaidību;

f) jebkādus pasākumus, ko vienība veikusi, lai novērstu vai mazinātu materiālo vai nemateriālo kaitējumu;

g) jebkuru apstiprinātu rīcības kodeksu vai apstiprinātu sertifikācijas mehānismu ievērošanu;

h) to, cik lielā mērā pie atbildības sauktās fiziskās vai juridiskās personas sadarbojas ar kompetentajām iestādēm;

8. Kompetentās iestādes savus izpildes panākšanas pasākumus sīki argumentē. Pirms šādu pasākumu pieņemšanas kompetentās iestādes paziņo attiecīgajām vienībām savus sākotnējos konstatējumus. Tās arī dod minētajām vienībām saprātīgu laiku apsvērumu iesniegšanai, izņemot pienācīgi pamatotus gadījumus, kad citādi tiktu kavēta tūlītēja rīcība incidentu novēršanai vai reaģēšanai uz tiem.

9. Dalībvalstis nodrošina, ka to kompetentās iestādes, kas minētas šajā direktīvā, īstenojot savas uzraudzības un izpildes panākšanas pilnvaras, informē attiecīgās tās pašas dalībvalsts kompetentās iestādes, kas minētas Direktīvā (ES) 2022/2557, cenšoties nodrošināt, ka vienība, kas identificēta kā kritiska vienība saskaņā ar Direktīvu (ES) 2022/2557, ievēro šo direktīvu. Attiecīgā gadījumā Direktīvā (ES) 2022/2557 minētās kompetentās iestādes var pieprasīt šajā direktīvā minētajām kompetentajām iestādēm īstenot savas uzraudzības un izpildes panākšanas pilnvaras attiecībā uz vienību, kas ir identificēta kā kritiska vienība saskaņā ar Direktīvu (ES) 2022/2557.

10. Dalībvalstis nodrošina, ka to kompetentās iestādes, kas paredzētas šajā direktīvā, sadarbojas ar attiecīgās dalībvalsts attiecīgajām Regulā (ES) 2022/2554 minētajām kompetentajām iestādēm. Jo īpaši dalībvalstis nodrošina, ka to kompetentās iestādes, kas minētas šajā direktīvā, informē saskaņā ar Regulas (ES) 2022/2554 32. panta 1. punktu izveidoto Pārraudzības forumu, kad tās īsteno savas uzraudzības un izpildes panākšanas pilnvaras, kuru mērķis ir nodrošināt, lai būtiska vienība, kas ir identificēta kā kritiski svarīgu IKT trešo pušu pakalpojumu sniedzēja saskaņā ar Regulas (ES) 2022/2554 31. pantu, ievērotu šo direktīvu.

33. pants

Uzraudzības un izpildes panākšanas pasākumi attiecībā uz svarīgām vienībām

1. Saņemot pierādījumus, norādes vai informāciju par to, ka svarīga vienība, iespējams, neievēro šo direktīvu, jo īpaši tās 21. un 23. pantu, dalībvalstis nodrošina, ka kompetentās iestādes rīkojas, nepieciešamības gadījumā īstenojot *ex post* uzraudzības pasākumus. Dalībvalstis nodrošina, ka minētie pasākumi ir iedarbīgi, samērīgi un atturoši, ņemot vērā apstākļus katrā atsevišķā gadījumā.

2. Dalībvalstis nodrošina, ka kompetentajām iestādēm, kad tās īsteno savus uzraudzības uzdevumus attiecībā uz svarīgām vienībām, ir pilnvaras piemērot minētajām vienībām vismaz:

a) inspekcijas uz vietas un attālinātu *ex post* uzraudzību, ko veic apmācīti speciālisti;

b) mērķtiecīgas drošības revīzijas, ko veic neatkarīga struktūra vai kompetenta iestāde;

c) drošības skenēšanu, pamatojoties uz objektīviem, nediskriminējošiem, taisnīgiem un pārredzamiem riska novērtēšanas kritērijiem, vajadzības gadījumā sadarbībā ar attiecīgo vienību;

d) tādas informācijas pieprasījumus, kas nepieciešama, lai *ex post* novērtētu attiecīgās vienības pieņemtos kiberdrošības risku pārvaldības pasākumus, tostarp dokumentētas kiberdrošības rīcībpolitikas, kā arī atbilstību pienākumam iesniegt informāciju kompetentajām iestādēm atbilstīgi 28. pantam;

e) pieprasījumus piekļūt datiem, dokumentiem un informācijai, kas nepieciešama to uzraudzības uzdevumu izpildei;

f) pieprasījumus par pierādījumiem, ka tiek īstenotas kiberdrošības rīcībpolitikas, piemēram, kvalificēta revidenta veikto drošības revīziju rezultātiem un attiecīgajiem pamatā esošajiem pierādījumiem.

Šā punkta pirmās daļas b) apakšpunktā minēto mērķtiecīgo drošības revīziju pamatā ir riska novērtējumi, ko veic kompetentā iestāde vai revidētā vienība, vai cita ar risku saistīta pieejamā informācija.

Ikvienas mērķtiecīgās drošības revīzijas rezultātus dara pieejamus kompetentajai iestādei. Šādas mērķtiecīgas drošības revīzijas, ko veic neatkarīga struktūra, izmaksas sedz revidētā vienība, izņemot pienācīgi pamatotus gadījumus, kad kompetentā iestāde nolemj citādi.

3. Īstenojot savas pilnvaras saskaņā ar 2. punkta d), e) vai f) apakšpunktu, kompetentās iestādes norāda pieprasījuma mērķi un precizē prasīto informāciju.

4. Dalībvalstis nodrošina, ka kompetentajām iestādēm, īstenojot izpildes panākšanas procedūras attiecībā uz svarīgām vienībām, ir pilnvaras vismaz:

a) izdot brīdinājumus par attiecīgo vienību šīs direktīvas pārkāpumiem;

b) pieņemt saistošus norādījumus vai rīkojumu, pieprasot attiecīgajām vienībām novērst konstatētos trūkumus vai šīs direktīvas pārkāpumus;

c) uzdot attiecīgajām iestādēm izbeigt rīcību, ar ko pārkāpj šo direktīvu, un atturēties no tādas rīcības atkārtošanas;

d) uzdot attiecīgajām vienībām konkrētā veidā un konkrētā laikposmā nodrošināt savu kiberdrošības risku pārvaldības pasākumu atbilstību 21. pantam vai izpildīt ziņošanas pienākumu, kas noteikts 23. pantā;

e) uzdot attiecīgajām vienībām informēt fiziskās vai juridiskās personas, attiecībā uz kurām tās sniedz pakalpojumus vai veic darbības, kuras var ietekmēt būtiski kiberdraudi, par draudu raksturu, kā arī par visiem iespējamajiem aizsardzības vai korektīviem pasākumiem, ko attiecīgās fiziskās vai juridiskās personas var veikt, reaģējot uz šādiem draudiem;

f) uzdot attiecīgajām vienībām saprātīgā termiņā īstenot ieteikumus, kas sniegti drošības revīzijas rezultātā;

g) uzdot attiecīgajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos tiek pārkāpta šī direktīva;

h) piemērot vai pieprasīt, lai attiecīgās struktūras, tiesas vai tribunāli saskaņā ar valsts tiesību aktiem piemēro administratīvu naudas sodu atbilstoši 34. pantam papildus jebkuriem no pasākumiem, kas minēti šā punkta a)–g) apakšpunktā.

5. Šīs direktīvas 32. panta 6., 7. un 8. punktu *mutatis mutandis* piemēro uzraudzības un izpildes panākšanas pasākumiem, kas paredzēti šajā pantā attiecībā uz svarīgajām vienībām.

6. Dalībvalstis nodrošina, ka to kompetentās iestādes, kas paredzētas šajā direktīvā, sadarbojas ar attiecīgās dalībvalsts attiecīgajām Regulā (ES) 2022/2554 minētajām kompetentajām iestādēm. Jo īpaši dalībvalstis nodrošina, ka to kompetentās iestādes, kas minētas šajā direktīvā, informē saskaņā ar Regulas (ES) 2022/2554 32. panta 1. punktu izveidoto Pārraudzības forumu, kad tās īsteno savas uzraudzības un izpildes panākšanas pilnvaras, kuru mērķis ir nodrošināt, lai būtiska vienība, kas ir identificēta kā kritiski svarīgu IKT trešo pušu pakalpojumu sniedzēja saskaņā ar Regulas (ES) 2022/2554 31. pantu, ievērotu šo direktīvu.

34. pants

Vispārīgi nosacījumi administratīvo naudas sodu piemērošanai būtiskajām un svarīgajām vienībām

1. Dalībvalstis nodrošina, ka administratīvie naudas sodi, kas par šīs direktīvas pārkāpumiem piemēroti būtiskajām un svarīgajām vienībām saskaņā ar šo pantu, ir iedarbīgi, samērīgi un atturoši, ņemot vērā katra atsevišķa gadījuma apstākļus.

2. Administratīvos naudas sodus piemēro papildus jebkuram no pasākumiem, kas minēti 32. panta 4. punkta a)–h) apakšpunktā, 32. panta 5. punktā un 33. panta 4. punkta a)–g) apakšpunktā.

3. Izlemjot, vai piemērot administratīvu naudas sodu, un lemjot par tā summu katrā individuālā gadījumā, pienācīgi ņem vērā vismaz 32. panta 7. punktā paredzētos elementus.

4. Dalībvalstis nodrošina, ka tad, ja būtiskās vienības pārkāpj 21. vai 23. pantu, tām saskaņā ar šā panta 2. un 3. punktu piemēro administratīvu naudas sodu maksimāli vismaz 10 000 000 EUR vai maksimāli vismaz 2 % no tā uzņēmuma kopējā globālā apgrozījuma iepriekšējā finanšu gadā, pie kura pieder būtiskā vienība, atkarībā no tā, kura summa ir lielāka.

5. Dalībvalstis nodrošina, ka tad, ja svarīgās vienības pārkāpj 21. vai 23. pantu, tām saskaņā ar šā panta 2. un 3. punktu piemēro administratīvu naudas sodu maksimāli vismaz 7 000 000 EUR vai maksimāli vismaz 1,4 % no tā uzņēmuma kopējā globālā apgrozījuma iepriekšējā finanšu gadā, pie kura pieder svarīgā vienība, atkarībā no tā, kura summa ir lielāka.

6. Dalībvalstis var paredzēt pilnvaras saskaņā ar kompetentās iestādes iepriekšēju lēmumu piemērot periodiskus soda maksājumus, lai piespiestu būtisko vai svarīgo vienību izbeigt šīs direktīvas pārkāpšanu.

7. Neskarot 32. un 33. 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.

8. Ja dalībvalsts tiesību sistēmā nav paredzēti administratīvi naudas sodi, attiecīgā dalībvalsts nodrošina, ka šo pantu piemēro tā, ka naudas sodu ierosina kompetentā iestāde un piemēro valsts kompetentās tiesas vai tribunāli, vienlaikus nodrošinot, ka minētie tiesiskās aizsardzības līdzekļi ir efektīvi un tiem ir tāda pati ietekme kā kompetento iestāžu piemērotiem administratīviem naudas sodiem. Jebkurā gadījumā uzliktie naudas sodi ir iedarbīgi, samērīgi un atturoši. Dalībvalsts līdz 2024. gada 17. oktobrim paziņo Komisijai to tiesību aktu noteikumus, ko tā pieņem saskaņā ar šo punktu, un nekavējoties paziņo par jebkuru turpmāku grozošo aktu vai noteikumu grozījumu.

35. pants

Pārkāpumi, kas ietver persondatu aizsardzības pārkāpumu

1. Ja kompetentajām iestādēm uzraudzības vai izpildes panākšanas gaitā kļūst zināms, ka būtiskas vai svarīgas vienības izdarīts šīs direktīvas 21. un 23. pantā noteikto pienākumu pārkāpums var ietvert persondatu aizsardzības pārkāpumu, kā definēts Regulas (ES) 2016/679 4. panta 12) punktā un kas ir jāpaziņo atbilstoši minētās regulas 33. pantam, tās bez liekas kavēšanās informē uzraudzības iestādes, kā noteikts minētās regulas 55. un 56. pantā.

2. Ja uzraudzības iestādes, kā minēts Regulas (ES) 2016/679 55. vai 56. pantā, piemēro administratīvu naudas sodu saskaņā ar minētās regulas 58. panta 2. punkta i) apakšpunktu, kompetentās iestādes nepiemēro administratīvu naudas sodu saskaņā ar šīs direktīvas 34. pantu par šā panta 1. punktā minēto pārkāpumu, kas izriet no tās pašas rīcības, par kuru ir piemērots administratīvais naudas sods saskaņā ar Regulas (ES) 2016/679 58. panta 2. punkta i) apakšpunktu. Tomēr kompetentās iestādes var noteikt izpildes panākšanas pasākumus, kas paredzēti šīs direktīvas 32. panta 4. punkta a)–h) apakšpunktā, 32. panta 5. punktā un 33. panta 4. punkta a)–g) apakšpunktā.

3. Ja uzraudzības iestāde, kas ir kompetenta atbilstīgi Regulai (ES) 2016/679, ir iedibināta dalībvalstī, kura nav kompetentās iestādes dalībvalsts, kompetentā iestāde informē uzraudzības iestādi, kas ir iedibināta pašas dalībvalstī, par iespējamu 1. punktā minēto datu aizsardzības pārkāpumu.

36. pants

Sodi

Dalībvalstis paredz noteikumus par sodiem, kas piemērojami par to valsts noteikumu pārkāpumiem, kuri pieņemti, ievērojot šo direktīvu, un veic visus nepieciešamos pasākumus, lai nodrošinātu to piemērošanu. Paredzētie sodi ir iedarbīgi, samērīgi un atturoši. Dalībvalstis līdz 2025. gada 17. janvārim dara zināmus minētos noteikumus un pasākumus Komisijai un nekavējoties paziņo tai par jebkādiem turpmākiem grozījumiem, kas tos ietekmē.

37. pants

Savstarpēja palīdzība

1. Ja vienība sniedz pakalpojumus vairāk nekā vienā dalībvalstī vai sniedz pakalpojumus vienā vai vairākās dalībvalstīs un tās tīklu un informācijas sistēmas atrodas vienā vai vairākās citās dalībvalstīs, attiecīgo dalībvalstu kompetentās iestādes vajadzības gadījumā sadarbojas un cita citai palīdz. Minētā sadarbība ietver vismaz turpmāk minēto:

a) kompetentās iestādes, kas piemēro uzraudzības vai izpildes panākšanas pasākumus dalībvalstī, ar vienotā kontaktpunkta starpniecību informē pārējo attiecīgo dalībvalstu kompetentās iestādes un apspriežas ar tām par veiktajiem uzraudzības un izpildes panākšanas pasākumiem;

b) kompetentā iestāde var pieprasīt, lai cita kompetentā iestāde veic uzraudzības vai izpildes panākšanas pasākumus;

c) kompetentā iestāde, saņemot pamatotu lūgumu no citas kompetentās iestādes, sniedz otrai kompetentajai iestādei savstarpēju palīdzību, kas ir proporcionāla pašas rīcībā esošajiem resursiem, lai uzraudzības vai izpildes panākšanas pasākumus varētu īstenot efektīvi, iedarbīgi un konsekventi.

Pirmās daļas c) apakšpunktā minētā savstarpējā palīdzība var ietvert informācijas pieprasījumus un uzraudzības pasākumus, tostarp pieprasījumus veikt inspekcijas uz vietas vai attālinātu uzraudzību, vai mērķtiecīgas drošības revīzijas. Kompetentā iestāde, kurai ir adresēts palīdzības lūgums, neatsaka minēto lūgumu, ja vien netiek konstatēts, ka tā nav kompetenta sniegt pieprasīto palīdzību, pieprasītā palīdzība nav samērīga ar kompetentās iestādes uzraudzības uzdevumiem, vai ja lūgums attiecas uz informāciju vai ir saistīts ar darbībām, kuras, ja tās tiktu izpaustas vai veiktas, būtu pretrunā attiecīgās dalībvalsts būtiskām valsts drošības, sabiedrības drošības vai aizsardzības interesēm. Pirms šāda pieprasījuma noraidīšanas kompetentā iestāde apspriežas ar citām attiecīgajām kompetentajām iestādēm, kā arī – pēc kādas no attiecīgo dalībvalstu pieprasījuma – ar Komisiju un *ENISA*.

2. Attiecīgā gadījumā un pēc kopīgas vienošanās kompetentās iestādes no dažādām dalībvalstīm var veikt kopīgas uzraudzības darbības.

VIII NODAĻA

DELEĢĒTIE UN ĪSTENOŠANAS AKTI

38. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 24. panta 2. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no 2023. gada 16. janvāra.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 24. 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 jau spēkā esošos deleģētos aktus.

4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar ekspertiem ar katras dalībvalsts ieceltajiem ekspertiem 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 24. 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.

39. 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, minēto procedūru izbeidz, nepanākot rezultātu, ja atzinuma sniegšanas termiņā tā nolemj komitejas priekšsēdētājs vai to pieprasa kāds komitejas loceklis.

IX NODAĻA

NOBEIGUMA NOTEIKUMI

40. pants

Pārskatīšana

Komisija līdz 2027. gada 17. oktobrim un pēc tam reizi 36 mēnešos pārskata šīs direktīvas darbību un sniedz ziņojumu Eiropas Parlamentam un Padomei. Ziņojumā jo īpaši novērtē minēto attiecīgo vienību lielumu un I un II pielikumā minētās vienības nozares, apakšnozares un veida nozīmīgumu ekonomikas darbībai un sabiedrībai saistībā ar kiberdrošību. Šajā nolūkā un lai turpinātu attīstīt stratēģisko un operatīvo sadarbību, Komisija ņem vērā sadarbības grupas un *CSIRT* tīkla ziņojumus par stratēģiskā un operatīvā līmenī gūto pieredzi. Ziņojumam vajadzības gadījumā pievieno leģislatīva akta priekšlikumu.

41. pants

Transponēšana

1. Dalībvalstis līdz 2024. gada 17. oktobrim pieņem un publicē noteikumus, kas vajadzīgi, lai izpildītu šīs direktīvas prasības. Dalībvalstis par to tūlīt informē Komisiju.

Tās piemēro minētos aktus no 2024. gada 18. oktobra.

2. Kad dalībvalstis pieņem 1. punktā minētos noteikumus, tajos ietver atsauci uz šo direktīvu vai arī šādu atsauci pievieno to oficiālajai publikācijai. Dalībvalstis nosaka paņēmienus, kā izdarāma šāda atsauce.

42. pants

Grozījums Regulā (ES) Nr. 910/2014

Regulas (ES) Nr. 910/2014 19. pantu svītro no 2024. gada 18. oktobra.

43. pants

Grozījums Direktīvā (ES) 2018/1972

Direktīvas (ES) 2018/1972 40. un 41. pantu svītro no 2024. gada 18. oktobra.

44. pants

Atcelšana

Direktīva (ES) 2016/1148 tiek atcelta no 2024. gada 18. oktobra.

Atsauces uz atcelto direktīvu uzskata par atsaucēm uz šo direktīvu, un tās lasa saskaņā ar atbilstības tabulu III pielikumā.

45. pants

Stāšanās spēkā

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

46. pants

Adresāti

Šī direktīva ir adresēta dalībvalstīm.

Strasbūrā, 2022. gada 14. decembrī

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētāja	*priekšsēdētājs*
R. METSOLA	M. BEK

I PIELIKUMS

SEVIŠĶI KRITISKĀS NOZARES

Nozare	Apakšnozare	Vienības veids
1. Enerģētika	a) Elektroenerģija	— Elektroenerģijas uzņēmumi, kā definēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/944 ([1]) 2. panta 57. punktā un kas pilda piegādes funkciju, kā definēts minētās direktīvas 2. panta 12) punktā
		— Sadales sistēmu operatori, kā definēts Direktīvas (ES) 2019/944 2. panta 29) punktā
		— Pārvades sistēmu operatori, kā definēts Direktīvas (ES) 2019/944 2. panta 35) punktā
		— Ražotāji, kā definēts Direktīvas (ES) 2019/944 2. panta 38) punktā
		— Nominēti elektroenerģijas tirgus operatori, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2019/943 ([2]) 2. panta 8) punktā; — Tirgus dalībnieki, kā definēts Regulas (ES) 2019/943 2. panta 25) punktā un kas sniedz agregēšanas, pieprasījumreakcijas vai enerģijas uzkrāšanas pakalpojumus, kā definēts Direktīvas (ES) 2019/944 2. panta 18), 20) un 59) punktā — Uzlādes punkta operatori, kas atbild par tāda uzlādes punkta pārvaldību un ekspluatāciju, kurš galalietotājiem sniedz uzlādes pakalpojumu, arī mobilitātes pakalpojuma sniedzēja vārdā un uzdevumā
	b) Centralizēta siltumapgāde un aukstumapgāde	— Centralizētas siltumapgādes un aukstumapgādes operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2018/2001 ([3]) 2. panta 19) punktā
	c) Nafta	— Naftas pārvades cauruļvadu operatori
		— Naftas ražošanas operatori, pārstrādes un attīrīšanas iekārtas, uzglabāšana un pārvade
		— Centrālās krājumu uzturēšanas struktūras, kā definēts Direktīvas 2009/119/EK ([4]) 2. panta f) punktā
	d) Gāze	— Piegādes uzņēmumi, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2009/73/EK ([5]) 2. panta 8) punktā
		— Sadales sistēmu operatori, kā definēts Direktīvas 2009/73/EK 2. panta 6) punktā
		— Pārvades sistēmu operatori, kā definēts Direktīvas 2009/73/EK 2. panta 4) punktā
		— Uzglabāšanas sistēmas operatori, kā definēts Direktīvas 2009/73/EK 2. panta 10) punktā
		— SDG sistēmas operatori, kā definēts Direktīvas 2009/73/EK 2. panta 12) punktā
		— Dabasgāzes uzņēmumi, kā definēts Direktīvas 2009/73/EK 2. panta 1) punktā
		— Dabasgāzes pārstrādes un attīrīšanas iekārtu operatori
	e) Ūdeņradis	— Ūdeņraža ražošanas, uzglabāšanas un pārvades operatori

Nozare	Apakšnozare	Vienības veids
2. Transports	a) Gaisa transports	— Gaisa pārvadātāji, kā definēts Regulas (EK) Nr. 300/2008 3. panta 4) punktā un ko izmanto komerciālos nolūkos
		— Lidostu pārvaldības struktūras, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2009/12/EK ([6]) 2. panta 2) punktā, lidostas, kā definēts minētās direktīvas 2. panta 1) punktā, tostarp galvenās lidostas, kas uzskaitītas Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1315/2013 ([7]) II pielikuma 2. iedaļā, un vienības, kuras nodarbojas ar tādu palīgiekārtu ekspluatāciju, kas atrodas lidostās
		— Satiksmes vadības kontroles operatori, kuri sniedz gaisa satiksmes vadības (ATC) pakalpojumu, kā definēts Eiropas Parlamenta un Padomes Regulas (EK) Nr. 549/2004 ([8]) 2. panta 1) punktā
	b) Dzelzceļa transports	— Infrastruktūras pārvaldītāji, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2012/34/ES ([9]) 3. panta 2) punktā
		— Dzelzceļa pārvadājumu uzņēmumi, kā definēts Direktīvas 2012/34/ES 3. panta 1) punktā, tostarp apkalpes vietas operatori, kā definēts minētās direktīvas 3. panta 12) punktā
	c) Ūdens transports	— Iekšējo, jūras un piekrastes ūdens transporta pasažieru un kravu pārvadājumu uzņēmumi, kā attiecībā uz jūras transportu definēts Eiropas Parlamenta un Padomes Regulas (EK) Nr. 725/2004 ([10]) I pielikumā, neietverot atsevišķos kuģus, kurus ekspluatē minētie uzņēmumi
		— Tādu ostu pārvaldības struktūras, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2005/65/EK ([11]) 3. panta 1) punktā, tostarp to ostas iekārtas, kā definēts Regulas (EK) Nr. 725/2004 2. panta 11) punktā, un vienības, kas ekspluatē rūpnīcas un iekārtas, kuras atrodas ostās
		— Tādu kuģu satiksmes dienestu operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2002/59/EK ([12]) 3. panta o) punktā
	d) Auto-transports	— Par autoceļiem atbildīgās iestādes, kā definēts Komisijas Deleģētās regulas (ES) 2015/962 ([13]) 2. panta 12) punktā un kuras ir atbildīgas par satiksmes pārvaldības kontroli, izņemot publiskas vienības, attiecībā uz kurām satiksmes pārvaldība vai intelektisko transporta sistēmu vadība ir tikai nebūtiska to vispārējās darbības daļa
		— Tādu intelektisko transporta sistēmu operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2010/40/ES ([14]) 4. panta 1) punktā
3. Banku pakalpojumi		Kredītiestādes, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 575/2013 ([15]) 4. panta 1) punktā
4. Finanšu tirgus infrastruktūras		— Tādu tirdzniecības vietu operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2014/65/ES ([16]) 4. panta 24) punktā
		— Centrālie darījumu partneri (CCP), kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 648/2012 ([17]) 2. panta 1) punktā

Nozare	Apakšnozare	Vienības veids
5. Veselība		— Veselības aprūpes sniedzēji, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2011/24/ES ([18]) 3. panta g) punktā
		— ES references laboratorijas, kas minētas Eiropas Parlamenta un Padomes Regulas (ES) 2022/2371 ([19]) 15. pantā
		— Vienības, kuras veic izpētes un izstrādes darbības attiecībā uz zālēm, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2001/83/EK ([20]) 1. panta 2) punktā; — Vienības, kas ražo farmaceitiskās pamatvielas un farmaceitiskos preparātus, kuri minēti *NACE* 2. red. C sadaļas 21. nodaļā — Vienības, kas ražo medicīniskās ierīces, kuras uzskata par kritiski svarīgām sabiedrības veselības ārkārtas situācijas laikā (sabiedrības veselības ārkārtas situācijas kritiski svarīgo ierīču saraksts) Eiropas Parlamenta un Padomes Regulas (ES) 2022/123 ([21]) 22. panta nozīmē
6. Dzeramais ūdens		Dzeramā ūdens, kā definēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2020/2184 ([22]) 2. panta 1. punkt a) apakšpunktā, piegādātāji un izplatītāji, izslēdzot izplatītājus, kuriem dzeramā ūdens izplatīšana ir nebūtiska daļa no to veiktās patēriņa preču un pārējo preču izplatīšanas vispārējās darbības
7. Notekūdeņi		Uzņēmumi, kas savāc, utilizē vai attīra komunālos notekūdeņus, sadzīves notekūdeņus vai rūpnieciskos notekūdeņus, kā definēts Padomes Direktīvas 91/271/EEK ([23]) 2. panta 1), 2) un 3) punktā, izņemot uzņēmumus, kuriem komunālo notekūdeņu, sadzīves notekūdeņu vai rūpniecisko notekūdeņu savākšana, utilizēšana vai attīrīšana ir nebūtiska to vispārējās darbības daļa
8. Digitālā infrastruktūra		— Interneta plūsmu apmaiņas punktu nodrošinātāji
		— DNS pakalpojumu sniedzēji, izņemot saknes nosaukuma serveru operatorus
		— ALD nosaukumu reģistri
		— Mākoņpakalpojumu sniedzēji
		— Datu centru pakalpojumu sniedzēji
		— Satura piegādes tīklu nodrošinātāji
		— Uzticamības pakalpojuma sniedzēji
		— Publisko elektronisko sakaru tīklu nodrošinātāji
		— Publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji
9. IKT pakalpojumu pārvaldība (uzņēmumu darījumi ar uzņēmumiem)		— Pārvaldītu pakalpojumu sniedzēji — Pārvaldītu drošības pakalpojumu sniedzēji

Nozare	Apakšnozare	Vienības veids
10. Valsts pārvalde		— Centrālo valdību valsts pārvaldes vienības, ko definējusi dalībvalsts saskaņā ar valsts tiesību aktiem
		— Reģionālā līmeņa valsts pārvaldes vienības, ko definējusi dalībvalsts saskaņā ar valsts tiesību aktiem
11. Kosmoss		Zemes infrastruktūras, kas pieder dalībvalstīm vai privātā sektora personām vai ko pārvalda un ekspluatē dalībvalstis vai privātā sektora personas, operatori, kas atbalsta kosmosā izvietotu pakalpojumu sniegšanu, izņemot publisko elektronisko sakaru tīklu nodrošinātājus

([1]) Eiropas Parlamenta un Padomes Direktīva (ES) 2019/944 (2019. gada 5. jūnijs) par kopīgiem noteikumiem attiecībā uz elektroenerģijas iekšējo tirgu un ar ko groza Direktīvu 2012/27/ES (OV L 158, 14.6.2019., 125. lpp.).

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2019/943 (2019. gada 5. jūnijs) par elektroenerģijas iekšējo tirgu (OV L 158, 14.6.2019., 54. lpp.).

([3]) Eiropas Parlamenta un Padomes Direktīva (ES) 2018/2001 (2018. gada 11. decembris) par no atjaunojamajiem energoresursiem iegūtas enerģijas izmantošanas veicināšanu (OV L 328, 21.12.2018., 82. lpp.).

([4]) Padomes Direktīva 2009/119/EK (2009. gada 14. septembris), ar ko dalībvalstīm uzliek pienākumu uzturēt jēlnaftas un/vai naftas produktu obligātas rezerves (OV L 265, 9.10.2009., 9. lpp.).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(19) Eiropas Parlamenta un Padomes Regula (ES) 2022/2371 (2022. gada 23. novembris) par nopietniem pārrobežu veselības apdraudējumiem un ar ko atceļ Lēmumu Nr. 1082/2013/ES (OV L 314, 6.12.2022., 26. lpp.).

(20) Eiropas Parlamenta un Padomes Direktīva 2001/83/EK (2001. gada 6. novembris) par Kopienas kodeksu, kas attiecas uz cilvēkiem paredzētām zālēm (OV L 311, 28.11.2001., 67. lpp.).

(21) Eiropas Parlamenta un Padomes Regula (ES) 2022/123 (2022. gada 25. janvāris) par pastiprinātu Eiropas Zāļu aģentūras lomu attiecībā uz zālēm un medicīniskajām ierīcēm krīžgatavības un krīžu pārvarēšanas kontekstā (OV L 20, 31.1.2022., 1. lpp.).

(22) Eiropas Parlamenta un Padomes Direktīva (ES) 2020/2184 (2020. gada 16. decembris) par dzeramā ūdens kvalitāti (OV L 435, 23.12.2020., 1. lpp.).

(23) Padomes Direktīva 91/271/EEK (1991. gada 21. maijs) par komunālo notekūdeņu attīrīšanu (OV L 135, 30.5.1991., 40. lpp.).

II PIELIKUMS

CITAS KRITISKĀS NOZARES

Nozare	Apakšnozare	Vienības veids
1. Pasta un kurjeru pakalpojumi		Tādu pasta pakalpojumu sniedzēji, kā definēts Direktīvas 97/67/EK 2. panta 1.a punktā, tostarp kurjeru pakalpojumu sniedzēji
2. Atkritumu apsaimniekošana		Uzņēmumi, kas veic atkritumu apsaimniekošanu, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2008/98/EK ([1]) 3. panta 9) punktā, izņemot uzņēmumus, kuriem atkritumu apsaimniekošana nav to galvenā saimnieciskā darbība
3. Ķimikāliju izgatavošana, ražošana un izplatīšana		Uzņēmumi, kas veic vielu ražošanu un vielu vai maisījumu izplatīšanu, kā minēts Eiropas Parlamenta un Padomes Regulas (EK) Nr. 1907/2006 ([2]) 3. panta 9) un 14) punktā, un uzņēmumi, kas ražo izstrādājumus no vielām vai maisījumiem, kā definēts minētās regulas 3. panta 3) punktā
4. Pārtikas ražošana, pārstrāde un izplatīšana		Pārtikas uzņēmumi, kā definēts Eiropas Parlamenta un Padomes Regulas (EK) Nr. 178/2002 ([3]) 3. panta 2) punktā un kas nodarbojas ar izplatīšanu vairumtirdzniecībā, rūpniecisko ražošanu un pārstrādi
5. Ražošana	a) Medicīnisko ierīču un *in vitro* diagnostikas medicīnisko ierīču ražošana	Vienības, kuras ražo medicīniskas ierīces, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2017/745 ([4]) 2. panta 1) punktā, un vienības, kuras ražo *in vitro* diagnostikas medicīniskas ierīces, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2017/746 ([5]) 2. panta 2) punktā, izņemot vienības, kuras ražo šīs direktīvas I pielikuma 5. punkta piektajā ievilkumā minētās medicīniskās ierīces
	b) Datoru, elektronisko un optisko iekārtu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. C sadaļas 26. nodaļā
	c) Elektrisko iekārtu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. C sadaļas 27. nodaļā
	d) Citur neklasificētu iekārtu, mehānismu un darba mašīnu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. C sadaļas 28. nodaļā
	e) Automobiļu, piekabju un puspiekabju ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. C sadaļas 29. nodaļā
	f) Citu transportlīdzekļu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. C sadaļas 30. nodaļā

Nozare	Apakšnozare	Vienības veids
6. Digitālo pakalpojumu sniedzēji		— Tiešsaistes tirdzniecības vietu nodrošinātāji
		— Tiešsaistes meklētājprogrammu nodrošinātāji
		— Sociālās tīklošanās pakalpojumu platformu nodrošinātāji
7. Pētniecība		Pētniecības organizācijas

([1]) Eiropas Parlamenta un Padomes Direktīva 2008/98/EK (2008. gada 19. novembris) par atkritumiem un par dažu direktīvu atcelšanu (OV L 312, 22.11.2008., 3. lpp.).

([2]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 1907/2006 (2006. gada 18. decembris), kas attiecas uz ķimikāliju reģistrēšanu, vērtēšanu, licencēšanu un ierobežošanu (*REACH*), un ar kuru izveido Eiropas Ķimikāliju aģentūru, groza Direktīvu 1999/45/EK un atceļ Padomes Regulu (EEK) Nr. 793/93 un Komisijas Regulu (EK) Nr. 1488/94, kā arī Padomes Direktīvu 76/769/EEK un Komisijas Direktīvu 91/155/EEK, Direktīvu 93/67/EEK, Direktīvu 93/105/EK un Direktīvu 2000/21/EK (OV L 396, 30.12.2006., 1. lpp.).

([3]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 178/2002 (2002. gada 28. janvāris), ar ko paredz pārtikas aprites tiesību aktu vispārīgus principus un prasības, izveido Eiropas Pārtikas nekaitīguma iestādi un paredz procedūras saistībā ar pārtikas nekaitīgumu (OV L 31, 1.2.2002., 1. lpp.).

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2017/745 (2017. gada 5. aprīlis), kas attiecas uz medicīniskām ierīcēm, ar ko groza Direktīvu 2001/83/EK, Regulu (EK) Nr. 178/2002 un Regulu (EK) Nr. 1223/2009 un atceļ Padomes Direktīvas 90/385/EEK un 93/42/EEK (OV L 117, 5.5.2017., 1. lpp.).

([5]) Eiropas Parlamenta un Padomes Regula (ES) 2017/746 (2017. gada 5. aprīlis) par *in vitro* diagnostikas medicīniskām ierīcēm un ar ko atceļ Direktīvu 98/79/EK un Komisijas Lēmumu 2010/227/ES (OV L 117, 5.5.2017., 176. lpp.).

III PIELIKUMS

ATBILSTĪBAS TABULA

Direktīva (ES) 2016/1148	Šī direktīva
1. panta 1. punkts	1. panta 1. punkts
1. panta 2. punkts	1. panta 2. punkts
1. panta 3. punkts	—
1. panta 4. punkts	2. panta 12. punkts
1. panta 5. punkts	2. panta 13. punkts
1. panta 6. punkts	2. panta 6. un 11. punkts
1. panta 7. punkts	4. pants
2. pants	2. panta 14. punkts
3. pants	5. pants
4. pants	6. pants
5. pants	—
6. pants	—
7. panta 1. punkts	7. panta 1. un 2. punkts
7. panta 2. punkts	7. panta 4. punkts
7. panta 3. punkts	7. panta 3. punkts
8. panta 1. līdz 5. punkts	8. panta 1. līdz 5. punkts
8. panta 6. punkts	13. panta 4. punkts
8. panta 7. punkts	8. panta 6. punkts
9. panta 1., 2. un 3. punkts	10. panta 1., 2. un 3. punkts
9. panta 4. punkts	10. panta 9. punkts
9. panta 5. punkts	10. panta 10. punkts
10. panta 1., 2. punkts un 3. punkta pirmā daļa	13. panta 1., 2. un 3. punkts
10. panta 3. punkta otrā daļa	23. panta 9. punkts
11. panta 1. punkts	14. panta 1. un 2. punkts
11. panta 2. punkts	14. panta 3. punkts
11. panta 3. punkts	14. panta 4. punkta pirmās daļas a) līdz q) apakšpunkti un s) apakšpunkts, un 7. punkts
11. panta 4. punkts	14. panta 4. punkta pirmās daļas r) apakšpunkts un otrā daļa
11. panta 5. punkts	14. panta 8. punkts
12. panta 1. līdz 5. punkts	15. panta 1. līdz 5. punkts
13. pants	17. pants
14. panta 1. un 2. punkts	21. panta 1. līdz 4. punkts
14. panta 3. punkts	23. panta 1. punkts
14. panta 4. punkts	23. panta 3. punkts
14. panta 5. punkts	23. panta 5., 6. un 8. punkts

Direktīva (ES) 2016/1148	Šī direktīva
14. panta 6. punkts	23. panta 7. punkts
14. panta 7. punkts	23. panta 11. punkts
15. panta 1. punkts	31. panta 1. punkts
15. panta 2. punkta pirmās daļas a) apakšpunkts	32. panta 2. punkta e) apakšpunkts
15. panta 2. punkta pirmās daļas b) apakšpunkts	32. panta 2. punkta g) apakšpunkts
15. panta 2. punkta otrā daļa	32. panta 3. punkts
15. panta 3. punkts	32. panta 4. punkta b) apakšpunkts
15. panta 4. punkts	31. panta 3. punkts
16. panta 1.un 2. punkts	21. panta 1. līdz 4. punkts
16. panta 3. punkts	23. panta 1. punkts
16. panta 4. punkts	23. panta 3. punkts
16. panta 5. punkts	—
16. panta 6. punkts	23. panta 6. punkts
16. panta 7. punkts	23. panta 7. punkts
16. panta 8. un 9. punkts	21. panta 5. punkts un 23. panta 11. punkts
16. panta 10. punkts	—
16. panta 11. punkts	2. panta 1., 2. un 3. punkts
17. panta 1. punkts	33. panta 1. punkts
17. panta 2. punkta a) apakšpunkts	32. panta 2. punkta e) apakšpunkts
17. panta 2. punkta b) apakšpunkts	32. panta 4. punkta b) apakšpunkts
17. panta 3. punkts	37. panta 1. punkta a) un b) apakšpunkts
18. panta 1. punkts	26. panta 1. punkta b) apakšpunkts un 2. punkts
18. panta 2. punkts	26. panta 3. punkts
18. panta 3. punkts	26. panta 4. punkts
19. pants	25. pants
20. pants	30. pants
21. pants	36. pants
22. pants	39. pants
23. pants	40. pants
24. pants	—
25. pants	41. pants
26. pants	45. pants
27. pants	46. pants
I pielikuma 1. punkts	11. panta 1. punkts
I pielikuma 2. punkta a) apakšpunkta i) līdz iv) punkts	11. panta 2. punkta a) līdz d) apakšpunkts

Direktīva (ES) 2016/1148	Šī direktīva
I pielikuma 2. punkta a) apakšpunkta v) punkts	11. panta 2. punkta f) apakšpunkts
I pielikuma 2. punkta b) apakšpunkts	11. panta 4. punkts
I pielikuma 2. punkta c) apakšpunkta i) līdz ii) punkts	11. panta 5. punkta a) apakšpunkts
II pielikums	I pielikums
III pielikuma 1. un 2. punkts	II pielikuma 6. punkts
III pielikuma 3. punkts	I pielikuma 8. punkts