Eiropas Savienības
Padome

Briselē, 2021. gada 26. novembrī
(OR. en)

14337/21

Starpiestāžu lieta:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

PIEZĪME

Sūtītājs:	Padomes Ģenerālsekretariāts
Saņēmējs:	Padome
Iepr. dok. Nr.:	9583/2/21, 11724/21
K-jas dok. Nr.:	14150/20
Temats:	Priekšlikums – Eiropas Parlamenta un Padomes Direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu 2016/1148 *– vispārēja pieeja*

I. IEVADS

1. Komisija 2020. gada 16. decembrī pieņēma priekšlikumu direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā (pārskatīta TID direktīva jeb "TID 2") [1], ar mērķi aizstāt pašreizējo Direktīvu par tīklu un informācijas sistēmu drošību ("TID direktīva") [2].

[1] Priekšlikums – Eiropas Parlamenta un Padomes Direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148.

[2] Eiropas Parlamenta un Padomes Direktīva 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

Priekšlikums bija viena no darbībām, kas paredzētas ES kiberdrošības stratēģijā digitālajai desmitgadei [3], lai nodrošinātu, ka iedzīvotāji un uzņēmumi gūst labumu no uzticamām digitālajām tehnoloģijām.

2. Priekšlikuma pamatā ir Līguma par Eiropas Savienības darbību (LESD) 114. pants, un tā mērķis ir vēl vairāk uzlabot publisko un privāto vienību, kompetento iestāžu un visas Savienības noturību un spēju reaģēt uz incidentiem.

3. Eiropas Parlamentā par priekšlikumu atbildīgā komiteja ir Rūpniecības, pētniecības un enerģētikas komiteja (*ITRE*). *ITRE* komiteja 2021. gada 28. oktobrī pieņēma referenta ziņojumu.

4. Eiropas Ekonomikas un sociālo lietu komiteja 2021. gada 28. aprīlī pieņēma savu atzinumu.

5. Pastāvīgo pārstāvju komiteja 2021. gada 3. februārī nolēma par priekšlikumu apspriesties ar Eiropas Reģionu komiteju [4]. Līdz šim Eiropas Reģionu komiteja savu atzinumu nav sniegusi.

6. Eiropas Datu aizsardzības uzraudzītājs 2021. gada 11. martā sniedza savu atzinumu [5].

7. Savos 2021. gada 22. marta secinājumos par ES kiberdrošības stratēģiju digitālajai desmitgadei [6] Padome ņēma vērā jauno priekšlikumu, kura pamatā ir TID direktīva, un atkārtoti pauda atbalstu valstu kiberdrošības satvaru stiprināšanai un saskaņošanai un noturīgai sadarbībai starp dalībvalstīm.

8. Eiropadome 2021. gada 21. un 22. oktobra secinājumos aicināja virzīt uz priekšu darbu pie priekšlikuma pārskatītai TID direktīvai.

---

[3] 14133/20.
[4] 5573/21.
[5] Atzinums 5/2021 par kiberdrošības stratēģiju un TID 2.0 direktīvu.
[6] 6722/21.

II. DARBS PADOMES DARBA SAGATAVOŠANAS STRUKTŪRĀS

9. Padomē priekšlikumu izskatīja Kiberjautājumu horizontālā darba grupa (turpmāk – "*HWPCI*"). Priekšlikuma izskatīšana sākās Portugāles prezidentūras laikā 19. janvārī ar rūpīgu priekšlikuma caurskatīšanu, dodot dalībvalstīm iespēju izklāstīt savus jautājumus un norādīt galvenās bažas, kā arī no Komisijas saņemt detalizētus skaidrojumus par pārskatītajā direktīvā veiktajām izmaiņām.

10. Portugāles prezidentūras laikā priekšlikuma izklāstīšanai un caurskatīšanai *HWPCI* veltīja 17 sanāksmes. 2021. gada 4. jūnijā TTE padomei tika iesniegts caurskatīšanas progresa ziņojums.

11. Kopš tā laika darbs ir turpinājies un Slovēnijas prezidentūras laikā kļuvis intensīvāks, lai Padomes (Transports, telekomunikācijas un enerģētika) 2021. gada 3. decembra sanāksmē panāktu vispārēju pieeju. Prezidentvalsts Slovēnija TID 2 priekšlikuma pārskatīšanai ir veltījusi 15 sanāksmes un daudzas divpusējas diskusijas visos līmeņos.

12. *HWPCI* savā darbā koncentrējās uz priekšlikuma teksta pārstrādāšanu vispirms attiecībā uz TID 2 direktīvas mijiedarbību ar nozaru tiesību aktiem un tās darbības jomu, jo īpaši attiecībā uz valsts pārvaldi, DNS saknes serveriem un izslēgšanas noteikumu, un pēc tam cita starpā arī uz salīdzinošo izvērtēšanu, jurisdikciju un savstarpēju palīdzību, koordinētu neaizsargātības atklāšanu, domēnu nosaukumu un reģistrācijas datu datubāzēm un starptautisko sadarbību.

13. Pirmais kompromisa priekšlikums par ierosinātās direktīvas tekstu tika izdots 2021. gada 21. septembrī [7], pamatojoties uz rakstiskajiem komentāriem un neoficiāliem dokumentiem, kas bija saņemti no dalībvalstīm, kā arī iepriekšējiem kompromisa priekšlikumiem par TID 2 direktīvas mijiedarbību ar nozaru tiesību aktiem un TID 2 direktīvas darbības jomu.

[7] 12019/21.

14. Prezidentvalsts sagatavotā kompromisa priekšlikuma jaunākā pārskatītā versija [8] tika apspriesta darba grupā 2021. gada 22. novembrī. Delegācijas kopumā kompromisa tekstu novērtēja atzinīgi, taču dažām delegācijām joprojām bija izpētes atrunas vai komentāri par atsevišķām kompromisa priekšlikuma daļām. Noteiktās teksta daļās joprojām tika ierosināts veikt dažas tehniskas izmaiņas.

III. SATURS

15. Pamatojoties uz diskusijām darba grupā, par galvenajiem politiskajiem jautājumiem ir atzīti turpmāk minētie punkti.

a) Darbības joma (2. pants)

Kopš diskusiju sākuma par TID 2 priekšlikumu dalībvalstis galvenokārt bažas paudušas par to, ka ievērojami palielināts to vienību skaits, uz kurām attiecas direktīva, un jo īpaši par maksimālā lieluma noteikuma ieviešanu, saskaņā ar kuru direktīvas darbības jomā ietilpst visas vidējās un lielās vienības, kas darbojas nozarēs vai sniedz pakalpojumus, uz kuriem attiecas TID 2 direktīva. Lai gan kompromisa priekšlikumā šis vispārējais noteikums ir saglabāts, tajā ir iekļauti papildu noteikumi, lai nodrošinātu nepieciešamo proporcionalitāti, augstāku riska pārvaldības līmeni un skaidrus svarīguma kritērijus, pēc kuriem nosaka vienības, kuras ietilpst direktīvas darbības jomā. Turklāt kompromisa priekšlikumā ir iekļauti konkrēti noteikumi par prioritāšu noteikšanu uzraudzības pasākumu izmantošanā saskaņā ar pieeju, kas balstīta uz risku.

[8] 12019/5/21 REV 5.

b) Valsts pārvalde (2. panta 2.a punkts)

Valsts pārvaldes iekļaušana TID 2 direktīvas darbības jomā ir jautājums, par kuru tika ļoti daudz debatēts, ņemot vērā to, ka valsts pārvaldes sektors ir atšķirīgāks par citām nozarēm, uz kurām attiecas TID 2 direktīva. Prezidentvalsts ir centusies rast līdzsvarotu pieeju, kurā ņemtas vērā valsts pārvaldes sistēmu īpatnības un ar kuru nodrošina, ka dalībvalstīm ir zināma elastība, kad jānosaka tās valsts pārvaldes vienības, kuras ietilpst TID 2 darbības jomā. Tādēļ kompromisa tekstā TID 2 attiecas uz centrālo valdību publiskās pārvaldes vienībām, taču dalībvalstis var arī noteikt, ka direktīva attiecas uz valsts pārvaldes vienībām reģionālā un vietējā līmenī.

c) Izslēgšanas noteikums (2. panta 3.a un 3.aa punkts)

Dalībvalstis vēlējās vēl vairāk precizēt izslēgšanas noteikumu, proti, ka direktīvu nepiemēro vienībām, kas galvenokārt darbojas aizsardzības, valsts drošības, sabiedriskās drošības vai tiesībaizsardzības jomā, vai darbībām attiecībā uz valsts drošību vai aizsardzību. Direktīva neattiecas arī uz tiesu iestādēm, parlamentiem un centrālajām bankām.

d) Mijiedarbība ar nozaru tiesību aktiem

Dalībvalstis uzsvēra, ka TID 2 direktīva ir jāsaskaņo ar nozaru tiesību aktiem, jo īpaši Regulu par finanšu sektora digitālās darbības noturību ("*DORA*") un Direktīvu par kritisko vienību noturību ("*CER*" direktīva). TID 2 direktīvā, kurai vajadzētu būt par pamatu minimālajai saskaņošanai kiberdrošības jomā, ir iekļauts īpašs pants par nozarspecifiskiem Savienības aktiem (2.b pants). Attiecībā uz mijiedarbību ar *CER* direktīvu kompromisa priekšlikums nodrošina lielāku skaidrību par "visu apdraudējumu" pieeju. Citi svarīgi papildinājumi ir saistīti ar kompetento iestāžu sadarbības mehānismiem saskaņā ar attiecīgajiem tiesību aktiem.

e) Savstarpēja mācīšanās (16. pants)

Ar dažiem izņēmumiem dalībvalstis iebilda pret to, ka Komisija nosaka obligātu salīdzinošo izvērtēšanu. Ierosinātais kompromiss nodrošina, ka jaunais savstarpējas mācīšanās mehānisms balstās uz savstarpēju uzticēšanos un ir brīvprātīgs un dalībvalstu virzīts process.

f) Jurisdikcija un teritorialitāte (24. pants) un savstarpēja palīdzība (34. pants)

Dalībvalstis ir paudušas bažas par sekām, kas rodas, ja attiecībā uz vienībām IKT nozarē ir diferencēta jurisdikcija, kā to ierosinājusi Komisija. Kompromisa tekstā jurisdikcija ir precizēta, pamatojoties uz vienību veidu, kā arī ir nostiprināts formulējums par savstarpējo palīdzību.

g) Ziņošanas pienākumi (20. pants)

Ņemot vērā dalībvalstu paustās bažas par to, ka tas pārmērīgi noslogotu vienības, uz kurām attiecas TID 2 direktīva, un novestu pie pārmērīgas ziņošanas, kompromisa tekstā nav iekļauta obligātā ziņošana par nozīmīgiem kiberdraudiem.

IV. NOBEIGUMS

16. Pastāvīgo pārstāvju komiteja 2021. gada 24. novembrī panāca vienošanos par pielikumā izklāstīto kompromisa tekstu un nolēma to iesniegt Padomei (Transports, telekomunikācijas un enerģētika), lai tā pieņemtu vispārēju pieeju.

17. Tādēļ Padome tiek aicināta apstiprināt prezidentvalsts iesniegto kompromisa tekstu, kas izklāstīts pielikumā, un 2021. gada 3. decembra sanāksmē pieņemt vispārēju pieeju.

PIELIKUMS

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA,

ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu [9],

ņemot vērā Reģionu komitejas atzinumu [10],

saskaņā ar parasto likumdošanas procedūru,

[9] OV C [..], [..], [..]. lpp.
[10] OV C [..], [..], [..]. lpp.

tā kā:

(1) Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/1148 [11] mērķis bija veidot kiberdrošības spējas Savienībā, mazinot draudus tīklu un informācijas sistēmām, ko izmanto pamatpakalpojumu sniegšanai galvenajās nozarēs, un nodrošinot šādu pakalpojumu nepārtrauktību, kad notiek kiberdrošības incidenti, tādējādi sniedzot ieguldījumu Savienības ekonomikas un sabiedrības efektīvā darbībā.

(2) Kopš Direktīvas (ES) 2016/1148 stāšanās spēkā ir panākts ievērojams progress Savienības kiberdrošības noturības līmeņa paaugstināšanā. Minētās direktīvas pārskatīšana apliecināja, ka direktīva ir bijusi kā katalizators institucionālajai un regulatīvajai pieejai attiecībā uz kiberdrošību Savienībā, bruģējot ceļu būtiskām pārmaiņām domāšanas veidā. Direktīva ir nodrošinājusi valstu regulējumu pabeigšanu, nosakot valsts [...] stratēģijas **par tīklu un informācijas sistēmu drošību**, veidojot valstu spējas un īstenojot regulatīvus pasākumus, kas aptver būtiskas infrastruktūras un dalībniekus, kurus noteikusi katra dalībvalsts. Tā ir arī veicinājusi sadarbību Savienības līmenī, izveidojot sadarbības grupu [12] un valstu datordrošības incidentu reaģēšanas vienību tīklu ("*CSIRT* tīkls") [13]. Neraugoties uz šiem sasniegumiem, Direktīvas (ES) 2016/1148 pārskatīšanā ir konstatētas nepilnības, kas liedz tai efektīvi risināt pašreizējās un jaunās kiberdrošības problēmas.

---

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

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

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

(3) Tīklu un informācijas sistēmas ir kļuvušas par būtisku ikdienas dzīves iezīmi, ko raksturo ātra digitālā pārveide un sabiedrības savstarpējā savienotība, tai skaitā pārrobežu apmaiņa. Šīs attīstības rezultātā ir paplašinājusies kiberdraudu aina, radot jaunas problēmas, attiecībā uz kurām ir vajadzīgi pielāgoti, koordinēti un inovatīvi reaģēšanas pasākumi visās dalībvalstīs. Kiberdrošības incidentu skaits, apmērs, sarežģītība, biežums un ietekme pieaug un rada būtiskus draudus tīklu un informācijas sistēmu darbībai. Rezultātā kiberincidenti var kavēt saimniecisko darbību īstenošanu iekšējā tirgū, radīt finansiālus zaudējumus, apdraudēt lietotāju uzticēšanos un radīt lielu kaitējumu Savienības ekonomikai un sabiedrībai. Tāpēc sagatavotība kiberdrošības jomā un efektivitāte tagad iekšējā tirgus pienācīgai darbībai ir vēl svarīgākas nekā jebkad iepriekš.

(4) Direktīvas (ES) 1148/2016 juridiskais pamats bija Līguma par Eiropas Savienības darbību (LESD) 114. pants, kura mērķis ir iekšējā tirgus izveide un darbība, uzlabojot pasākumus valstu regulējumu tuvināšanai. Kiberdrošības prasības, kas noteiktas vienībām, kuras sniedz pakalpojumus vai veic ekonomiski svarīgas darbības, ievērojami atšķiras starp dalībvalstīm prasību veida, to detalizācijas līmeņa un uzraudzības metodes ziņā. Minētās atšķirības rada papildu izmaksas un grūtības uzņēmumiem, kas piedāvā pārrobežu preces vai pakalpojumus. Prasības, ko nosaka viena dalībvalsts un kas atšķiras no citas dalībvalsts noteiktajām prasībām vai pat ir pretrunā tām, var būtiski ietekmēt minētās pārrobežu darbības.

Turklāt iespējamība, ka kiberdrošības [...] **pasākumu** struktūra vai īstenošana var nebūt optimāla vienā dalībvalstī, visticamāk, ietekmēs pārējo dalībvalstu kiberdrošības līmeni, jo īpaši, ņemot vērā intensīvo pārrobežu apmaiņu. Direktīvas (ES) 2016/1148 pārskatīšanā ir atklājies, ka tās īstenošana dalībvalstīs ievērojami atšķiras, arī attiecībā uz tās darbības jomu, kuras precīza noteikšana lielā mērā tika atstāta dalībvalstu ziņā. Direktīva (ES) 2016/1148 arī sniedza dalībvalstīm ļoti plašu rīcības brīvību attiecībā uz tajā noteikto drošības un incidentu paziņošanas prasību īstenošanu. Tāpēc minētie pienākumi dalībvalstu līmenī tika īstenoti ļoti atšķirīgi. Līdzīgas īstenošanas atšķirības bija vērojamas attiecībā uz direktīvas noteikumiem par uzraudzību un izpildi.

(5) Visas šīs atšķirības sadrumstalo iekšējo tirgu un tām var būt prejudiciāla ietekme uz tā darbību, jo īpaši ietekmējot pakalpojumu pārrobežu sniegšanu un kiberdrošības noturības līmeni, jo tiek piemēroti atšķirīgi [...] **pasākumi**. Šīs direktīvas mērķis ir novērst šādas plašas atšķirības starp dalībvalstīm, jo īpaši izklāstot minimālos noteikumus attiecībā uz koordinēta tiesiskā regulējuma darbību, nosakot mehānismus efektīvai atbildīgo iestāžu sadarbībai katrā dalībvalstī, atjauninot to nozaru un darbību sarakstu, uz kurām attiecas kiberdrošības pienākumi, un paredzot efektīvus tiesiskās aizsardzības līdzekļus un sankcijas, kas ir svarīgas, lai šie pienākumi tiktu efektīvi izpildīti. Tāpēc Direktīva (ES) 2016/1148 būtu jāatceļ un jāaizstāj ar šo direktīvu.

(6) [...] Dalībvalstīm **būtu jāspēj** veikt nepieciešamos pasākumus, lai nodrošinātu savu būtisko drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrisko drošību un lai ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem[...]. [...]**Direktīva nebūtu jāpiemēro konkrētām publiskām vai privātām vienībām, kas veic darbības šajās jomās. Tā nebūtu jāpiemēro arī šajās jomās veiktajām vienību darbībām. Turklāt** dalībvalstīm nav jāsniedz informācija, kuras izpaušana būtu pretrunā to būtiskajām sabiedriskās drošības interesēm. [...]**S**varīgi ir valstu [...] **vai** Savienības noteikumi par klasificētas informācijas aizsardzību, vienošanās par neizpaušanu un neformālas vienošanās par informācijas neizpaušanu, piemēram, Gaismas signālu protokols [14].

(6.a) Jebkādai persondatu apstrādei saskaņā ar šo direktīvu piemēro Savienības tiesību aktus par persondatu un privātuma aizsardzību. Konkrēti, šī direktīva neskar Regulu (ES) 2016/679 un Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK, un tāpēc tai jo īpaši nebūtu jāietekmē to neatkarīgo uzraudzības iestāžu uzdevumi un pilnvaras, kuras ir kompetentas uzraudzīt atbilstību attiecīgajiem Savienības tiesību aktiem datu aizsardzības jomā.

---

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

(7) Līdz ar Direktīvas (ES) 2016/1148 atcelšanu būtu jāpaplašina piemērošanas joma pa nozarēm, aptverot lielāku ekonomikas daļu, ņemot vērā 4.–6. apsvērumā izklāstītos apsvērumus. Tāpēc to nozaru skaits, uz kurām attiecas Direktīva (ES) 2016/1148, būtu jāpalielina, lai nodrošinātu to nozaru un pakalpojumu pilnīgu aptvērumu, kuri ir ļoti svarīgi galvenajām sociālajām un saimnieciskajām darbībām iekšējā tirgū. Noteikumi nedrīkstētu atšķirties atkarībā no tā, vai vienības ir pamatpakalpojumu sniedzēji vai digitālo pakalpojumu sniedzēji. Ir pierādīts, ka šāda diferencēšana ir novecojusi, jo tā neatspoguļo nozaru vai pakalpojumu faktisko nozīmīgumu sociālajām un saimnieciskajām darbībām iekšējā tirgū.

(8) Saskaņā ar Direktīvu (ES) 2016/1148 dalībvalstīm bija pienākums noteikt, kuras vienības atbilst kritērijiem, lai tās uzskatītu par pamatpakalpojumu sniedzējiem ("identifikācijas process"). Lai šajā ziņā mazinātu lielās atšķirības starp dalībvalstīm un nodrošinātu juridisko noteiktību attiecībā uz riska pārvaldības prasībām un ziņošanas pienākumiem visām attiecīgajām vienībām, būtu jāievieš vienots kritērijs to vienību noteikšanai, kuras ir šīs direktīvas piemērošanas jomā. Minētajam kritērijam vajadzētu būt maksimālā lieluma noteikumam, saskaņā ar kuru visi vidējie un lielie uzņēmumi, kas definēti Komisijas Ieteikumā 2003/361/EK [15] un darbojas nozarēs vai sniedz pakalpojumus, uz kuriem attiecas šī direktīva, ir tās piemērošanas jomā. [...]

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

(8.a) Lai nodrošinātu skaidru pārskatu par vienībām, kas ietilpst šīs direktīvas darbības jomā, dalībvalstīm būtu jāspēj izveidot valsts mehānismus patstāvīgai paziņošanai, saskaņā ar kuriem vienībām, uz kurām attiecas šī direktīva, ir jāiesniedz vismaz savs nosaukums, adrese un kontaktinformācija, kā arī jānorāda nozare, kurā tās darbojas, vai to sniegtā pakalpojuma veids un attiecīgā gadījumā jāiesniedz to dalībvalstu saraksts, kurās attiecīgā vienība savus pakalpojumus sniedz šajā direktīvā minētajām kompetentajām iestādēm vai struktūrām, ko šajā nolūkā izraudzījušās dalībvalstis. Dalībvalstis var lemt par piemērotajiem mehānismiem, ja valsts līmenī pastāv reģistri, kas ļauj identificēt vienības, kuras ietilpst šīs direktīvas darbības jomā.

(9) [...] Šī direktīva būtu jāattiecina arī uz **mikrovienībām vai** mazām vienībām [...], kas atbilst noteiktiem kritērijiem, kuri norāda uz būtisku lomu dalībvalstu tautsaimniecībā vai sabiedrībā vai konkrētās nozarēs vai pakalpojumu veidos. Dalībvalstīm vajadzētu būt atbildīgām par [...] to, ka Komisijai **iesniedz vismaz attiecīgu informāciju par identificēto vienību skaitu, nozari, pie kuras tās pieder, vai to sniegtā pakalpojuma veidu un par konkrētajiem kritērijiem, pēc kuriem tās identificētas. Dalībvalstis var arī nolemt Komisijai iesniegt šo vienību nosaukumus, ja tas ir saskaņā ar valsts drošības noteikumiem.**

(9.a) Valsts pārvaldes vienības, kas veic darbības valsts drošības, aizsardzības, sabiedriskās drošības un tiesībaizsardzības jomā, kā arī tiesu iestādes, parlamenti un centrālās bankas ir izslēgtas no šīs direktīvas darbības jomas. Šajā direktīvā vienības, kam ir regulatīva kompetence, neuzskata par tādām, kas veic darbības tiesībaizsardzības jomā, un tāpēc tās šo iemeslu dēļ nav izslēgtas no šīs direktīvas darbības jomas. Turklāt šīs direktīvas darbības jomā neietilpst centrālās valdības publiskās pārvaldes vienības, kas saskaņā ar starptautisku nolīgumu izveidotas kopā ar trešo valsti.

(9.aa) Dalībvalstīm būtu jāspēj noteikt, ka vienības, kas pirms šīs direktīvas stāšanās spēkā identificētas kā pamatpakalpojumu sniedzēji saskaņā ar Direktīvu (ES) 2016/4118, ir uzskatāmas par būtiskām vienībām.

(9.aaa) Šī direktīva neattiecas uz dalībvalstu diplomātiskajām un konsulārajām pārstāvniecībām ārvalstīs un uz to IKT infrastruktūru, ko izmanto šādas pārstāvniecības, ja šāda infrastruktūra atrodas ārvalstīs vai tiek izmantota lietotājiem ārvalstīs.

(10) Komisija kopā ar sadarbības grupu var izdot pamatnostādnes par mikrouzņēmumiem un mazajiem uzņēmumiem piemērojamo kritēriju īstenošanu.

(11) [...] **Vienības, kuras ietilpst šīs direktīvas darbības jomā, būtu jāiedala divās kategorijās – būtiskas un svarīgas –, ņemot vērā nozares vai sniegto pakalpojumu veida svarīguma pakāpi, kā arī šo vienību lielumu. Šajā sakarā attiecīgā gadījumā būtu pienācīgi jāņem vērā arī visi attiecīgie nozaru riska novērtējumi vai norādījumi, ko sniegušas kompetentās iestādes.** Gan uz būtiskām, gan uz svarīgām vienībām būtu jāattiecina [...] riska pārvaldības prasības un ziņošanas pienākumi. Uzraudzības un sodu režīmi starp šīm abām vienību kategorijām būtu jādiferencē, lai nodrošinātu taisnīgu līdzsvaru starp prasībām un pienākumiem**, kas balstīti uz risku,** no vienas puses, un administratīvo slogu, kas izriet no atbilstības uzraudzības, no otras puses.

(12) **Šajā direktīvā ir noteikts pamats kiberdrošības riska pārvaldības pasākumiem un ziņošanas pienākumiem visās nozarēs, kas ietilpst tās darbības jomā. Lai izvairītos no Savienības tiesību aktos paredzēto kiberdrošības noteikumu sadrumstalotības, ja tiek uzskatīts, ka augsta kiberdrošības līmeņa nodrošināšanai ir nepieciešami papildu nozarspecifiski noteikumi, kas attiecas uz** kiberdrošības riska pārvaldības pasākumiem **un ziņošanas pienākumiem, Komisijai būtu jāizvērtē, vai šādus noteikumus varētu paredzēt īstenošanas aktā saskaņā ar šajā direktīvā paredzētajām pilnvarām. Ja šāds akts minētajam nolūkam nav piemērots,** nozarspecifiski tiesību akti **varētu** palīdzēt nodrošināt augstu kiberdrošības līmeni, vienlaikus pilnībā ņemot vērā [...] **attiecīgo** nozaru specifiku un sarežģītību. **Iemesli, kāpēc īstenošanas akts saskaņā ar šajā direktīvā paredzētajām pilnvarām nebija piemērots, jāpaskaidro nozarspecifiskajos tiesību aktos. Vienlaikus šādos nozarspecifiskos Savienības tiesību aktu noteikumos būtu pienācīgi jāņem vērā vajadzība pēc visaptverošas un saskaņotas kiberdrošības sistēmas.** [...] Tas neskar esošās īstenošanas pilnvaras, kas piešķirtas Komisijai vairākās nozarēs, tai skaitā transporta un enerģētikas nozarē.

(12.a) Ja nozarspecifiskā Savienības tiesību aktā **ir noteikumi** [...], saskaņā ar kuriem būtiskām vai svarīgām vienībām ir jāpieņem **pasākumi, kas ietekmes ziņā ir vismaz līdzvērtīgi šajā direktīvā noteiktajiem pienākumiem attiecībā uz** kiberdrošības riska pārvaldību [...] **un pienākumiem** ziņot par **nozīmīgiem** incidentiem vai nozīmīgiem kiberdraudiem [...], tad būtu jāpiemēro minētie nozarspecifiskie noteikumi**, tostarp par uzraudzību un izpildi**. **Nosakot, vai Savienības tiesību akta nozarspecifiskajos noteikumos izklāstītajiem pienākumiem ir līdzvērtīga ietekme, būtu jāņem vērā šādi aspekti: i) kiberdrošības riska pārvaldības pasākumiem vajadzētu būt atbilstīgiem un samērīgiem tehniskiem un organizatoriskiem pasākumiem, ar kuriem pārvalda riskus, kas apdraud tādu tīklu un informācijas sistēmu drošību, ko attiecīgās vienības izmanto savu pakalpojumu sniegšanā, un tajos būtu jāiekļauj vismaz visi šajā direktīvā noteiktie elementi; ii) pienākumam ziņot par nozīmīgiem incidentiem un kiberdraudiem vajadzētu būt vismaz līdzvērtīgam šajā direktīvā izklāstītajiem pienākumiem attiecībā uz paziņojumu saturu, formātu un termiņiem; iii) nozarspecifiskos Savienības tiesību aktos noteiktajai kārtībai, kādā vienības un attiecīgās iestādes ziņo, vajadzētu būt vismaz līdzvērtīgai šajā direktīvā izklāstītajām prasībām attiecībā uz saturu, formātu un termiņiem, un tajā būtu jāņem vērā *CSIRT* loma; iv) pārrobežu sadarbības prasībām attiecībā uz attiecīgajām iestādēm vajadzētu būt vismaz līdzvērtīgām šajā direktīvā noteiktajām prasībām. Ja nozarspecifiskie Savienības tiesību akta noteikumi neaptver visas vienības kādā konkrētā nozarē, kas ietilpst šīs direktīvas darbības jomā, šīs direktīvas attiecīgos noteikumus būtu jāturpina piemērot vienībām, uz kurām neattiecas minētie nozarspecifiskie noteikumi.**

(12.aa) Komisijai **būtu periodiski jāpārskata līdzvērtīgas ietekmes prasības piemērošana attiecībā uz nozarspecifiskiem Savienības tiesību aktu noteikumiem** [...]. **Gatavojot periodisko pārskatīšanu, Komisijai jāapspriežas ar sadarbības grupu**.

(12.aaa) Turpmākos nozarspecifiskos Savienības tiesību aktos būtu pienācīgi jāņem vērā šīs direktīvas 4. pantā izklāstītās definīcijas un uzraudzības un izpildes sistēma, kas noteikta šīs direktīvas VI nodaļā.

(12.ab) Ja nozarspecifiskos Savienības tiesību aktu noteikumos ir noteikts, ka būtiskām vai svarīgām vienībām jāpieņem pasākumi, kas ietekmes ziņā ir vismaz līdzvērtīgi šajā direktīvā noteiktajiem ziņošanas pienākumiem, būtu jāizvairās no ziņošanas pienākumu pārklāšanās un būtu jānodrošina saskaņotība un efektivitāte attiecībā uz to, kā tiek apstrādāti paziņojumi par kiberdraudiem vai incidentiem. Ar minētajiem nozarspecifiskajiem noteikumiem šajā nolūkā var ļaut dalībvalstīm izveidot kopīgu, automātisku un tiešu ziņošanas mehānismu nozīmīgu incidentu un kiberdraudu paziņošanai gan iestādēm, kuru uzdevumi ir izklāstīti attiecīgajos nozarspecifiskajos noteikumos, gan kompetentajām iestādēm, tostarp attiecīgā gadījumā vienotajam kontaktpunktam un *CSIRT*, kuras atbild par šajā direktīvā paredzētajiem kiberdrošības uzdevumiem, vai mehānismu, kas nodrošina sistemātisku un tūlītēju informācijas apmaiņu un sadarbību starp attiecīgajām iestādēm un *CSIRT* attiecībā uz šādu paziņojumu apstrādi. Lai vienkāršotu ziņošanu un ieviestu kopīgu, automātisku un tiešu ziņošanas mehānismu, dalībvalstis saskaņā ar nozarspecifiskiem tiesību aktiem var izmantot vienoto kontaktpunktu, ko tās izveido saskaņā ar šīs direktīvas 11. panta 5.a punktu. Lai nodrošinātu saskaņotību, ziņošanas pienākumi, kas noteikti nozarspecifiskos Savienības tiesību aktos, būtu jāsaskaņo ar šajā direktīvā precizētajiem ziņošanas pienākumiem. Dalībvalstis var noteikt, ka šajā direktīvā minētās kompetentās iestādes vai valstu *CSIRT* ir ziņojumu adresāti saskaņā ar nozarspecifiskiem tiesību aktiem.

(13) Eiropas Parlamenta un Padomes Regula XXXX/XXXX būtu jāuzskata par konkrētas nozares Savienības tiesību aktu saistībā ar šo direktīvu attiecībā uz finanšu sektora vienībām. Regulas XXXX/XXXX noteikumi par informācijas un komunikācijas tehnoloģiju (IKT) riska pārvaldības pasākumiem, ar IKT saistītu incidentu pārvaldību un jo īpaši incidentu paziņošanu, kā arī par digitālās darbības noturības testēšanu, informācijas apmaiņas pasākumiem un IKT trešo personu risku būtu jāpiemēro to noteikumu vietā, kuri [...] **ir izklāstīti šajā** direktīvā. Tāpēc dalībvalstīm šīs direktīvas noteikumi par kiberdrošības riska pārvaldību [...] un ziņošanas pienākumiem, [...] kā arī uzraudzību un izpildi nebūtu jāpiemēro finanšu vienībām, uz kurām attiecas Regula XXXX/XXXX. Vienlaikus ir svarīgi uzturēt ciešas attiecības un informācijas apmaiņu ar finanšu sektoru saskaņā ar šo direktīvu. Šajā nolūkā Regula XXXX/XXXX ļauj [...] Eiropas uzraudzības iestādēm (EUI) attiecībā uz finanšu sektoru un valsts kompetentajām iestādēm atbilstoši Regulai XXXX/XXXX [...] piedalīties sadarbības grupas [...] **darbā**, apmainīties ar informāciju un sadarboties ar vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar šo direktīvu**,** [...] **kā arī** ar valstu *CSIRT*. Kompetentajām iestādēm atbilstoši Regulai XXXX/XXXX būtu jānosūta ziņas par būtiskiem ar IKT saistītiem incidentiem **un nozīmīgiem kiberdraudiem** arī vienotajiem kontaktpunktiem**, kompetentajām iestādēm vai valstu *CSIRT***, kas izraudzīti saskaņā ar šo direktīvu. **To var panākt, automātiski un tieši nosūtot paziņojumus par incidentiem vai izveidojot kopīgu ziņošanas platformu.** Turklāt dalībvalstīm arī turpmāk būtu jāiekļauj finanšu sektors savās kiberdrošības stratēģijās, un valstu *CSIRT* [...] **var** ietvert finanšu sektoru savās darbībās.

(13.a) Lai izvairītos no to kiberdrošības pienākumu atšķirībām un dublēšanās, kurus piemēro vienībām I pielikuma 2. punkta a) apakšpunktā minētajā aviācijas nozarē, valsts iestādēm, kas izraudzītas saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 300/2008 [16] un Regulu (ES) 2018/1139 [17], un šajā direktīvā minētajām kompetentajām iestādēm būtu jāsadarbojas saistībā ar kiberdrošības riska pārvaldības pasākumu īstenošanu un minēto pasākumu uzraudzību valsts līmenī. Vienības atbilstību kiberdrošības riska pārvaldības pasākumiem saskaņā ar šo direktīvu valsts iestādes, kas izraudzītas saskaņā ar Regulu (EK) Nr. 300/2008 un Regulu (ES) 2018/1139, [...] varētu uzskatīt par atbilstību prasībām, kas noteiktas minētajās regulās un attiecīgajos deleģētajos un īstenošanas aktos, kuri pieņemti, ievērojot minētās regulas.

---

16 **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.).**

17 **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.).**

(14) Ņemot vērā saikni starp kiberdrošību un vienību fizisko drošību, Eiropas Parlamenta un Padomes Direktīvā (ES) XXX/XXX un šajā direktīvā būtu jānodrošina saskaņota pieeja. Lai to panāktu, dalībvalstīm būtu jānodrošina, ka kritiskās vienības **[**un tām līdzvērtīgas vienības**]**, ievērojot Direktīvu (ES) XXX/XXX, tiek uzskatītas par būtiskām vienībām atbilstoši šai direktīvai. Dalībvalstīm būtu arī jānodrošina, ka to kiberdrošības stratēģijās ir paredzēts politikas satvars uzlabotai koordinācijai starp kompetento iestādi atbilstoši šai direktīvai un kompetento iestādi atbilstoši Direktīvai (ES) XXX/XXX saistībā ar informācijas apmaiņu par incidentiem un kiberdraudiem un uzraudzības uzdevumu īstenošanu. Abās direktīvās minētajām **kompetentajām** [...] **i**estādēm būtu jāsadarbojas un jāapmainās ar informāciju, jo īpaši saistībā ar kritisko vienību noteikšanu, kiberdraudiem, kiberdrošības riskiem, incidentiem**, kā arī ar kiberdrošību nesaistītiem riskiem, draudiem un incidentiem**, kas ietekmē kritiskās vienības **[**vai **kritiskajām vienībām līdzvērtīgas vienības],** [...] **tostarp** par kiberdrošības **un fiziskiem** pasākumiem, ko veikušas kritiskās vienības**, un attiecībā uz šādām vienībām veikto uzraudzības darbību rezultātiem. Turklāt, lai racionalizētu uzraudzības darbības starp kompetentajām iestādēm, kas izraudzītas saskaņā ar abām direktīvām, un lai attiecīgajām vienībām mazinātu administratīvo slogu, kompetentajām iestādēm būtu jācenšas saskaņot incidentu paziņošanas veidnes un uzraudzības procesus.** [...] **Attiecīgā gadījumā** Direktīvā (ES) XXX/XXX minētās kompetentās iestādes **var prasīt** šajā direktīvā minētajām kompetentajām iestādēm [...], lai tās īsteno savas uzraudzības un izpildes pilnvaras [...] **attiecībā uz** būtisku vienību, kas identificēta kā kritiska. [...]

(14.a) Vienības, kas pieder pie digitālās infrastruktūras nozares, būtībā balstās uz tīklu un informācijas sistēmām, un tāpēc ar pienākumiem, kurus minētajām vienībām nosaka šajā direktīvā, būtu visaptveroši jāpievēršas šādu sistēmu fiziskajai drošībai kā daļai no to kiberdrošības riska pārvaldības un ziņošanas pienākumiem. Tā kā uz minētajiem jautājumiem attiecas šī direktīva, Direktīvas (ES) XXX/XXX [*CER*] III–VI nodaļā noteiktos pienākumus šādām vienībām nepiemēro.

(15) 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. Tādēļ šī direktīva būtu jāpiemēro **iekšējam tirgum svarīgu** DNS pakalpojumu sniedzējiem visā DNS **nodrošināšanas un** noregulējuma ķēdē, tostarp [...] augstākā līmeņa domēna (ALD) nosaukumu **reģistriem** [...], **vienībām, kas sniedz domēna nosaukuma reģistrācijas pakalpojumus,** autoritatīvo nosaukumu serveru **operatoriem** saistībā ar domēnu nosaukumiem un rekursīvo atrisinātāju **operatoriem**. **Termins "DNS pakalpojumu sniedzējs" nebūtu jāattiecina uz DNS pakalpojumiem, ko sniedz attiecīgās vienības un ar to saistīto vienību pašu vajadzībām. Šai pakalpojumu sniedzēju kategorijai noteiktie kiberdrošības pienākumi, kas izriet no šīs direktīvas, attiecas tikai uz kiberdrošības riska pārvaldības pasākumiem un ziņošanu, un tādējādi tie neskar globālās DNS pārvaldību, ko veic daudzpusēja ieinteresēto personu kopiena.**

(16) Mākoņdatošanas pakalpojumos būtu jāiekļauj pakalpojumi, kas ļauj pēc pieprasījuma plaši un attālināti piekļūt kopīgojamu un sadalītu datošanas resursu mērogojamam un elastīgam pūlam. Minētie 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. Iepriekš minēto 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 tīkla glabāšanu, bez cilvēciskas mijiedarbības ar mākoņdatošanas pakalpojumu 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, darbstaciju) izmantošanu.

Termins "mērogojams" attiecas uz datošanas resursiem, kurus mākoņdatošanas pakalpojuma sniedzējs elastīgi piešķir neatkarīgi no resursu ģeogrāfiskās atrašanās vietas, lai risinātu pieprasījuma svārstības. Termins "elastīgs pūls" ir izmantots, lai aprakstītu tos datošanas resursus, kuri tiek nodrošināti un atbrīvoti saskaņā ar pieprasījumu, lai pieejamos resursus ātri palielinātu un samazinātu atkarībā no noslodzes. Termins "kopīgojams" ir izmantots, lai aprakstītu tos datošanas resursus, kas tiek sniegti daudziem lietotājiem, kuriem ir kopīga piekļuve pakalpojumam, bet apstrāde notiek katram lietotājam atsevišķi, kaut arī pakalpojums tiek sniegts no vienas un tās pašas elektroniskās iekārtas. Termins "sadalīts" ir izmantots, lai aprakstītu tos datošanas resursus, kas atrodas dažādos tīklotos datoros vai ierīcēs un kas īsteno savstarpēju saziņu un koordināciju, izmantojot ziņojumu sūtīšanu.

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

(18) Pakalpojumus, ko piedāvā datu centru pakalpojumu sniedzēji, ne vienmēr var sniegt mākoņdatošanas pakalpojuma veidā. Tas nozīmē, ka datu centri var nebūt daļa no mākoņdatošanas infrastruktūras. Lai pārvaldītu visus riskus tīklu un informācijas sistēmu drošībai, šī direktīva būtu jāattiecina arī uz tādu datu centru pakalpojumu sniedzējiem, kuri nav mākoņdatošanas pakalpojumi. Šajā direktīvā termins "datu centra pakalpojums" būtu jāattiecina uz tāda pakalpojuma sniegšanu, kas ietver struktūras vai struktūru grupas, kuras paredzētas tāda informācijas tehnoloģijas un tīkla aprīkojuma centralizētai izmitināšanai, savstarpējai savienošanai un darbībai, kas sniedz datu uzglabāšanas, apstrādes un transportēšanas pakalpojumus kopā ar visām ierīcēm un infrastruktūrām jaudas sadalei un vides kontrolei. Termins "datu centra pakalpojums" neattiecas uz iekšējiem, korporatīviem datu centriem, ko tur īpašumā un ekspluatē attiecīgās vienības vajadzībām.

(19) Pasta pakalpojumu sniedzēji Eiropas Parlamenta un Padomes Direktīvas 97/67/EK [18] nozīmē, [...] **tostarp** kurjeru [...] pakalpojumu sniedzēji, būtu jāiekļauj šīs direktīvas darbības jomā, ja tie nodrošina vismaz vienu no posmiem pasta piegādes ķēdē un jo īpaši sniedz atmuitošanas, šķirošanas vai sadales pakalpojumus, arī savākšanas pakalpojumus. Transporta pakalpojumi, kurus neveic saistībā ar kādu no minētajiem posmiem, būtu jāizslēdz no pasta pakalpojumu jomas.

---

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

(20) Šī pieaugošā savstarpējā atkarība ir rezultāts tam, ka pakalpojumu sniegšanas tīklam arvien biežāk ir pārrobežu raksturs un tas arvien vairāk ir savstarpēji atkarīgs, izmantojot pamatinfrastruktūras visā Savienībā tādās nozarēs kā enerģētika, transports, digitālā infrastruktūra, dzeramais ūdens un notekūdeņi, veselība, konkrēti valsts pārvaldes aspekti, kā arī kosmoss, ciktāl tas attiecas uz tādu konkrētu pakalpojumu sniegšanu, kuri ir atkarīgi no virszemes infrastruktūrām, ko tur īpašumā, pārvalda vai ekspluatē dalībvalstis vai attiecīgās privātpersonas, tādējādi neaptverot infrastruktūras, ko tur īpašumā, pārvalda vai ekspluatē Savienība vai tās vārdā kā daļu no tās kosmosa programmām. Šī savstarpējā atkarība nozīmē, ka jebkuram traucējumam, pat tādam, kas sākotnēji ierobežots līdz vienai vienībai vai vienai nozarei, var būt plašāka lavīnveida ietekme, iespējams, rezultātā izraisot tālejošas un ilgstošas negatīvas sekas pakalpojumu sniegšanā iekšējā tirgū. Covid-19 pandēmija ir parādījusi mūsu arvien vairāk savstarpēji atkarīgās sabiedrības neaizsargātību, neraugoties uz zemas varbūtības riskiem.

(**20.a**) **Lai sasniegtu un uzturētu augstu kiberdrošības līmeni, šajā direktīvā prasītajām valstu kiberdrošības stratēģijām būtu jāietver saskaņoti satvari, kas paredz pārvaldību kiberdrošības jomā. Šīs stratēģijas var veidot viens vai vairāki leģislatīvi vai neleģislatīvi dokumenti.**

(21) Ņemot vērā atšķirības valstu pārvaldes struktūrās un lai garantētu jau esošo nozaru noteikumu izpildi vai aizsargātu Savienības uzraudzības un regulatīvās struktūras, dalībvalstīm būtu jāspēj izraudzīties vairāk nekā vienu valsts kompetento iestādi, kas ir atbildīga par to, lai saskaņā ar šo direktīvu pildītu uzdevumus saistībā ar būtisko un svarīgo vienību tīklu un informācijas sistēmu drošību. Dalībvalstīm būtu jāspēj uzticēt šo funkciju esošai iestādei.

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

(23) Kompetentajām iestādēm vai *CSIRT* būtu efektīvi un lietpratīgi jāsaņem paziņojumi par incidentiem no vienībām**, arī lai attiecīgos gadījumos sekmētu savlaicīgu reaģēšanu uz incidentiem un sniegtu atbildi ziņotājai vienībai**. Būtu jānosaka vienotajiem kontaktpunktiem pienākums pārsūtīt incidentu paziņojumus citu skarto dalībvalstu vienotajiem kontaktpunktiem. [...]

(23.a) Nozarspecifiskos Savienības tiesību aktos, kuros prasīts veikt kiberdrošības riska pārvaldības pasākumus vai pildīt ziņošanas pienākumus, kas ietekmes ziņā ir vismaz līdzvērtīgi tiem, kas noteikti šajā direktīvā, varētu paredzēt, ka to izraudzītās kompetentās iestādes īsteno savas uzraudzības un izpildes pilnvaras attiecībā uz šādiem pasākumiem vai pienākumiem ar to kompetento iestāžu palīdzību, kuras izraudzītas saskaņā ar šo direktīvu. Attiecīgās kompetentās iestādes šajā nolūkā varētu izveidot sadarbības mehānismus. Šādos sadarbības mehānismos cita starpā varētu precizēt procedūras attiecībā uz uzraudzības darbību koordinēšanu, tostarp izmeklēšanas un uz vietas veicamu pārbaužu procedūras saskaņā ar valsts tiesību aktiem, un mehānismu attiecīgas informācijas apmaiņai starp kompetentajām iestādēm par uzraudzību un izpildi, tostarp piekļuvi ar kiberjautājumiem saistītai informācijai, ko pieprasa saskaņā ar šo direktīvu izraudzītās kompetentās iestādes.

(24) Visās dalībvalstīs vajadzētu būt atbilstīgam aprīkojumam gan tehnisko, gan organizatorisko spēju ziņā, lai novērstu un atklātu tīklu un informācijas sistēmu incidentus un riskus, reaģētu uz tiem un tos mazinātu. Tāpēc dalībvalstīm būtu jānodrošina, ka tajās ir labi funkcionējošas, pamatprasībām atbilstīgas *CSIRT*, kas tiek dēvētas arī par datorapdraudējumu reaģēšanas vienībām (*CERT*), lai nodrošinātu efektīvas un saderīgas spējas incidentu risināšanai un risku novēršanai un efektīvas sadarbības nodrošināšanai Savienības līmenī. Lai uzlabotu uzticības pilnas attiecības starp vienībām un *CSIRT*, gadījumos, kad *CSIRT* ir kompetentās iestādes daļa, dalībvalstis [...] **var** apsvērt funkcionālu nošķīrumu starp *CSIRT* veiktajiem operatīvajiem uzdevumiem, jo īpaši attiecībā uz informācijas apmaiņu un atbalstu vienībām, un kompetento iestāžu uzraudzības darbībām.

(25) Attiecībā uz persondatiem *CSIRT* saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 [19], ja to pieprasa vienības atbilstoši šai direktīvai un to vārdā, būtu jāspēj nodrošināt to pakalpojumu sniegšanai izmantoto tīklu un informācijas sistēmu proaktīvu skenēšanu. **Attiecīgos gadījumos** dalībvalstīm būtu jāizvirza mērķis nodrošināt vienlīdzīgu tehnisko spēju līmeni visām nozaru *CSIRT*. Dalībvalstis var lūgt Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) palīdzību valsts *CSIRT* attīstīšanā.

(26) Ņemot vērā to, cik svarīga ir starptautiskā sadarbība kiberdrošības jomā, *CSIRT* būtu jāspēj piedalīties starptautiskos sadarbības tīklos papildus *CSIRT* tīklam, ko izveido ar šo direktīvu. **Tādēļ *CSIRT* un kompetentās iestādes varētu apmainīties ar informāciju, tostarp persondatiem, ar trešo valstu *CSIRT* vai to iestādēm, lai tās varētu veikt savus uzdevumus saskaņā ar Regulu (ES) 2016/679. Ja nav saskaņā ar Regulas (ES) 2016/679 45. pantu pieņemta lēmuma par aizsardzības līmeņa pietiekamību vai nav attiecīgu garantiju saskaņā ar minētās regulas 46. pantu, apmaiņu ar persondatiem, kas tiek uzskatīta par nepieciešamu, lai mazinātu nozīmīgus kiberdraudus un reaģētu uz notiekošu nozīmīgu incidentu, varētu uzskatīt par tādu, kurai ir svarīgs iemesls sabiedrības interesēs Regulas (ES) 2016/679 49. panta 1. punkta d) apakšpunkta nozīmē.**

---

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

(27) Saskaņā ar pielikumu Komisijas Ieteikumam (ES) 2017/1548 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm ("Plāns") [20] plašapmēra incidents būtu jāsaprot kā incidents, kuram ir nozīmīga ietekme uz vismaz divām dalībvalstīm vai kura radītie traucējumi pārsniedz dalībvalsts spēju uz tiem reaģēt. Atkarībā no to cēloņa un ietekmes plašapmēra incidenti var izvērsties par visaptverošām krīzēm, kas padara neiespējamu iekšējā tirgus pienācīgu darbību. Ņemot vērā šādu incidentu plašo tvērumu un to, ka vairākumā gadījumu tiem ir pārrobežu raksturs, dalībvalstīm un attiecīgajām Savienības iestādēm, struktūrām un aģentūrām būtu jāsadarbojas tehniskā, operatīvā un politiskā līmenī, lai pienācīgi koordinētu reaģēšanu visā Savienībā.

(28) Tā kā tīklu un informācijas sistēmu neaizsargātības ļaunprātīga izmantošana var izraisīt būtiskus traucējumus un kaitējumu, kiberdrošības riska mazināšanā svarīgs faktors ir šādas neaizsargātības ātra apzināšana un novēršana. Tāpēc vienībām, kas attīsta **vai pārvalda** šādas sistēmas, būtu jāievieš atbilstīgas procedūras rīcībai gadījumos, kad tiek atklāta neaizsargātība. Tā kā neaizsargātību bieži konstatē un paziņo (atklāj) trešās personas (ziņotājas vienības), IKT produktu ražotājam vai pakalpojumu sniedzējam būtu arī jāievieš nepieciešamās procedūras informācijas par neaizsargātību saņemšanai no trešām personām. Šajā saistībā starptautiskie standarti ISO/IEC 30111 un ISO/IEC [...] **29147** sniedz norādījumus attiecīgi par rīcību neaizsargātības gadījumā un neaizsargātības atklāšanu. Attiecībā uz neaizsargātības atklāšanu īpaši svarīga ir koordinācija starp ziņotājām vienībām un IKT produktu ražotājiem vai pakalpojumu sniedzējiem. Koordinēta neaizsargātības atklāšana ir strukturēts process, kurā par neaizsargātību tiek ziņots organizācijām tādā veidā, lai organizācija varētu diagnosticēt un novērst neaizsargātību, pirms sīkāka informācija par to tiek darīta zināma trešām personām vai sabiedrībai. Koordinētā neaizsargātības atklāšanā būtu arī jāietver koordinācija starp ziņotāju vienību un organizāciju attiecībā uz neaizsargātības izlabošanas un publiskošanas termiņu.

---

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

(29) Tāpēc dalībvalstīm būtu jāveic pasākumi, lai veicinātu koordinētu neaizsargātības atklāšanu, ieviešot atbilstošu valsts politiku. **Īstenojot savu valsts politiku, dalībvalstīm būtu jācenšas, cik vien iespējams, risināt problēmas, kas skar neaizsargātības pētniekus, tostarp to, ka viņiem var tikt noteikta krimināltatbildība saskaņā ar viņu valsts tiesisko kārtību.** [...] Dalībvalstīm būtu jāizraugās *CSIRT*, lai tā uzņemtos "koordinatora" lomu, nepieciešamības gadījumā darbodamās kā starpnieks starp ziņotājām vienībām un IKT produktu ražotājiem vai pakalpojumu sniedzējiem. *CSIRT* koordinatora pienākumos būtu jo īpaši jāiekļauj attiecīgo vienību apzināšana un saziņa ar tām, ziņotāju vienību atbalstīšana, atklāšanas termiņu apspriešana un vairākas organizācijas ietekmējošas neaizsargātības pārvaldība (vairāku pušu **koordinēta** neaizsargātības atklāšana). Ja **paziņotā** neaizsargātība **varētu būtiski ietekmēt vienības** [...] vairāk nekā vienā dalībvalstī, izraudzītajām *CSIRT* [...] **attiecīgos gadījumos** būtu jāsadarbojas *CSIRT* tīklā.

(30) Piekļuve pareizai un savlaicīgai informācijai par neaizsargātību, kas skar IKT produktus un pakalpojumus, veicina kiberdrošības riska pārvaldības uzlabošanu. Šajā ziņā publiski pieejamas informācijas par neaizsargātību avoti ir svarīgs rīks vienībām un to lietotājiem, kā arī valsts kompetentajām iestādēm un *CSIRT*. Šā iemesla dēļ *ENISA* būtu jāizveido brīvprātīgs neaizsargātības reģistrs, kurā būtiskas un svarīgas vienības un to piegādātāji, kā arī vienības, uz kurām neattiecas šīs direktīvas piemērošanas joma, **vai izraudzītās *CSIRT*** var atklāt neaizsargātību un sniegt neaizsargātības informāciju, kas ļauj lietotājiem veikt atbilstīgus riska mazināšanas pasākumus.

(31) Lai gan līdzīgi neaizsargātības reģistri vai datubāzes jau pastāv, to mitinātāji un uzturētāji ir vienības, kuru iedibinājuma vieta nav Savienībā. Eiropas neaizsargātības reģistrs, ko uztur *ENISA*, nodrošinātu uzlabotu pārredzamību attiecībā uz publiskošanas procesu, pirms neaizsargātība tiek oficiāli atklāta, un noturību gadījumos, kad notiek traucējumi vai pārtraukumi līdzīgu pakalpojumu sniegšanā. Lai, ciktāl iespējams, izvairītos no centienu dublēšanās un nodrošinātu papildināmību, *ENISA* būtu jāizvērtē iespēja noslēgt strukturētus sadarbības nolīgumus ar līdzīgiem reģistriem trešo valstu jurisdikcijās. ***ENISA* jo īpaši būtu jāizpēta iespēja cieši sadarboties ar kopējās neaizsargātības un eksponētības (*CVE*) sistēmas operatoriem, tostarp iespēja kļūt par galveno *CVE* numerācijas iestādi.**

(32) **Sadarbības grupai būtu jāturpina atbalstīt un veicināt stratēģisko sadarbību un informācijas apmaiņu, kā arī stiprināt dalībvalstu savstarpējo uzticēšanos un paļāvību.** Sadarbības grupai būtu reizi divos gados jāizstrādā darba programma, kurā iekļauj darbības, kas grupai jāveic, lai īstenotu tās mērķus un uzdevumus. Saskaņā ar šo direktīvu pieņemtās pirmās programmas termiņš būtu jāpielāgo saskaņā ar Direktīvu (ES) 2016/1148 pieņemtās pēdējās programmas termiņam, lai izvairītos no iespējamiem traucējumiem grupas darbā.

(33) Izstrādājot norādījumu dokumentus, sadarbības grupai būtu konsekventi jāapzina valsts risinājumi un pieredze, jānovērtē sadarbības grupas nodevumu ietekme uz valstu pieejām, jāapspriež īstenošanas problēmas un jāformulē īpaši ieteikumi, kas jāizpilda, labāk īstenojot esošos noteikumus.

(34) Sadarbības grupai arī turpmāk vajadzētu būt elastīgam forumam un būtu jāspēj reaģēt uz mainīgām un jaunām politikas prioritātēm un problēmām, vienlaikus ņemot vērā resursu pieejamību. Tai būtu jāorganizē regulāras kopīgas sanāksmes ar attiecīgajām privātā sektora ieinteresētajām personām no visas Savienības, lai apspriestu grupas veiktās darbības un apkopotu informāciju par jaunām politikas problēmām. Lai uzlabotu sadarbību Savienības līmenī, grupai būtu jāapsver iespēja pieaicināt Savienības struktūras un aģentūras, kas iesaistītas kiberdrošības politikā, piemēram, Eiropas Kibernoziedzības apkarošanas centru (*EC3*), Eiropas Savienības Aviācijas drošības aģentūru (*EASA*) un Eiropas Savienības Kosmosa programmas aģentūru (*EUSPA*), lai tās piedalītos tās darbā.

(35) Lai uzlabotu sadarbību, kompetentajām iestādēm un *CSIRT* vajadzētu būt iespējai piedalīties apmaiņas shēmās, kas paredzētas amatpersonām no citām dalībvalstīm. Kompetentajām iestādēm būtu jāveic pasākumi, kas nepieciešami, lai amatpersonas no citām dalībvalstīm varētu efektīvi piedalīties uzņēmējas kompetentās iestādes pasākumos.

(35.a) *CSIRT* tīklam būtu jāturpina palīdzēt stiprināt paļāvību un uzticēšanos un jāveicina ātra un efektīva operatīvā sadarbība starp dalībvalstīm. Lai uzlabotu operatīvo sadarbību Savienības līmenī, *CSIRT* tīklam būtu jāapsver iespēja aicināt Savienības struktūras un aģentūras, kas iesaistītas kiberdrošības politikā, piemēram, Eiropolu, piedalīties tā darbā.

(36) [...]

(36.a) Lai veicinātu šīs direktīvas noteikumu efektīvu īstenošanu, piemēram, saistībā ar neaizsargātības pārvaldību, kiberdrošības risku pārvaldību, ziņošanas un informācijas apmaiņas pasākumiem, dalībvalstis var sadarboties ar trešām valstīm un veikt darbības, kas tiek uzskatītas par atbilstošām minētajam nolūkam, tostarp apmainīties ar informāciju par apdraudējumiem, incidentiem, neaizsargātību, rīkiem un metodēm, taktiku, paņēmieniem un procedūrām, gatavību kiberkrīžu pārvaldībai un mācībām, apmācību, uzticēšanās veidošanu un strukturētu informācijas apmaiņas kārtību. Šādiem sadarbības nolīgumiem būtu jāatbilst Savienības tiesību aktiem datu aizsardzības jomā.

(37) Dalībvalstīm būtu jāsniedz ieguldījums Ieteikumā (ES) 2017/1584 noteiktā ES satvara reaģēšanai kiberdrošības krīzēs izveidošanā, izmantojot esošos sadarbības tīklus, jo īpaši **Eiropas** Kiberkrīžu sadarbības organizāciju tīklu (*EU-CyCLONe*), *CSIRT* tīklu un sadarbības grupu. *EU-CyCLONe* un *CSIRT* tīklam būtu jāsadarbojas, pamatojoties uz procedūrām, kas nosaka šādas sadarbības procesuālo kārtību, **un jāizvairās no jebkādas uzdevumu dublēšanās.** *EU-CyCLONe* reglamentā būtu jāprecizē kārtība, kādā tīklam būtu jādarbojas, cita starpā paredzot uzdevumus, sadarbības veidus, mijiedarbību ar citiem attiecīgiem dalībniekiem un veidnes informācijas apmaiņai, kā arī saziņas līdzekļus. Attiecībā uz krīžu pārvaldību Savienības **politiskajā** līmenī attiecīgajām pusēm būtu jāpaļaujas uz integrētajiem krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismiem. Šim nolūkam Komisijai būtu jāizmanto krīzes augstlīmeņa starpnozaru koordinācijas process *ARGUS*. Ja krīzei ir nozīmīgs ārējās politikas vai kopīgās drošības un aizsardzības politikas (KDAP) aspekts, būtu jāiedarbina Eiropas Ārējās darbības dienesta (EĀDD) mehānisms reaģēšanai krīzes situācijās (*CRM*).

(37.a) *EU-CyCLONe* būtu jādarbojas kā starpniektīklam starp tehnisko un politisko līmeni plašapmēra kiberdrošības incidentu un krīžu laikā. Tam būtu jāuzlabo sadarbība operatīvā līmenī, pamatojoties uz *CSIRT* tīkla konstatējumiem un izmantojot savas spējas, lai veiktu plašapmēra incidentu un krīžu ietekmes analīzi, un atbalstot lēmumu pieņemšanu politiskā līmenī. ES iestādēm, struktūrām un aģentūrām būtu jāizraugās kompetenta iestāde, kas atbild par plašapmēra drošības incidentu un krīžu pārvaldību, lai tā kļūtu par *EU-CyCLONe* locekli.

(38) [...]

(39) [...]

(39.a) Tīklu un informācijas sistēmas drošības nodrošināšana lielā mērā ir būtisko un svarīgo vienību pienākums. Būtu jāattīsta un jāpopularizē riska pārvaldības kultūra, kas ietver riska novērtējumu un faktiskajiem riskiem atbilstīgu drošības pasākumu īstenošanu.

(40) Riska pārvaldības pasākumos būtu **jāņem vērā, cik lielā mērā vienība ir atkarīga no tīklu un informācijas sistēmām, un** jāietver pasākumi nolūkā identificēt visus incidentu riskus, novērst, atklāt incidentus un reaģēt uz tiem, un mazināt to ietekmi. Tīklu un informācijas sistēmu drošībai būtu jāietver glabāto, pārsūtīto un apstrādāto datu drošība.

(40.a) Tā kā tīklu un informācijas sistēmu drošības apdraudējumiem var būt dažāda izcelsme, šajā direktīvā piemēro "visu apdraudējumu" pieeju, kas ietver tīklu un informācijas sistēmu un to fiziskās vides aizsardzību pret jebkādiem notikumiem, piemēram, zādzību, ugunsgrēku, plūdiem, telesakaru vai elektroapgādes pārtraukumiem, vai pret jebkādu neatļautu fizisku piekļuvi, kā arī pret bojājumiem un traucējumiem vienības informācijas un informācijas apstrādes iekārtās, kas varētu apdraudēt glabāto, pārsūtīto vai apstrādāto datu vai pakalpojumu, kurus piedāvā vai kuriem var piekļūt ar tīklu un informācijas sistēmu starpniecību, pieejamību, autentiskumu, integritāti vai konfidencialitāti. Tāpēc riska pārvaldības pasākumos būtu jāpievēršas arī fiziskajai un vides drošībai, iekļaujot pasākumus vienības tīklu un informācijas sistēmu aizsardzībai pret sistēmas traucējumiem, cilvēka kļūdām, ļaunprātīgām darbībām vai dabas parādībām atbilstoši Eiropas vai starptautiski atzītiem standartiem, piemēram, tiem, kas iekļauti ISO 27000 sērijā. Šajā saistībā vienībām savu riska pārvaldības pasākumu ietvaros būtu jāpievēršas arī cilvēkresursu drošībai un jāievieš atbilstīga piekļuves kontroles politika. Minētajiem pasākumiem vajadzētu būt saskaņā ar Direktīvu XXXX [KVN direktīva].

(40.b) Ja nav atbilstošu Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemtas saskaņā ar Regulu (ES) 2019/881, dalībvalstis varētu pieprasīt vienībām izmantot sertificētus IKT produktus, pakalpojumus un procesus vai iegūt sertifikātu saskaņā ar pieejamām valsts kiberdrošības shēmām, lai nodrošinātu atbilstību šajā direktīvā noteiktajām kiberdrošības riska pārvaldības prasībām.

(41) Lai izvairītos no nesamērīga finansiāla un administratīva sloga radīšanas būtiskajām un svarīgajām vienībām, kiberdrošības riska pārvaldības prasībām vajadzētu būt samērīgām ar risku, kas [...] **tiek radīts** attiecīgām tīklu un informācijas sistēmām, ņemot vērā jaunākos sasniegumus saistībā ar šādiem pasākumiem **un to īstenošanas izmaksas**. **Būtu pienācīgi jāņem vērā arī vienības lielums, kā arī incidentu rašanās iespējamība un to smaguma pakāpe.**

(41.a) Lai atvieglotu regulatīvo slogu, prasības par kiberdrošības riska pārvaldības pasākumu īstenošanu attiecībā uz vidējām, mazām vai mikrovienībām principā vajadzētu mīkstināt, ja vien svarīguma kritēriji vai valsts riska novērtējumi neattaisno stingrākas prasības, jo īpaši attiecībā uz vienībām, kas atbilst šajā direktīvā noteiktajiem ar svarīgumu saistītajiem kritērijiem.

(42) Būtiskajām un svarīgajām vienībām būtu jānodrošina savās darbībās izmantoto tīklu un informācijas sistēmu drošība. Tās galvenokārt ir privātas tīklu un informācijas sistēmas, kuras pārvalda iekšējais IT personāls vai kuru drošība tiek nodrošināta, izmantojot ārpakalpojumus. Kiberdrošības riska pārvaldības un ziņošanas prasības atbilstoši šai direktīvai būtu jāattiecina uz būtiskajām un svarīgajām vienībām neatkarīgi no tā, vai tās veic savu tīklu un informācijas sistēmu uzturēšanu iekšēji vai šim nolūkam izmanto ārpakalpojumus.

(42.aa) DNS pakalpojumu sniedzējiem, ALD nosaukumu reģistriem un vienībām, kas sniedz domēnu nosaukuma reģistrācijas pakalpojumus saistībā ar ALD, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīklu nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem un pārvaldītu drošības pakalpojumu sniedzējiem, ņemot vērā to pārrobežu raksturu, būtu jāpiemēro lielāka saskaņotības pakāpe Savienības līmenī. Tāpēc kiberdrošības pasākumu īstenošana būtu jāveicina ar īstenošanas aktu.

(43) Risināt kiberdrošības riskus, kas izriet no vienības piegādes ķēdes un tās attiecībām ar tās piegādātājiem, ir īpaši svarīgi, ņemot vērā tādu incidentu izplatību, kuros vienības ir cietušas kiberuzbrukumos un kuros ļaunprātīgi dalībnieki ir spējuši apdraudēt vienības tīklu un informācijas sistēmu drošību, izmantojot neaizsargātību, kas skar trešo personu produktus un pakalpojumus. Tāpēc vienībām būtu jānovērtē un jāņem vērā to piegādātāju un pakalpojumu sniedzēju produktu vispārējā kvalitāte un kiberdrošības prakse, tai skaitā to drošas attīstības procedūras.

(44) Pakalpojumu sniedzēju vidū pārvaldītu drošības pakalpojumu sniedzējiem (*MSSP*) tādās jomās kā reaģēšana uz incidentiem, ielaušanās testēšana, drošības revīzijas un konsultācijas ir īpaši svarīga loma, palīdzot vienībām to centienos atklāt incidentus un reaģēt uz tiem. Tomēr arī šādi *MSSP* paši ir bijuši kiberuzbrukumu mērķis, un tie rada īpašu kiberdrošības risku, jo ir cieši iesaistīti operatoru darbībās. Tāpēc vienībām, izvēloties *MSSP*, būtu jāievēro īpaša piesardzība.

(44.a) Valsts kompetentās iestādes savu uzraudzības uzdevumu ietvaros var izmantot arī tādus kiberdrošības pakalpojumus kā drošības revīzijas un ielaušanās testēšana vai reaģēšana uz incidentiem. Lai vienībām, kā arī valsts kompetentajām iestādēm palīdzētu izraudzīties kvalificētus un uzticamus kiberdrošības pakalpojumu sniedzējus, Komisijai ar sadarbības grupas un *ENISA* palīdzību būtu jāapsver iespēja pieprasīt Eiropas kiberdrošības sertifikācijas shēmas saskaņā ar Regulas (ES) 2019/881 48. pantu.

(45) Vienībām būtu arī jāpievēršas kiberdrošības riskiem, kas izriet no to mijiedarbības un attiecībām ar citām ieinteresētajām personām plašākā ekosistēmā. Vienībām jo īpaši būtu jāveic atbilstīgi pasākumi, lai nodrošinātu, ka to sadarbība ar akadēmiskajām un pētniecības iestādēm notiek atbilstoši to kiberdrošības politikai un ka tās ietvaros tiek ievērota laba prakse attiecībā uz drošu piekļuvi un informācijas izplatīšanu kopumā un jo īpaši intelektuālā īpašuma aizsardzību. Līdzīgi, ņemot vērā datu nozīmīgumu un vērtību vienību darbībās, vienībām, paļaujoties uz trešo personu sniegtiem datu transformēšanas un datu analīzes pakalpojumiem, būtu jāveic visi atbilstīgie kiberdrošības pasākumi.

(46) Lai turpinātu pievērsties galvenajiem piegādes ķēdes riskiem un palīdzētu vienībām, kas darbojas nozarēs, uz kurām attiecas šī direktīva, pienācīgi pārvaldīt ar piegādes ķēdēm un piegādātājiem saistītus kiberdrošības riskus, sadarbības grupai, iesaistot attiecīgās valsts iestādes un sadarbojoties ar Komisiju un *ENISA*, būtu jāveic koordinēti nozaru piegādes ķēžu riska novērtējumi, kā tas jau tika darīts attiecībā uz 5G tīkliem saskaņā ar Ieteikumu (ES) 2019/534 par 5G tīklu kiberdrošību [21], lai par katru nozari apzinātu, kuri ir kritiskie IKT pakalpojumi, sistēmas vai produkti, attiecīgie draudi un neaizsargātība.

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

(47) Piegādes ķēžu riska novērtējumos, ievērojot attiecīgās nozares iezīmes, būtu jāņem vērā gan tehniski, gan attiecīgā gadījumā netehniski faktori, tai skaitā tie, kas definēti Ieteikumā (ES) 2019/534, ES mēroga koordinētajā 5G tīklu drošības novērtējumā un ES rīkkopā par 5G kiberdrošību, kuru saskaņojusi sadarbības grupa. Lai apzinātu piegādes ķēdes, par kurām būtu jāveic koordinēts riska novērtējums, būtu jāņem vērā šādi kritēriji: i) tas, ciktāl būtiskās un svarīgās vienības izmanto īpašus kritiskus IKT pakalpojumus, sistēmas vai produktus un paļaujas uz tiem; ii) īpašu kritisku IKT pakalpojumu, sistēmu vai produktu nozīmīgums kritisku vai sensitīvu funkciju veikšanā, arī persondatu apstrādē; iii) alternatīvu IKT pakalpojumu, sistēmu vai produktu pieejamība; iv) IKT pakalpojumu, sistēmu vai produktu vispārējās piegādes ķēdes noturība pret notikumiem, kas izraisa traucējumus, un v) attiecībā uz jauniem IKT pakalpojumiem, sistēmām vai produktiem – to iespējamais turpmākais nozīmīgums vienību darbībām.

(48) Lai racionalizētu juridiskos pienākumus, kas noteikti publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem un uzticamības pakalpojumu sniedzējiem saistībā ar to tīklu un informācijas sistēmu drošību, un lai šīs vienības un to attiecīgās kompetentās iestādes varētu gūt labumu no tiesiskā regulējuma, kas izveidots ar šo direktīvu (ieskaitot par riska un incidentu risināšanu atbildīgo *CSIRT* izraudzīšanos, kompetento iestāžu un struktūru piedalīšanos sadarbības grupas un *CSIRT* tīkla darbā), tie būtu jāiekļauj šīs direktīvas piemērošanas jomā. Tāpēc atbilstošie noteikumi, kas paredzēti Eiropas Parlamenta un Padomes Regulā (ES) Nr. 910/2014 [22] un Eiropas Parlamenta un Padomes Direktīvā (ES) 2018/1972 [23] saistībā ar drošības un paziņošanas **prasību** piemērošanu šo veidu vienībām, būtu jāatceļ.

---

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

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

(48.a) Šajā direktīvā noteiktie drošības pienākumi būtu jāuzskata par papildinājumu prasībām, kas uzticamības pakalpojumu sniedzējiem noteiktas saskaņā ar Regulu (ES) Nr. 910/2014 (*eIDAS* regula). Būtu jāprasa, lai uzticamības pakalpojumu sniedzēji saskaņā ar šo direktīvu veic visus atbilstīgos un samērīgos pasākumus to risku pārvaldīšanai, kas tiek radīti to pakalpojumiem, tostarp attiecībā uz klientiem un atkarīgajām trešām personām, un ziņo par drošības incidentiem. Šādiem drošības un ziņošanas pienākumiem būtu jāattiecas arī uz sniegtā pakalpojuma fizisko aizsardzību. Regulas (ES) 910/2014 24. pantu turpina piemērot.

(48.aa) Dalībvalstis var piešķirt *eIDAS* uzraudzības iestādēm kompetento iestāžu lomu uzticamības pakalpojumu jomā, lai nodrošinātu pašreizējās prakses turpināšanu un izmantotu *eIDAS* regulas piemērošanā gūtās zināšanas un pieredzi. Ja minētā loma ir piešķirta citai iestādei, valsts kompetentajām iestādēm saskaņā ar šo direktīvu būtu laikus cieši jāsadarbojas, apmainoties ar attiecīgo informāciju, lai nodrošinātu efektīvu uzraudzību un uzticamības pakalpojumu sniedzēju atbilstību šajā direktīvā un Regulā [XXXX/XXXX] noteiktajām prasībām.

Attiecīgā gadījumā valsts kompetentajai iestādei saskaņā ar šo direktīvu būtu nekavējoties jāinformē *eIDAS* uzraudzības iestāde par visiem paziņotajiem būtiskajiem kiberdraudiem vai incidentiem, kas ietekmē uzticamības pakalpojumus, kā arī par jebkādu uzticamības pakalpojumu sniedzēja neatbilstību šīs direktīvas prasībām. Dalībvalstis ziņošanas nolūkā var attiecīgā gadījumā izmantot vienoto kontaktpunktu, kas izveidots, lai panāktu vienotu un automātisku ziņošanu par incidentiem gan *eIDAS* uzraudzības iestādei, gan šajā direktīvā minētajai kompetentajai iestādei. Noteikumiem par ziņošanas pienākumiem nebūtu jāskar Regula (ES) 2016/679 un Eiropas Parlamenta un Padomes Direktīva 2002/58/EK [24].

---

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

(49) Attiecīgā gadījumā un lai izvairītos no nevajadzīgiem traucējumiem, **transponēšanas pasākumos, ko dalībvalstis īsteno saistībā ar šo direktīvu**, būtu jāņem vērā esošās valsts pamatnostādnes [...], kas pieņemtas, lai transponētu ar drošības pasākumiem saistītos noteikumus, kuri paredzēti Direktīvas (ES) 2018/1972[...] 40. un 41. pantā, **tādējādi balstoties uz zināšanām un prasmēm, kas jau iegūtas, piemērojot Direktīvu (ES) 2018/1972, attiecībā uz drošības riska pārvaldības pasākumiem un incidentu paziņojumiem**. ***ENISA*** **var arī izstrādāt norādījumus par drošības un ziņošanas prasībām publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem, lai atvieglotu saskaņošanu, pāreju un pēc iespējas samazinātu traucējumus. Dalībvalstis var piešķirt valsts regulatīvajām iestādēm kompetento iestāžu lomu elektronisko sakaru jomā, lai nodrošinātu pašreizējās prakses turpināšanu un izmantotu Direktīvas (ES) 2018/1972 piemērošanā gūtās zināšanas un pieredzi.**

(50) Tā kā palielinās numurneatkarīgo starppersonu sakaru pakalpojumu nozīme, ir jānodrošina, ka uz tiem attiecas arī piemērotas drošības prasības, ņemot vērā to specifiku un ekonomisko svaru. Šādu pakalpojumu sniedzējiem tādējādi būtu arī jānodrošina radītajam riskam atbilstošs tīklu un informācijas sistēmu drošības līmenis. Tā kā numurneatkarīgo starppersonu sakaru pakalpojumu sniedzēji nemēdz faktiski kontrolēt signālu pārraidi tīklos, risku šādiem pakalpojumiem savā ziņā var uzskatīt par zemāku nekā tradicionālajiem elektronisko sakaru pakalpojumiem. Tas pats attiecas uz starppersonu sakaru pakalpojumiem, kuros izmanto numurus un kuros netiek īstenota faktiska kontrole pār signālu pārraidi.

(51) Iekšējais tirgus ir vairāk atkarīgs no interneta darbības nekā jebkad iepriekš. Praktiski visu būtisko un svarīgo vienību pakalpojumi ir atkarīgi no internetā sniegtajiem pakalpojumiem. Lai nodrošinātu būtisko un svarīgo vienību pakalpojumu netraucētu sniegšanu, ir svarīgi, lai publiskajiem elektronisko sakaru tīkliem, piemēram, interneta pamattīkliem vai zemūdens sakaru kabeļiem, būtu ieviesti atbilstīgi kiberdrošības pasākumi un lai tie ziņotu par saistītajiem incidentiem.

(52) Attiecīgā [...] **gadījumā** vienībām būtu jāinformē to pakalpojumu saņēmēji par konkrētiem [...] pasākumiem, kurus tie var veikt, lai mazinātu **no būtiska kiberdrauda** izrietošo risku, kas tiem rodas. **Vienībām attiecīgā gadījumā un jo īpaši gadījumos, kad būtiskais kiberdrauds var materializēties, par šādu apdraudējumu būtu jāpaziņo vienlaikus gan kompetentajām iestādēm vai *CSIRT*, gan saviem pakalpojumu saņēmējiem.** Prasībai informēt lietotājus par šādiem apdraudējumiem nebūtu jāatbrīvo vienības no pienākuma par saviem līdzekļiem veikt atbilstīgus un steidzamus pasākumus, lai izlabotu vai likvidētu jebkurus kiberdraudus un atjaunotu normālu pakalpojuma drošības līmeni. Šāda informācija par [...]**kiber**draudiem būtu jāsniedz saņēmējiem bez maksas.

(53) Jo īpaši publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem būtu jāinformē pakalpojumu saņēmēji par konkrētiem un nozīmīgiem kiberdraudiem un par pasākumiem, ko tie var veikt, lai aizsargātu to sakaru drošību, izmantojot, piemēram, konkrētu veidu programmatūru vai šifrēšanas tehnoloģijas.

(54) Lai garantētu elektronisko sakaru tīklu un pakalpojumu drošību, būtu jāveicina šifrēšanas, jo īpaši pilnīgas šifrēšanas, izmantošana, kam nepieciešamības gadījumā saskaņā ar principiem par drošību un privātumu pēc noklusējuma 18. panta nolūkos vajadzētu būt obligātai šādu pakalpojumu sniedzējiem un tīklu nodrošinātājiem. Pilnīgas šifrēšanas izmantošana būtu jāsaskaņo ar dalībvalstu pilnvarām, lai nodrošinātu dalībvalstu būtisko drošības interešu un sabiedrības aizsardzību un ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem atbilstoši Savienības tiesību aktiem. Risinājumos par likumīgu piekļuvi informācijai pilnīgi šifrētos sakaros būtu jāsaglabā šifrēšanas efektivitāte privātuma un sakaru drošības aizsardzībā, vienlaikus efektīvi reaģējot uz noziedzīgiem nodarījumiem.

(55) Šī direktīva nosaka divposmu pieeju attiecībā uz incidentu paziņošanu, lai panāktu pareizo līdzsvaru starp ātru ziņošanu, kas palīdz mazināt incidentu iespējamo izplatīšanos un ļauj vienībām lūgt atbalstu, no vienas puses, un padziļinātu ziņošanu, kurā gūst vērtīgu mācību no individuāliem incidentiem un laika gaitā uzlabo individuālu uzņēmumu un visu nozaru noturību pret kiberdraudiem, no otras puses. Ja vienības konstatē incidentu, tām vajadzētu būt pienākumam iesniegt sākotnējo paziņojumu 24 stundu laikā, kā arī galīgo ziņojumu ne vēlāk kā viena mēneša laikā. Sākotnējā paziņojumā būtu jāiekļauj tikai informācija, kas ir obligāti nepieciešama, lai informētu kompetentās iestādes par incidentu un vajadzības gadījumā ļautu vienībai lūgt palīdzību. Šādā paziņojumā attiecīgā gadījumā būtu jānorāda, vai incidentu varētu būt izraisījusi nelikumīga vai ļaunprātīga darbība. Dalībvalstīm būtu jānodrošina, ka prasība iesniegt šo sākotnējo paziņojumu nenovirza ziņotājas vienības resursus no darbībām, kas saistītas ar incidentu risināšanu un kas būtu jānosaka par prioritārām. Lai turpmāk novērstu to, ka incidentu paziņošanas pienākumi novirza resursus no reaģēšanas uz incidentiem vai var citādi traucēt vienību centienus šajā saistībā, dalībvalstīm būtu arī jāparedz, ka pienācīgi pamatotos gadījumos un pēc vienošanās ar kompetentajām iestādēm vai *CSIRT* attiecīgā vienība var atkāpties no 24 stundu termiņa sākotnējam paziņojumam un viena mēneša termiņa galīgajam ziņojumam.

(55.a) Proaktīva pieeja kiberdraudiem ir kiberdrošības riska pārvaldības būtisks komponents, kam būtu jāļauj kompetentajām iestādēm efektīvi novērst kiberdraudu materializēšanos reālos incidentos, kas var radīt ievērojamus materiālos vai nemateriālos zaudējumus. Šajā nolūkā ļoti svarīgi ir ziņot par būtiskiem kiberdraudiem.

(56) Būtiskas un svarīgas vienības bieži atrodas situācijā, kad konkrēts incidents, ņemot vērā tā iezīmes, ir jāpaziņo dažādām iestādēm, jo to paredz paziņošanas pienākumi, kas ietverti dažādos tiesību instrumentos. Šādi gadījumi rada papildu slogus un var arī izraisīt nenoteiktību attiecībā uz šādu paziņojumu formātu un procedūrām. Ņemot to vērā, kā arī lai vienkāršotu ziņošanu par drošības incidentiem, dalībvalstis [...] **varētu** izveidot *vienotu kontaktpunktu* visiem paziņojumiem, kas jāsniedz saskaņā ar šo direktīvu un arī citiem Savienības tiesību aktiem, piemēram, Regulu (ES) 2016/679 un Direktīvu 2002/58/EK. *ENISA* kopā ar sadarbības grupu būtu jāizstrādā vienotas ziņojumu veidnes, pieņemot pamatnostādnes, ar kurām vienkāršo un racionalizē ziņojamo informāciju, ko pieprasa Savienības tiesību akti, un mazina slogus uzņēmumiem.

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

(58) Incidentu dēļ daudzos gadījumos tiek apdraudēti persondati. Šajā saistībā kompetentajām iestādēm būtu jāsadarbojas un jāapmainās ar informāciju par visiem būtiskajiem jautājumiem ar datu aizsardzības iestādēm un uzraudzības iestādēm atbilstoši Direktīvai 2002/58/EK.

(59) Lai garantētu DNS drošību, stabilitāti un noturību, kas savukārt veicina vienādi augsta līmeņa kiberdrošību Savienībā, ir svarīgi uzturēt precīzas un pilnīgas domēnu nosaukumu un reģistrācijas datu (tā dēvētie "*WHOIS* dati") datubāzes un nodrošināt likumīgu piekļuvi šādiem datiem. Ja tiek apstrādāti persondati, šādā apstrādē ievēro Savienības datu aizsardzības tiesību aktus.

(60) Šādu datu savlaicīga pieejamība publiskajām iestādēm, tai skaitā kompetentajām iestādēm atbilstoši Savienības vai valstu tiesību aktiem, lai novērstu un izmeklētu noziedzīgus nodarījumus vai sodītu par tiem, *CERT*, [...]*CSIRT* un – attiecībā uz to klientu datiem – elektronisko sakaru tīklu nodrošinātājiem un pakalpojumu sniedzējiem un kiberdrošības tehnoloģiju nodrošinātājiem un pakalpojumu sniedzējiem, kas darbojas minēto klientu vārdā, ir svarīga, lai novērstu un apkarotu domēnu nosaukumu sistēmu ļaunprātīgu izmantošanu, jo īpaši lai novērstu un atklātu kiberdrošības incidentus un ziņotu par tiem. Šādā piekļuvē būtu jāievēro Savienības datu aizsardzības tiesību akti, ciktāl tā ir saistīta ar persondatiem.

(61) Lai nodrošinātu precīzu un pilnīgu domēnu nosaukumu reģistrācijas datu pieejamību, ALD reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD (tā dēvētajiem reģistratoriem), būtu jāsavāc domēnu nosaukumu reģistrācijas dati un jāgarantē to integritāte un pieejamība. **Attiecībā uz reģistrācijas datiem vienībām jo īpaši būtu jāpārbauda reģistrētāja nosaukums un e-pasta adrese.** [...] ALD reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, būtu jānosaka politika un procedūras precīzu un pilnīgu reģistrācijas datu vākšanai un uzturēšanai, kā arī neprecīzu reģistrācijas datu novēršanai un izlabošanai saskaņā ar Savienības datu aizsardzības noteikumiem.

(62) ALD reģistriem un vienībām, kas tiem sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jādara publiski pieejami domēnu nosaukumu reģistrācijas dati, uz kuriem neattiecas Savienības datu aizsardzības noteikumi, piemēram, dati, kas attiecas uz juridiskām personām [25]. ALD reģistriem un vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, būtu arī jānodrošina leģitīmiem piekļuves prasītājiem likumīga piekļuve īpašiem domēnu nosaukumu reģistrācijas datiem par fiziskām personām saskaņā ar Savienības datu aizsardzības tiesību aktiem. Dalībvalstīm būtu jānodrošina, ka ALD reģistri un vienības, kas tiem sniedz domēnu nosaukumu reģistrācijas pakalpojumus, bez nepamatotas kavēšanās atbild uz [...] pieprasījumiem izpaust domēnu nosaukumu reģistrācijas datus, **ko iesnieguši tādi leģitīmi piekļuves prasītāji kā kompetentās iestādes atbilstoši Savienības vai valstu tiesību aktiem valsts drošības un krimināltiesību jomā vai *CSIRT***. ALD reģistriem un vienībām, kas tiem sniedz domēnu nosaukumu reģistrācijas pakalpojumus, būtu jānosaka politika un procedūras reģistrācijas datu, tai skaitā pakalpojumu līmeņa līgumu, publicēšanai un izpaušanai, lai izpildītu leģitīmo piekļuves prasītāju piekļuves pieprasījumus. Piekļuves procedūrā var arī ietvert saskarnes, portāla vai cita tehniska rīka izmantošanu, lai nodrošinātu efektīvu sistēmu reģistrācijas datu pieprasīšanai un piekļūšanai tiem. **Dalībvalstīm būtu jānodrošina, ka visu veidu piekļuve domēna reģistrācijas datiem (gan persondatiem, gan nepersondatiem) ir bez maksas.** Lai veicinātu saskaņotu praksi visā iekšējā tirgū, Komisija var pieņemt pamatnostādnes par šādām procedūrām, neskarot Eiropas Datu aizsardzības kolēģijas kompetences, **ievērojot un papildinot starptautiskos standartus, ko izstrādājusi daudzpusēja ieinteresēto personu kopiena**.

---

25 [...]Eiropas Parlamenta [...]un Padomes Regulas (ES) 2016/679 14. apsvērums: "šī regula neattiecas uz tādu personas datu apstrādi, kas skar juridiskas personas un jo īpaši uzņēmumus, kuriem ir juridiskas personas statuss, tostarp juridiskās personas nosaukumu, uzņēmējdarbības formu un kontaktinformāciju".

(63) [...] Būtiskajām un svarīgajām vienībām atbilstoši šai direktīvai vajadzētu būt tās dalībvalsts jurisdikcijā, kurā tās sniedz pakalpojumus. **Vienībām, kas minētas šīs direktīvas I pielikuma 1.–7. punktā un 10. punktā, uzticamības pakalpojumu sniedzējiem un interneta plūsmu apmaiņas punktu nodrošinātājiem, kas minēti I pielikuma 8. punktā un II pielikuma 1.–5. punktā, vajadzētu būt tās dalībvalsts jurisdikcijā, kurā tie ir iedibināti.** 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 nolemj īstenot jurisdikciju, tām būtu jāizvairās no tā, ka viena un tā pati rīcība par šajā direktīvā noteikto pienākumu neizpildi tiek sodīta vairāk nekā vienu reizi.**

(64) Lai ņemtu vērā DNS pakalpojumu sniedzēju, ALD nosaukumu reģistru, **vienību, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD**, satura piegādes tīklu nodrošinātāju, mākoņdatošanas pakalpojumu sniedzēju, datu centru pakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju pakalpojumu un darbību pārrobežu raksturu, tikai vienai dalībvalstij vajadzētu būt jurisdikcijai pār šīm vienībām. Jurisdikcija būtu jāpiedēvē tai dalībvalstij, kurā attiecīgajai vienībai ir tās galvenā iedibinājuma vieta Savienībā. Iedibinājuma vietas kritērijs šīs direktīvas nolūkos ietver darbības efektīvu īstenošanu ar stabila veidojuma starpniecību. Šāda veidojuma juridiskā forma neatkarīgi no tā, vai tas ir filiāle vai meitasuzņēmums ar juridiskas personas statusu, šajā saistībā nav noteicošais faktors.

Tam, vai šis kritērijs ir izpildīts, vajadzētu būt atkarīgam no tā, vai tīklu un informācijas sistēmas fiziski atrodas noteiktā vietā; šādu sistēmu klātbūtne un izmantošana pati par sevi nav uzskatāma par šādu galveno iedibinājuma vietu un tāpēc nav izšķirošs kritērijs galvenās iedibinājuma vietas noteikšanai. Par galveno iedibinājuma vietu būtu jāuzskata vieta, kur **galvenokārt** Savienībā tiek pieņemti ar kiberdrošības riska pārvaldības pasākumiem saistīti lēmumi. Parasti tā ir vieta, kur atrodas uzņēmumu centrālā administrācija Savienībā. Ja **nevar noteikt vietu, kur galvenokārt tiek pieņemti šādi lēmumi, vai** ja šādus lēmumus nepieņem Savienībā, būtu jāuzskata, ka galvenā iedibinājuma vieta ir dalībvalstīs, kurās vienībai ir iedibinājuma vieta ar vislielāko darbinieku skaitu Savienībā. Ja pakalpojumus sniedz uzņēmumu grupa, par uzņēmumu grupas galveno uzņēmējdarbības vietu būtu jāuzskata kontrolējošā uzņēmuma galvenā iedibinājuma vieta.

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

(64.aa) Lai nodrošinātu skaidru pārskatu par DNS pakalpojumu sniedzējiem, ALD nosaukumu reģistriem, vienībām, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, satura piegādes tīklu nodrošinātājiem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, kas saskaņā ar šīs direktīvas darbības jomu sniedz pakalpojumus visā Savienībā, *ENISA* būtu jāizveido un jāuztur šādu vienību reģistrs, pamatojoties uz dalībvalstu saņemtajiem paziņojumiem, attiecīgā gadījumā izmantojot savus valsts mehānismus patstāvīgai paziņošanai. Lai nodrošinātu šajā reģistrā iekļaujamās informācijas precizitāti un pilnīgumu, dalībvalstīm būtu jāiesniedz *ENISA* to valsts reģistros pieejamā informācija par minētajām vienībām. *ENISA* un dalībvalstīm būtu jāveic pasākumi šādu reģistru sadarbspējas veicināšanai, vienlaikus nodrošinot konfidenciālas vai klasificētas informācijas aizsardzību.

(65) Gadījumos, kad DNS pakalpojumu sniedzējs, ALD nosaukumu reģistrs, satura piegādes tīklu nodrošinātājs, mākoņdatošanas pakalpojumu sniedzējs, datu centra pakalpojumu sniedzējs un digitālo pakalpojumu sniedzējs, kam nav iedibinājuma vietas Savienībā, piedāvā pakalpojumus Savienībā, tam būtu jāizraugās pārstāvis. Lai noteiktu, vai šāda vienība piedāvā pakalpojumus Savienībā, būtu jāpārliecinās, vai ir acīmredzami tas, ka vienība plāno piedāvāt pakalpojumus personām vienā vai vairākās dalībvalstīs. Lai pārliecinātos par šādu nodomu, nepietiek tikai ar to vien, ka Savienībā ir pieejama vienības vai starpnieka tīmekļa vietne vai e-pasta adrese un cita kontaktinformācija vai ka tiek izmantota valoda, ko parasti izmanto trešā valstī, kurā ir vienības iedibinājuma vieta. Tomēr tādi faktori kā, piemēram, izmantotā valoda vai valūta, ko parasti izmanto vienā vai vairākās dalībvalstīs, piedāvājot pasūtīt pakalpojumus šajā citā valodā, vai Savienībā esošu klientu vai lietotāju pieminēšana var liecināt par to, ka vienība plāno piedāvāt pakalpojumus Savienībā. Pārstāvim būtu jārīkojas vienības vārdā, un kompetentajām iestādēm vai *CSIRT* vajadzētu būt iespējai sazināties ar pārstāvi. Pārstāvis būtu jāizraugās nepārprotami ar vienības rakstisku pilnvarojumu rīkoties tās vārdā attiecībā uz tās pienākumiem saskaņā ar šo direktīvu, tai skaitā attiecībā uz ziņošanu par incidentiem.

(66) Ja notiek apmaiņa ar informāciju, ko saskaņā ar valsts vai Savienības tiesību aktiem uzskata par klasificētu, vai šāda informācija tiek paziņota vai citādi koplietota atbilstoši šīs direktīvas noteikumiem, būtu jāpiemēro atbilstošie īpašie noteikumi par rīcību ar klasificētu informāciju.

(67) Tā kā kiberdraudi kļūst sarežģītāki un attīstītāki, labi atklāšanas un profilakses pasākumi lielā mērā ir atkarīgi no regulāras apdraudējumu un neaizsargātības izlūkdatu apmaiņas starp vienībām. Informācijas apmaiņa veicina lielāku informētību par kiberdraudiem, kas savukārt uzlabo vienību spēju novērst draudu pārtapšanu reālos incidentos un ļauj vienībām labāk ierobežot incidentu ietekmi un efektīvāk novērst to sekas. Nepastāvot Savienības līmeņa norādījumiem, šādu izlūkdatu apmaiņu, šķiet, ir kavējuši vairāki faktori, jo īpaši nenoteiktība attiecībā uz saderību ar konkurences un atbildības noteikumiem.

(68) Vienības būtu jāmudina kolektīvi izmantot to individuālās zināšanas un praktisko pieredzi stratēģiskā, taktiskā un darbības līmenī, lai uzlabotu to spējas pienācīgi novērtēt un uzraudzīt kiberdraudus, aizsargāties pret tiem un reaģēt uz tiem. Tādējādi ir nepieciešams nodrošināt iespējas, lai parādītos Savienības līmeņa mehānismi brīvprātīgiem informācijas apmaiņas pasākumiem. Šajā nolūkā dalībvalstīm būtu aktīvi jāatbalsta un jāmudina šādos informācijas apmaiņas mehānismos piedalīties arī attiecīgās vienības, kas nav šīs direktīvas darbības jomā. Minētie mehānismi būtu jāvada, pilnībā ievērojot Savienības konkurences noteikumus, kā arī Savienības datu aizsardzības tiesību aktu noteikumus.

(69) [...] Ciktāl tas ir stingri nepieciešams un samērīgi tīklu un informācijas drošības nodrošināšanai, **persondatu apstrādi**, ko veic **būtiskas un svarīgas** vienības [...] un drošības tehnoloģiju nodrošinātāji un pakalpojumu sniedzēji, **varētu uzskatīt par nepieciešamu, lai izpildītu juridisku pienākumu, vai** [...] par tādu, kas notiek attiecīgā datu pārziņa leģitīmajās interesēs**[...]**, kā minēts Regulā (ES) 2016/679. Tajā **varētu** [...] ietvert pasākumus, kas saistīti ar incidentu novēršanu, atklāšanu, analīzi un reaģēšanu uz tiem, pasākumus, kas veicina informētību par īpašiem kiberdraudiem, informācijas apmaiņu neaizsargātības izlabošanas un koordinētas atklāšanas kontekstā, brīvprātīgu informācijas apmaiņu par minētajiem incidentiem, [...] kiberdraudiem un neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem. Šādiem pasākumiem var būt vajadzīga [...] **dažādu** veidu persondatu apstrāde, **piemēram**: IP adreses, vienotie resursu vietrāži (URL), domēnu nosaukumi un e-pasta adreses. **Persondatu apstrāde, ko veic kompetentās iestādes, *SPOC* un *CSIRT*, būtu jānosaka valsts tiesību aktos un jāuzskata par nepieciešamu, lai izpildītu juridisku pienākumu vai kādu uzdevumu, ko veic sabiedrības interesēs vai saistībā ar datu pārzinim likumīgi piešķirto oficiālo pilnvaru īstenošanu, kā minēts Regulas (ES) 2016/679 6. panta 1. punkta c) vai e) apakšpunktā.**

(69.a) Dalībvalstu tiesību aktos var paredzēt noteikumus, kas ļauj kompetentajām iestādēm, *SPOC* un *CSIRT* – ciktāl tas ir stingri nepieciešams un samērīgi būtisku un svarīgu vienību tīklu un informācijas sistēmu drošības nodrošināšanai – apstrādāt īpašas persondatu kategorijas saskaņā ar Regulas (ES) 2016/679 9. pantu [...], jo īpaši paredzot piemērotus un konkrētus pasākumus fizisko personu pamattiesību un interešu aizsardzībai, tostarp tehniskus ierobežojumus šādu datu atkalizmantošanai un modernu drošības un privātuma saglabāšanas pasākumu, piemēram, pseidonimizācijas vai šifrēšanas, izmantošanai, ja anonimizācija var būtiski ietekmēt sasniedzamo mērķi.

(70) Lai nostiprinātu uzraudzības pilnvaras un darbības, kas palīdz nodrošināt efektīvu atbilstību, šajā direktīvā būtu jāparedz minimāls to uzraudzības darbību un līdzekļu saraksts, ar kuru starpniecību kompetentās iestādes **var** [...] uzraudzīt būtiskas un svarīgas vienības. Turklāt šajā direktīvā būtu jānosaka uzraudzības režīma nošķirums starp būtiskajām un svarīgajām vienībām, lai nodrošinātu pienākumu taisnīgu līdzsvaru gan vienībām, gan kompetentajām iestādēm. Tādējādi būtiskajām vienībām būtu jāpiemēro pilnīgs uzraudzības režīms (*ex ante* un *ex post*), savukārt svarīgajām vienībām būtu jāpiemēro vieglais uzraudzības režīms – tikai *ex post*. Attiecībā uz pēdējām minētajām tas nozīmē, ka svarīgajām vienībām nebūtu **jāpiemēro prasība**[...] sistemātiski **dokumentēt** atbilstību kiberdrošības riska pārvaldības prasībām, savukārt kompetentajām iestādēm būtu jāīsteno atpakaļejoša *ex post* pieeja uzraudzībai, un tādējādi tām nav vispārēja pienākuma uzraudzīt minētās vienības. **Svarīgas vienības var būt pakļautas *ex-post* uzraudzībai, pamatojoties uz pierādījumiem vai jebkādām norādēm, vai informāciju, kas darīta zināma kompetentajām iestādēm un ko šīs iestādes uzskata par tādu, kas liecina par šajā direktīvā noteikto pienākumu iespējamu neizpildi. Piemēram, tie varētu būt tāda veida pierādījumi, norādes vai informācija, ko kompetentajām iestādēm sniedz citas iestādes, vienības, pilsoņi, mediji vai citi avoti, publiski pieejama informācija, vai tie var izrietēt no citām darbībām, ko kompetentās iestādes veic, pildot savus uzdevumus.**

(70.a) Veicot *ex ante* uzraudzību, kompetentajām iestādēm vajadzētu būt iespējai samērīgā veidā lemt par prioritāšu noteikšanu attiecībā uz uzraudzības darbību un to rīcībā esošo līdzekļu 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 būtisku vienību klasificēšanai riska kategorijās un atbilstošas uzraudzības darbības un līdzekļus, kas ieteicami katrai riska kategorijai, piemēram, pārbaužu uz vietas vai mērķtiecīgu drošības revīziju, vai drošības skenēšanas izmantošana, biežums vai veids, pieprasāmās informācijas veids un minētās informācijas detalizācijas pakāpe. Šādu uzraudzības metodiku var papildināt arī ar darba programmām, un to var regulāri novērtēt un pārskatīt, tostarp attiecībā uz tādiem aspektiem kā resursu piešķiršana un vajadzības.

(70.aa) Attiecībā uz valsts pārvaldes vienībām uzraudzības pilnvaras būtu jāīsteno atbilstoši valsts regulējumam un tiesiskajai kārtībai. Dalībvalstīm vajadzētu būt iespējai lemt par piemērotu, samērīgu un efektīvu uzraudzības un izpildes pasākumu noteikšanu attiecībā uz šīm vienībām.

(70.aaa) Lai pierādītu atbilstību konkrētiem kiberdrošības riska pārvaldības pasākumiem, dalībvalstis varētu pieprasīt būtiskām un svarīgām vienībām izmantot kvalificētus uzticamības pakalpojumus vai paziņotās elektroniskās identifikācijas shēmas saskaņā ar Regulu (ES) Nr. 910/2014.

(71) Lai izpilde būtu efektīva, būtu jānosaka minimāls to administratīvo sankciju saraksts, kuras piemēro par šajā direktīvā paredzēto kiberdrošības riska pārvaldības un ziņošanas pienākumu pārkāpumiem, izveidojot skaidru un konsekventu satvaru šādām sankcijām visā Savienībā. Būtu pienācīgi jāņem vērā pārkāpuma veids, smagums un ilgums, faktiskais izraisītais kaitējums vai zaudējumi vai iespējamais kaitējums vai zaudējumi, kas būtu varējuši rasties, tas, vai pārkāpums izdarīts tīši vai nolaidības dēļ, darbības, kas veiktas, lai novērstu vai mazinātu radīto kaitējumu un/vai zaudējumus, atbildības pakāpe vai jebkādi būtiski iepriekšēji pārkāpumi, sadarbības ar kompetento iestādi pakāpe un jebkādi citi vainu pastiprinoši vai mīkstinoši apstākļi. Sodu, arī administratīvu naudas sodu, uzlikšanai būtu jāpiemēro atbilstīgas procesuālās garantijas saskaņā ar vispārīgiem Savienības tiesību principiem un Eiropas Savienības Pamattiesību hartu, tai skaitā efektīva tiesību aizsardzība tiesā un pienācīgas procedūras.

(71.a) Noteikumi, kas attiecas uz tādu fizisko personu atbildību, kurām kādā vienībā ir konkrēti pienākumi, ja tās nav izpildījušas šajā direktīvā noteiktos pienākumus, neprasa dalībvalstīm nodrošināt kriminālvajāšanu vai noteikt civiltiesisko atbildību par zaudējumiem, kas šāda pārkāpuma dēļ radušies trešām personām.

(72) Lai nodrošinātu šajā direktīvā noteikto pienākumu efektīvu izpildi, katrai kompetentajai iestādei vajadzētu būt pilnvarām uzlikt administratīvus naudas sodus vai pieprasīt to uzlikšanu.

(73) Ja administratīvi naudas sodi tiek uzlikti uzņēmumam, minētajā nolūkā uzņēmums būtu jāsaprot kā uzņēmums saskaņā ar LESD 101. un 102. pantu. Ja administratīvi naudas sodi tiek uzlikti personām, kas nav uzņēmums, uzraudzības iestādei, apsverot atbilstošo naudas soda apjomu, būtu jāņem vērā vispārējais ienākumu līmenis dalībvalstī, kā arī attiecīgās personas ekonomiskā situācija. Dalībvalstīm būtu jānosaka, vai un kādā apmērā administratīvi naudas sodi būtu piemērojami publiskām iestādēm. Administratīva naudas soda uzlikšana neietekmē citu kompetento iestāžu pilnvaru piemērošanu vai citu tādu sodu piemērošanu, kas noteikti valsts tiesību normās, ar kurām transponē šo direktīvu.

(74) Dalībvalstis [...] **var** pieņemt noteikumus par krimināLsodiem, ko piemēro, ja tiek pārkāptas valsts tiesību normas, ar kurām transponē šo direktīvu. Tomēr krimināLsodu piemērošanai par šādu valsts tiesību normu pārkāpumiem un saistītu administratīvu sodu piemērošanai nebūtu jāizraisa *ne bis in idem* principa pārkāpšana, kā to interpretējusi Tiesa.

(75) Ja ar šo direktīvu netiek saskaņoti administratīvie sodi vai ja tas nepieciešams citos gadījumos, piemēram, šajā direktīvā noteikto pienākumu smagu pārkāpumu gadījumos, dalībvalstīm būtu jāievieš sistēma, kas paredz iedarbīgus, samērīgus un atturošus sodus. Šādu sodu – krimināLu vai administratīvu – raksturs būtu jānosaka ar dalībvalsts tiesību aktiem.

(76) Lai vēl vairāk nostiprinātu to sodu iedarbīgumu un atturošo ietekmi, kuri piemērojami par atbilstoši šai direktīvai noteikto pienākumu pārkāpumiem, kompetentajām iestādēm vajadzētu būt pilnvarotām piemērot sankcijas, kas var būt sertifikācijas vai atļaujas darbības apturēšana attiecībā uz visiem būtiskas vienības sniegtajiem pakalpojumiem vai to daļu un pagaidu aizliegums fiziskai personai pildīt vadības funkcijas. Ņemot vērā šādu sankciju smagumu un ietekmi uz vienību darbībām un galu galā uz to patērētājiem, tās būtu jāpiemēro tikai tā, lai tās būtu samērīgas attiecībā pret pārkāpuma smagumu, un ņemot vērā katra gadījuma īpašos apstākļus, tai skaitā to, vai pārkāpums izdarīts tīši vai neuzmanības dēļ, un veiktās darbības radītā kaitējuma un/vai zaudējumu novēršanai vai mazināšanai. Šādas sankcijas būtu jāpiemēro tikai kā *ultima ratio*, proti, tikai pēc tam, kad visas citas attiecīgās izpildes darbības, kas noteiktas šajā direktīvā, jau ir izsmeltas, un tikai par laikposmu līdz brīdim, kad vienības, uz kurām sankcijas attiecas, veic nepieciešamās darbības, lai izlabotu trūkumus vai izpildītu kompetentās iestādes prasības, saistībā ar kurām šādas sankcijas tikušas piemērotas. Šādu sankciju piemērošanā ievēro atbilstīgas procesuālās garantijas saskaņā ar vispārīgiem Savienības tiesību principiem un Eiropas Savienības Pamattiesību hartu, tai skaitā efektīvu tiesību aizsardzību tiesā, pienācīgas procedūras, nevainīguma prezumpciju un tiesības uz aizstāvību.

(76.a) Lai nodrošinātu efektīvu uzraudzību un izpildi, jo īpaši lietās ar pārrobežu dimensiju, dalībvalstīm, kas ir saņēmušas savstarpējas palīdzības lūgumu, minētā pieprasījuma robežās būtu jāveic piemēroti uzraudzības un izpildes pasākumi attiecībā uz attiecīgo vienību, kas to teritorijā sniedz pakalpojumus vai kam tajā ir tīkls un informācijas sistēma.

(77) Ar šo direktīvu būtu jānosaka noteikumi par sadarbību starp kompetentajām iestādēm un uzraudzības iestādēm saskaņā ar Regulu (ES) 2016/679, lai vērstos pret pārkāpumiem, kas saistīti ar persondatiem.

(78) Šajā direktīvā būtu jāizvirza mērķis nodrošināt augstu atbildības līmeni par kiberdrošības riska pārvaldības pasākumiem un ziņošanas pienākumiem organizāciju līmenī. Šā iemesla dēļ to vienību pārvaldības struktūrām, uz kurām attiecas šīs direktīvas darbības joma, būtu jāapstiprina kiberdrošības riska pasākumi un jāuzrauga to īstenošana.

(79) Būtu jāievieš savstarpējas [...] **mācīšanās**[...] **sistēma**, **lai palīdzētu nostiprināt savstarpēju** uzticēšanos **un mācīties no paraugprakses un pieredzes**, ļaujot [...] dalībvalstu izraudzītajiem ekspertiem **apmainīties zināšanām** par[...] kiberdrošības politikas īstenošanu[...]. **Īstenojot savstarpējas mācīšanās sistēmu, īpaša uzmanība būtu jāpievērš tam, lai nodrošinātu, ka tā nerada nevajadzīgu vai nesamērīgu slogu attiecīgajām dalībvalstu iestādēm. Komisijai būtu jāizpēta visas iespējas, kā potenciāli garantēt finansiālu segumu izmaksām, kas varētu rasties saistībā ar savstarpējas mācīšanās misiju organizēšanu. Turklāt savstarpējas mācīšanās sistēmā būtu jāņem vērā līdzīgu mehānismu, piemēram, *CSIRT* tīkla salīdzinošās izvērtēšanas sistēmas, rezultāti, jārada pievienotā vērtība un jāizvairās no dublēšanās. Savstarpējas mācīšanās sistēmas īstenošanai nebūtu jāskar valstu vai Savienības tiesību akti par konfidenciālas un klasificētas informācijas aizsardzību. Pirms savstarpējas mācīšanās kārtu sākšanas dalībvalstis var veikt attiecīgo aspektu pašnovērtēšanu. Pēc sadarbības grupas pieprasījuma *ENISA* nepieciešamības gadījumā var sniegt norādījumus par pašnovērtējumu un attiecīgajām veidnēm. Dalībvalstis varētu pieņemt lēmumu publiskot savus ziņojumus.**

(80) [...]

(81) Lai nodrošinātu vienotus nosacījumus šīs direktīvas attiecīgo noteikumu īstenošanai attiecībā uz procesuālo kārtību, kas nepieciešama sadarbības grupas darbībai, ar riska pārvaldības pasākumiem saistītajiem tehniskajiem elementiem vai informācijas veidu, incidentu paziņojumu formātu un procedūru, **to vienību kategorijām, kurām ir jāizmanto konkrēti sertificēti IKT produkti, pakalpojumi un procesi**, būtu jādeleģē Komisijai īstenošanas pilnvaras. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 [26].

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

[26] 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.).

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

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

IR PIEŅĒMUŠI ŠO DIREKTĪVU.

I NODAĻA

Vispārīgi noteikumi

1. pants

Priekšmets

1. Šajā direktīvā ir paredzēti pasākumi ar mērķi nodrošināt vienādi augsta līmeņa kiberdrošību Savienībā, **lai uzlabotu iekšējā tirgus darbību**.

2. Minētajam nolūkam šajā direktīvā:

   a) ir noteikti dalībvalstu pienākumi pieņemt valsts kiberdrošības stratēģijas, izraudzīties valsts kompetentās iestādes, vienotos kontaktpunktus un datordrošības incidentu reaģēšanas vienības (*CSIRT*);

   b) ir noteikti kiberdrošības riska pārvaldības un ziņošanas pienākumi vienībām, kas minētas [...] **I un II pielikumā** [...];

   c) ir noteikti **noteikumi un** pienākumi attiecībā uz kiberdrošības informācijas apmaiņu.

2. pants

Darbības joma

1. Šī direktīva ir piemērojama **[...] I un II** pielikumā **minētajām** publiskām un privātām vienībām [...], **kuras izpilda vai pārsniedz maksimālos apjomus, kas noteikti vidējiem uzņēmumiem** [...] Komisijas Ieteikuma 2003/361/EK [27] nozīmē. **Minētā ieteikuma pielikuma 3. panta 4. punktu un 6. panta 2. punkta otro un trešo daļu nepiemēro šīs direktīvas nolūkā.**

2. [...]**Šī** direktīva ir piemērojama arī [...]neatkarīgi no **1. punktā minēto vienību**[...] lieluma, **ja**: [...]

   a) pakalpojumus sniedz kāda no šīm vienībām:

      i) publisko elektronisko sakaru tīklu **nodrošinātāji** vai publiski pieejamo elektronisko sakaru pakalpojumu **sniedzēji**, kas minēti I pielikuma 8. punktā;

      ii) kvalificēti uzticamības pakalpojumu sniedzēji, kas minēti I pielikuma XX. punktā;

      iii) nekvalificēti uzticamības pakalpojumu sniedzēji, kas minēti I pielikuma XX. punktā;

      iv) augstākā līmeņa domēnu nosaukumu reģistri [..], kas minēti I pielikuma 8. punktā;

   b) [...]

---

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

c) vienība ir vienīgais pakalpojuma sniedzējs, kas **dalībvalstī** sniedz pakalpojumu [...], **kas ir būtisks kritisku sabiedrisku vai ekonomisku darbību nodrošināšanai**;

d) vienības sniegtā pakalpojuma iespējamam traucējumam var būt [...] **būtiska** ietekme uz sabiedrības aizsardzību, sabiedrisko drošību vai sabiedrības veselību;

e) vienības sniegtā pakalpojuma iespējams traucējums var izraisīt [...] **būtiskus** sistēmiskus riskus, jo īpaši nozarēm, kurās šādam traucējumam var būt pārrobežu ietekme;

f) [...];

g) vienība ir identificēta kā kritiska vienība, ievērojot Eiropas Parlamenta un Padomes Direktīvu (ES) XXXX/XXXX [28] [Kritisko vienību noturības direktīva], **[**vai kā vienība, kas ir līdzvērtīga kritiskai vienībai, ievērojot minētās direktīvas 7. pantu**]**.

2.a Šī direktīva ir piemērojama arī centrālo valdību valsts pārvaldes vienībām, kas dalībvalstī par tādām atzītas saskaņā ar valsts tiesību aktiem un kas minētas I pielikuma 9. punktā, neatkarīgi no to lieluma. Dalībvalstis var noteikt, ka šī direktīva ir piemērojama arī valsts pārvaldes vienībām reģionālā un vietējā līmenī.

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

3. [...]

Šī direktīva neskar dalībvalstu pienākumus garantēt valsts drošību vai to pilnvaras aizsargāt citas valsts pamatfunkcijas, tostarp nodrošināt valsts teritoriālo integritāti un uzturēt likumību un kārtību.

3.a 1) Šo direktīvu nepiemēro:

a) vienībām, uz kurām neattiecas Savienības tiesību aktu darbības joma, un jebkurā gadījumā visām vienībām, kas galvenokārt veic darbības aizsardzības, valsts drošības, sabiedriskās drošības vai tiesībaizsardzības jomā, neatkarīgi no tā, kura vienība veic minētās darbības un vai vienība ir publiska vai privāta, neskarot 2. punktu;

b) vienībām, kas veic darbības tiesu iestāžu, parlamentu vai centrālo banku jomās.[...]

2) Ja valsts pārvaldes vienības veic darbības minētajās jomās tikai kā daļu no to vispārējām darbībām, tās pilnībā izslēdz no šīs direktīvas piemērošanas jomas.

3.aa Šo direktīvu nepiemēro:

i) darbībām, ko veic vienības, uz kurām neattiecas Savienības tiesību aktu darbības joma, un jebkurā gadījumā visām darbībām, kas saistītas ar valsts drošību vai aizsardzību, neatkarīgi no tā, kura vienība veic minētās darbības un vai vienība ir publiska vai privāta;

ii) darbībām, ko veic vienības tiesu iestādēs, parlamentos, centrālajās bankās un sabiedriskās drošības jomā, tostarp valsts pārvaldes vienības, kas veic tiesībaizsardzības darbības, lai novērstu, izmeklētu un atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus.

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

3.aaaa Šī direktīva neskar Savienības tiesību aktus par personas datu aizsardzību, konkrēti Regulu (ES) 2016/679 un Direktīvu 2002/58/EK.

3.b Šo direktīvu nepiemēro vienībām, uz kurām saskaņā ar *DORA* regulas 2. panta 4. punktu neattiecas Eiropas Parlamenta un Padomes Regulas (ES) XXXX/XXXX [*DORA* regula] prasības.

4. Šo direktīvu piemēro, neskarot [...] [29] [...] Eiropas Parlamenta un Padomes Direktīvas 2011/93/ES [30] un 2013/40/ES [31].

5. Neskarot LESD 346. pantu, informācijas – kas ir konfidenciāla, ievērojot Savienības un valstu tiesību normas, piemēram, normas par darījumdarbības konfidencialitāti, – apmaiņa notiek ar Komisiju un citām attiecīgajām iestādēm **saskaņā ar šo direktīvu** tikai tad, ja šāda apmaiņa ir nepieciešama šīs direktīvas piemērošanai. Apmainās tikai ar to informāciju, kas ir atbilstīga un samērīga šādas apmaiņas nolūkam. Informācijas apmaiņā ievēro minētās informācijas konfidencialitāti un aizsargā būtisko vai svarīgo vienību drošību un komerciālās intereses.

---

29 [...]

30 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.).

31 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.).

2.a pants

Būtiskas un svarīgas vienības

1. Vienības, kurām piemēro šo direktīvu, uzskata par būtiskām, ja tās ir:

i) šīs direktīvas I pielikuma 1.–8.a punktā un 10. punktā minētās vienības, kuras pārsniedz Komisijas Ieteikumā 2003/361/EK definētajiem vidējiem uzņēmumiem noteiktos maksimālos apjomus;

ii) vidēja lieluma vienības, kas minētas 2. panta 2. punkta a) apakšpunkta i) punktā;

iii) vienības, kas minētas šīs direktīvas 2. panta 2. punkta a) apakšpunkta ii) un iv) punktā, neatkarīgi no to lieluma;

iv) vienības, kas minētas šīs direktīvas 2. panta 2. punkta g) apakšpunktā un 2.a punktā, neatkarīgi no to lieluma;

v) vienības – ja tās ir dalībvalstu iedibinātas –, kuras saskaņā ar Direktīvu (ES) 2016/1148 vai valsts tiesību aktiem dalībvalstis bija identificējušas par pamatpakalpojumu sniedzējiem pirms šīs direktīvas stāšanās spēkā;

vi) II pielikumā minētās vienības, kas pārsniedz Komisijas Ieteikumā 2003/361/EK definētajiem vidējiem uzņēmumiem noteikto maksimālo apjomu un kuras dalībvalstis nosaka par būtiskām, pamatojoties uz 2. panta 2. punkta c)–e) apakšpunktā minētajiem kritērijiem;

vii) vidēja lieluma vienības Komisijas Ieteikuma 2003/361/EK nozīmē, ko dalībvalstis nosaka par būtiskām, pamatojoties uz 2. panta 2. punkta c)–e) apakšpunktā minētajiem kritērijiem;

viii) mikrovienības vai mazās vienības Komisijas Ieteikuma 2003/361/EK nozīmē, kas minētas 2. punkta a) apakšpunkta i) punktā vai identificētas saskaņā ar šā panta 2. punkta c)–e) apakšpunktu un ko dalībvalstis nosaka par būtiskām, pamatojoties uz valsts riska novērtējumiem.

2. Vienības, kurām piemēro šo direktīvu, uzskata par svarīgām, ja tās ir:

i) vienības, kas minētas šīs direktīvas I pielikumā un ir kvalificējamas kā vidējie uzņēmumi Komisijas Ieteikuma 2003/361/EK nozīmē, un vienības, kas minētas II pielikumā un kas izpilda vai pārsniedz maksimālos apjomus, kuri noteikti vidējiem uzņēmumiem Komisijas Ieteikuma 2003/361/EK [32] nozīmē;

ii) vienības, kas minētas šīs direktīvas 2. panta 2. punkta a) apakšpunkta iii) punktā, neatkarīgi no to lieluma;

iii) mazās vienības un mikrovienības, kas minētas 2. panta 2. punkta a) apakšpunkta i) punktā;

iv) mazās vienības un mikrovienības, ko dalībvalstis nosaka par svarīgām vienībām, pamatojoties uz 2. panta 2. punkta c)–e) apakšpunktu.

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

2.a pants

Paziņošanas mehānismi

1. **Dalībvalstis var izveidot valsts mehānismu patstāvīgai paziņošanai, saskaņā ar kuru visām vienībām, uz kurām attiecas šī direktīva, ir jāiesniedz vismaz savs nosaukums, adrese un kontaktinformācija, kā arī jānorāda nozare, kurā tās darbojas, vai to sniegtā pakalpojuma veids un attiecīgā gadījumā jāiesniedz to dalībvalstu saraksts, kurās attiecīgās vienības savus pakalpojumus sniedz kompetentajām iestādēm saskaņā ar šo direktīvu vai struktūrām, ko šajā nolūkā izraudzījušās dalībvalstis.**

2. Dalībvalstis [...] **attiecībā uz vienībām, ko tās identificējušas, ievērojot 2. panta 2. punkta b)–e) apakšpunktu, līdz [12 mēneši pēc šīs direktīvas transponēšanas termiņa beigām] iesniedz Komisijai vismaz attiecīgu informāciju par identificēto vienību skaitu, nozari, pie kuras tās pieder, vai to sniegtā pakalpojuma veidu, kas minēts pielikumos, un par konkrētajiem 2. panta 2. punkta nosacījumiem, saskaņā ar kuriem tās identificētas.** Dalībvalstis pārskata [...] **minēto informāciju** regulāri un pēc tam vismaz reizi divos gados un pēc nepieciešamības to atjaunina.

2.b pants

Nozarspecifiski Savienības akti

1. Ja [...] saskaņā ar **nozarspecifiskiem Savienības tiesību** aktiem [...] būtiskajām vai svarīgajām vienībām ir vai nu jāpieņem kiberdrošības riska pārvaldības pasākumi, vai jāpaziņo **būtiski** incidenti vai [...] kiberdraudi un ja šādas prasības to ietekmes ziņā ir vismaz līdzvērtīgas šajā direktīvā noteiktajiem pienākumiem, attiecīgos šīs direktīvas noteikumus, **tostarp noteikumus par uzraudzību un izpildi, kas paredzēti VI nodaļā, šādām vienībām** nepiemēro. **Ja nozarspecifiski Savienības tiesību akti neaptver visas vienības konkrētā nozarē, kas ietilpst šīs direktīvas darbības jomā, attiecīgos šīs direktīvas noteikumus turpina piemērot vienībām, uz kurām neattiecas minētie nozarspecifiskie noteikumi.**

2. Šā panta 1. punktā minētās prasības uzskata par ietekmes ziņā līdzvērtīgām šajā direktīvā noteiktajiem pienākumiem, ja attiecīgais nozarspecifiskais Savienības akts paredz tūlītēju, vajadzības gadījumā automātisku un tiešu piekļuvi incidentu paziņojumiem, ko kompetentās iestādes sniedz saskaņā ar šo direktīvu vai izraudzītajām *CSIRT*, un ja:

a) kiberdrošības riska pārvaldības pasākumi ir vismaz ietekmes ziņā līdzvērtīgi šīs direktīvas 18. panta 1. un 2. punktā noteiktajiem pasākumiem; vai

b) prasības paziņot par būtiskiem incidentiem ir vismaz ietekmes ziņā līdzvērtīgas 20. panta 1.–6. punktā noteiktajām prasībām.

3. Komisija periodiski pārskata šā panta 1. un 2. punktā paredzēto līdzvērtīgas ietekmes prasību piemērošanu attiecībā uz Savienības tiesību aktu nozarspecifiskajiem noteikumiem. Sagatavojot minētos periodiskos pārskatus, Komisija apspriežas ar sadarbības grupu un *ENISA*.

3. pants

Minimālā saskaņošana

Neskarot to pienākumus atbilstoši Savienības tiesību aktiem, dalībvalstis [...] var pieņemt vai paturēt spēkā noteikumus, kas nodrošina augstāku kiberdrošības līmeni **jomās, uz kurām attiecas šī direktīva**.

4. pants

Definīcijas

Šajā direktīvā piemēro šādas definīcijas:

1) "tīklu un informācijas sistēma" ir:

   a) elektronisko sakaru tīkls Direktīvas (ES) 2018/1972 2. panta 1. punkta nozīmē;

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

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

2) "tīklu un informācijas sistēmu drošība" ir tīklu un informācijas sistēmu spēja noteiktā uzticamības līmenī pretoties visiem **notikumiem**, kas **var** apdraudēt **[...]** glabājamo vai pārraidāmo, vai apstrādājamo datu pieejamību, autentiskumu, integritāti vai konfidencialitāti vai minēto tīklu un informācijas sistēmu piedāvātos vai ar to starpniecību pieejamos pakalpojumus;

2.a) "elektronisko sakaru pakalpojumi" ir elektronisko [...]sakaru pakalpojumi Direktīvas (ES) 2018/1972 2. panta 4. punkta nozīmē;

3) "kiberdrošība" ir kiberdrošība Eiropas Parlamenta un Padomes Regulas (ES) 2019/881 [33] 2. panta 1. punkta nozīmē;

4) "valsts **kiberdrošības** stratēģija" [...] ir saskaņots dalībvalsts satvars, kas nodrošina pārvaldību, lai sasniegtu stratēģiskus mērķus un prioritātes **kiberdrošības** [...] **jomā** [...] attiecīgajā dalībvalstī;

5) "incidents" ir jebkurš notikums, kas apdraud uzglabātu, 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;

5.a) "plašapmēra kiberdrošības incidents" ir incidents, kuram ir būtiska ietekme uz vismaz divām dalībvalstīm vai kura radītie traucējumi pārsniedz dalībvalsts spēju reaģēt uz to;

---

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

6) "incidenta risināšana" ir visas darbības un procedūras, kuru mērķis ir atklāt, analizēt un ierobežot incidentu, un reaģēšana uz to;

6.a) "risks" ir tādu zaudējumu vai traucējumu iespējamība, ko izraisa incidents, un to izsaka kā šādu zaudējumu vai traucējumu apjoma un minētā incidenta varbūtības apvienojumu;

(7) "kiberdrauds" ir kiberdrauds Regulas (ES) 2019/881 2. panta 8. punkta nozīmē;

7.**a) "nozīmīgs kiberdrauds" ir kiberdrauds, kuru, ņemot vērā tā tehniskās pamatīpašības, var uzskatīt par tādu, kas var nopietni ietekmēt kādas vienības vai tās lietotāju tīklu un informācijas sistēmas, radot ievērojamus materiālos vai nemateriālos zaudējumus;**

8) "neaizsargātība" ir IKT aktīva vai sistēmas [...] trūkums, uzņēmība vai nepilnība, ko var izmantot kiberdraudu gadījumā;

8.a) "gandrīz notikuši notikumi" ir notikumi, kas, iespējams, būtu varējuši nodarīt kaitējumu vienības vai tās lietotāju tīklam un informācijas sistēmām, bet kuru pilnīga izvēršanās tika sekmīgi novērsta;

9) "pārstāvis" ir jebkura fiziska vai juridiska persona, kura iedibināta Savienībā un ir skaidri izraudzīta rīkoties, lai pārstāvētu i) DNS pakalpojumu sniedzēju, augstākā līmeņa domēnu (ALD) nosaukumu reģistru, mākoņdatošanas pakalpojumu sniedzēju, datu centra pakalpojumu sniedzēju, satura piegādes tīkla nodrošinātāju, kā minēts I pielikuma 8. punktā, vai ii) vienības, kuras minētas II pielikuma [...] **6**. punktā un kuras nav iedibinātas Savienībā, un pie kurām var vērsties valsts kompetentā iestāde vai *CSIRT* vienības vietā attiecībā uz minētās vienības pienākumiem atbilstoši šai direktīvai;

10) "standarts" ir standarts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012 [34] 2. panta 1. punkta nozīmē;

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

12) "interneta plūsmu apmaiņas punkts (IPAP)" ir tīkla ierīce, kas nodrošina vairāk nekā divu neatkarīgu tīklu (autonomu sistēmu) savstarpēju savienošanu, galvenokārt lai veicinātu interneta datplūsmas apmaiņu; IPAP nodrošina savstarpēju savienošanu tikai autonomām sistēmām; IPAP nav vajadzīga interneta datplūsma starp jebkuru iesaistīto autonomo sistēmu pāri, lai šķērsotu jebkuru trešo autonomo sistēmu, un tas nemaina šādu datplūsmu un citādi neiejaucas tajā;

13) "domēnu nosaukumu sistēma (DNS)" ir hierarhiska sadalīta nosaukumu sistēma, kas ļauj galalietotājiem sasniegt pakalpojumus un resursus internetā;

14) "DNS pakalpojumu sniedzējs" ir vienība, kas sniedz rekursīvus vai autoritatīvus domēnu nosaukumu atrises pakalpojumus [...] **trešo pušu lietošanai, izņemot saknes nosaukumu serverus** [...];

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

15) "augstākā līmeņa domēnu nosaukumu reģistrs" ir vienība, kam deleģēts īpašs ALD un kas atbild par ALD pārvaldību, tai skaitā domēnu nosaukumu reģistrāciju ALD un ALD tehnisko darbību, kā arī tā nosaukumu serveru darbību, datubāzu uzturēšanu un ALD zonas datņu sadalīšanu starp nosaukumu serveriem, **vienlaikus izslēdzot situācijas, ka augstākā līmeņa domēnu nosaukumi tiek izmantoti tikai reģistrētāja paša vajadzībām**;

15.a) "vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD", ir ALD nosaukumu reģistri, ALD reģistratori un reģistratoru aģenti, piemēram, tālākpārdevēji un starpniekrservera pakalpojumu sniedzēji;

16) "digitāls pakalpojums" ir pakalpojums Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/1535 [35] 1. panta 1. punkta b) apakšpunkta nozīmē;

16.a) "uzticamības pakalpojumi" ir uzticamības pakalpojumi Regulas (ES) Nr. 910/2014 3. panta 16. punkta nozīmē;

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

16.b) "kvalificēts uzticamības pakalpojumu sniedzējs" ir kvalificēts uzticamības pakalpojumu sniedzējs Regulas (ES) Nr. 910/2014 3. panta 20. punkta nozīmē;

17) "tiešsaistes tirdzniecības vieta" ir digitāls pakalpojums Eiropas Parlamenta un Padomes Direktīvas 2005/29/EK [36] 2. panta n) punkta nozīmē;

18) "tiešsaistes meklētājprogramma" ir digitāls pakalpojums Eiropas Parlamenta un Padomes Regulas (ES) 2019/1150 [37] 2. panta 5. punkta nozīmē;

19) "mākoņdatošanas pakalpojums" ir digitāls pakalpojums, kas dod iespēju plaši un attālināti piekļūt kopīgojamu [...] datošanas resursu mērogojamam un elastīgam pūlam un pēc pieprasījuma to pārvaldīt**, arī tad, ja šie resursi ir izvietoti vairākās vietās**;

20) "datu centra pakalpojums" ir pakalpojums, kas ietver struktūras vai struktūru grupas, kuras paredzētas tāda informācijas tehnoloģijas un tīkla aprīkojuma centralizētai izmitināšanai, savstarpējai savienošanai un darbībai, kas sniedz datu uzglabāšanas, apstrādes un transportēšanas pakalpojumus kopā ar visām ierīcēm un infrastruktūrām jaudas sadalei un vides kontrolei;

---

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

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

21) "satura piegādes tīkls" ir ģeogrāfiski sadalītu serveru tīkls, kas nodrošina digitālā satura un pakalpojumu augstu pieejamību, piekļūstamību vai ātru piegādi interneta lietotājiem satura un pakalpojumu sniedzēju vārdā;

22) "sociālās tīklošanās pakalpojumu platforma" ir platforma, kas ļauj galalietotājiem pieslēgties, koplietot saturu, atklāt informāciju un savstarpēji sazināties, izmantojot vairākas ierīces, jo īpaši ar tērzētavu, paziņojumu, video un ieteikumu starpniecību[...];

23) "valsts pārvaldes vienība" ir vienība, **kas dalībvalstī par tādu ir atzīta saskaņā ar valsts tiesību aktiem**[...] un kas atbilst šādiem kritērijiem:

a) tā ir iedibināta ar mērķi apmierināt vispārējas vajadzības, un tai 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, reģionāla iestāde vai citi publisko tiesību subjekti, vai tās pārvaldību uzrauga minētās iestādes vai subjekti, vai tās vadībā, valdē vai uzraudzības padomē vairāk nekā pusi locekļu ieceļ valsts, reģionālās iestādes vai citi publisko tiesību subjekti;

d) tai ir pilnvaras adresēt fiziskām vai juridiskām personām administratīvus vai regulatīvus lēmumus, kas skar to tiesības saistībā ar personu, preču, pakalpojumu vai kapitāla pārrobežu pārvietošanos vai apriti.

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

25) "būtiska vienība" ir jebkura tāda veida vienība [...]**, kas minēta I pielikumā un atzīta par "būtisku" saskaņā ar 2.a panta 1. punktu**;

26) "svarīga vienība" ir jebkura tāda veida vienība [...], **kas minēta I un II pielikumā un atzīta par "svarīgu" saskaņā ar 2.a panta 2. punktu**.

26.a) "IKT produkts" ir IKT produkts Regulas (ES) 2019/881 2. panta 12. punkta nozīmē.

26.aa) "IKT pakalpojums" ir IKT pakalpojums Regulas (ES) 2019/881 2. panta 13. punkta nozīmē;

26.ab) "IKT process" ir IKT process Regulas (ES) 2019/881 2. panta 14. punkta nozīmē.

26.ac) "pārvaldīta pakalpojuma sniedzējs" ir jebkura vienība, kas sniedz tādus pakalpojumus kā tīkli, programmatūra, infrastruktūra un drošība, veicot pastāvīgas vai regulāras pārvaldības, atbalsta un aktīvas administrēšanas darbības klientu telpās, to pārvaldīta pakalpojuma sniedzēja datu centrā (mitināšana) vai trešās personas datu centrā.

26.ad) "pārvaldīta drošības pakalpojuma sniedzējs" ir jebkura vienība, kas sniedz drošības ierīču un sistēmu uzraudzības un pārvaldības ārpakalpojumu. Kopīgie pakalpojumi ietver pārvaldītu ugunsmūri, ielaušanās atklāšanu, virtuālu privāto tīklu, neaizsargātības skenēšanu un antivīrusu pakalpojumus.

Tas ietver arī augstas pieejamības drošības operāciju centru (vai nu no savām ierīcēm, vai no citiem datu centru pakalpojumu sniedzējiem) izmantošanu, lai sniegtu nepārtrauktus diennakts pakalpojumus, kas paredzēti, lai samazinātu to operatīvās drošības darbinieku skaitu, kuri uzņēmumam ir jāpieņem darbā, jāapmāca un jāpatur, lai uzturētu atbilstīgu drošības struktūru.

II NODAĻA

Koordinēti kiberdrošības tiesiskie regulējumi

5. pants

Valsts kiberdrošības stratēģija

1. Katra dalībvalsts pieņem valsts kiberdrošības stratēģiju, kurā nosaka stratēģiskos mērķus un atbilstīgus politikas un regulatīvus pasākumus, lai sasniegtu un uzturētu augstu kiberdrošības līmeni. Valsts kiberdrošības stratēģijā jo īpaši iekļauj:

   a) dalībvalstu kiberdrošības stratēģijas mērķus un prioritātes [...];

   b) pārvaldības satvaru minēto mērķu un prioritāšu sasniegšanai, tostarp politikas nostādnes, kas minētas 2. punktā, un [...] stratēģijas īstenošanā iesaistīto dažādo iestāžu un dalībnieku uzdevumus un pienākumus;

   c) [...] **norādes** attiecīgo aktīvu apzināšanai un kiberdrošības risku **novērtēšanai** konkrētajā dalībvalstī [...];

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

   e) [...]

f) politikas satvaru uzlabotai koordinācijai starp kompetentajām iestādēm atbilstoši šai direktīvai un Eiropas Parlamenta un Padomes Direktīvai (ES) XXXX/XXXX [38] [Kritisko vienību noturības direktīva], lai apmainītos ar informāciju **attiecīgā gadījumā** par **kiberdrošības riskiem,** [...] kiberdraudiem **un incidentiem, kā arī riskiem, draudiem un incidentiem, kas nav saistīti ar kiberdrošību**, un uzraudzības uzdevumu īstenošanu;

fa) politikas satvaru koordinācijai un sadarbībai starp kompetentajām iestādēm saskaņā ar šo direktīvu un kompetentajām iestādēm, kuras izraudzītas saskaņā ar nozarspecifiskiem tiesību aktiem.

2. Kā valsts kiberdrošības stratēģijas daļu dalībvalstis jo īpaši pieņem šādas politikas nostādnes:

a) politika, kas vērsta uz kiberdrošību piegādes ķēdē attiecībā uz IKT produktiem un pakalpojumiem, kurus [...] vienības izmanto pakalpojumu sniegšanai;

b) **politika** attiecībā uz [...] to, kā publiskajā iepirkumā iekļaut un noteikt ar kiberdrošību saistītas prasības IKT produktiem un pakalpojumiem, **tostarp kiberdrošības sertifikāciju**;

c) politika **attiecībā uz neaizsargātības pārvaldību, kas ietver** [...] **brīvprātīgas** koordinētas neaizsargātības atklāšanas **veicināšanu un sekmēšanu** 6. panta **1. punkta** nozīmē;

d) politika saistībā ar atvērtā interneta publiskā kodola vispārējās pieejamības, [...] integritātes **un konfidencialitātes** uzturēšanu;

e) politika kiberdrošības **izglītības un apmācības,** prasmju, izpratnes veidošanas, kā arī pētniecības un izstrādes iniciatīvu veicināšanai un attīstīšanai;

---

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

f) politika par atbalstu akadēmiskās un pētniecības iestādēm kiberdrošības rīku un drošas tīklu infrastruktūras attīstīšanā;

g) politika, attiecīgas procedūras un atbilstīgi informācijas apmaiņas rīki, ar kuriem atbalstīta brīvprātīga kiberdrošības informācijas apmaiņa starp uzņēmumiem, ievērojot Savienības tiesību aktus;

h) politika, kas vērsta uz MVU īpašajām vajadzībām, jo īpaši to MVU vajadzībām, kas nav šīs direktīvas darbības jomā, saistībā ar norādījumiem un atbalstu to noturības pret kiberdraudiem uzlabošanai.

3. Dalībvalstis paziņo savas valsts kiberdrošības stratēģijas Komisijai trīs mēnešu laikā pēc to pieņemšanas. **To darot,** dalībvalstis var nepaziņot **stratēģijas elementus, kas saistīti ar** [...] valsts drošību.

4. Dalībvalstis regulāri un vismaz reizi [...] **piecos** gados novērtē savas valsts kiberdrošības stratēģijas, pamatojoties uz galvenajiem darbības rādītājiem, un nepieciešamības gadījumā tās groza. Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) pēc dalībvalstu lūguma palīdz tām izstrādāt valsts stratēģiju un galvenos darbības rādītājus stratēģijas novērtēšanai.

6. pants

Koordinēta neaizsargātības atklāšana un Eiropas neaizsargātības reģistrs

1. Katra dalībvalsts izraugās vienu no savām *CSIRT*, kā minēts 9. pantā, par koordinatoru koordinētas neaizsargātības atklāšanas vajadzībām. Izraudzītā *CSIRT* rīkojas kā uzticams starpnieks, nepieciešamības gadījumā veicinot mijiedarbību starp ziņotāju vienību**,** **iespējamās neaizsargātības īpašnieku** un IKT produktu ražotāju vai IKT pakalpojumu sniedzēju. **Jebkura fiziska vai juridiska persona var (iespējams, anonīmi) ziņot izraudzītajai *CSIRT* par 4. panta 8. punktā minēto neaizsargātību. Izraudzītā *CSIRT* nodrošina rūpīgu pārbaudi saistībā ar ziņojumu un personas, kura ziņo par neaizsargātību, identitātes konfidencialitāti.** Ja paziņotā neaizsargātība [...] **varētu būtiski ietekmēt vienības vairāk nekā vienā dalībvalstī**, katras attiecīgās dalībvalsts izraudzītā *CSIRT* **attiecīgos gadījumos** sadarbojas ar **citām izraudzītajām *CSIRT***, *CSIRT* tīklā.

2. *ENISA* izstrādā un uztur Eiropas neaizsargātības reģistru**, apspriežoties ar sadarbības grupu**. Šajā nolūkā *ENISA* izveido un uztur atbilstīgas informācijas sistēmas, politikas nostādnes un procedūras, jo īpaši lai svarīgās un būtiskās vienības un to tīklu un informācijas sistēmu piegādātāji varētu atklāt un **brīvprātīgi** reģistrēt **publiski zināmu** neaizsargātību, kas saistīta ar IKT produktiem vai IKT pakalpojumiem, kā arī lai nodrošinātu visām ieinteresētajām personām piekļuvi reģistrā ietvertajai informācijai par neaizsargātību. Reģistrā jo īpaši iekļauj informāciju, kas raksturo neaizsargātību, ietekmēto IKT produktu vai IKT pakalpojumus un neaizsargātības smagumu, proti, apstākļus, kādos to var izmantot, saistītu ielāpu pieejamību un – ja nav pieejamu ielāpu – neaizsargātu produktu lietotājiem adresētus norādījumus**, ko sniegušas valstu kompetentās iestādes vai *CSIRT*,** par to, kā var mazināt no atklātās neaizsargātības izrietošos riskus. ***ENISA* nodrošina, ka Eiropas neaizsargātības reģistrs izmanto drošu un noturīgu sakaru un informācijas infrastruktūru.**

7. pants

Valstu kiberdrošības krīžu pārvaldības satvari

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

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

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

   a) valsts sagatavotības pasākumu un darbību mērķus;

   b) valsts kompetento iestāžu uzdevumus un pienākumus;

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

   d) sagatavotības pasākumus, tostarp regulārus vingrinājumus un apmācības darbības;

   e) attiecīgās iesaistītās publiskās un privātās [...] personas un infrastruktūru;

   f) valsts procedūras un pasākumus starp attiecīgajām valsts iestādēm un struktūrām, lai nodrošinātu dalībvalstu efektīvu dalību un atbalstu koordinētā plašapmēra kiberdrošības incidentu un krīžu pārvaldībā Savienības līmenī.

4. Dalībvalstis [...] **informē** Komisiju **par** savām izraudzītajām 1. punktā minētajām kompetentajām iestādēm un iesniedz **attiecīgo informāciju attiecībā uz šā panta 3. punkta prasībām par** to valsts plāniem reaģēšanai uz kiberdrošības incidentiem un krīzēm [...] trīs mēnešu laikā no izraudzīšanās un minēto plānu pieņemšanas. Dalībvalstis var neiekļaut [...] konkrētu informāciju, ja un ciktāl tas ir stingri nepieciešams [...] valsts drošības**, sabiedrības drošības vai aizsardzības interesēs**.

8. pants

Valsts kompetentās iestādes un vienotie kontaktpunkti

1. Katra dalībvalsts izraugās vienu vai vairākas kompetentās iestādes, kas atbild par kiberdrošību un par uzraudzības uzdevumiem, kas minēti šīs direktīvas VI nodaļā. Šim nolūkam dalībvalstis var izraudzīties esošu iestādi vai iestādes.

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

3. Katra dalībvalsts izraugās vienu valsts kontaktpunktu kiberdrošības jautājumos ("vienotais kontaktpunkts"). Ja dalībvalsts izraugās tikai vienu kompetento iestādi, minētā kompetentā iestāde ir arī attiecīgās dalībvalsts vienotais kontaktpunkts.

4. Katrs vienotais kontaktpunkts koordinē sadarbību, lai nodrošinātu dalībvalstu iestāžu pārrobežu sadarbību ar attiecīgajām iestādēm citās dalībvalstīs, kā arī lai nodrošinātu starpnozaru sadarbību ar citām valsts kompetentajām iestādēm dalībvalstī.

5. Dalībvalstis nodrošina, ka kompetentajām iestādēm, kas minētas 1. punktā, un vienotajiem kontaktpunktiem ir pietiekami resursi, lai efektīvi un lietpratīgi veiktu tiem uzticētos uzdevumus un tādējādi sasniegtu šīs direktīvas mērķus. Dalībvalstis nodrošina izraudzīto pārstāvju efektīvu, lietpratīgu un drošu sadarbību sadarbības grupā, kas minēta 12. pantā.

6. Katra dalībvalsts nekavējoties paziņo Komisijai izraudzīto kompetento iestādi, kas minēta 1. punktā, un vienoto kontaktpunktu, kas minēts 3. punktā, to uzdevumus un visas turpmākās ar tām saistītās izmaiņas. Katra dalībvalsts publisko izraudzītās iestādes un kontaktpunktus. Komisija publicē izraudzīto vienoto kontaktpunktu sarakstu.

9. pants

Datordrošības incidentu reaģēšanas vienības (*CSIRT*)

1. Katra dalībvalsts izraugās vienu vai vairākas *CSIRT*, kuras atbilst 10. panta 1. punktā izklāstītajām prasībām, kuru darbība attiecas vismaz uz I un II pielikumā minētajām nozarēm, apakšnozarēm vai vienībām un kuras ir atbildīgas par incidentu risināšanu saskaņā ar labi definētu procesu. *CSIRT* var izveidot kompetentajā iestādē, kas minēta 8. pantā.

2. Dalībvalstis nodrošina, ka katrai *CSIRT* ir pietiekami resursi, lai tās efektīvi pildītu to uzdevumus, kā izklāstīts 10. panta 2. punktā. **Veicot šos uzdevumus, *CSIRT* var piešķirt prioritāti konkrētu pakalpojumu sniegšanai vienībām, ievērojot uz risku balstītu pieeju.**

3. Dalībvalstis nodrošina, ka katras *CSIRT* rīcībā ir atbilstīga, droša un noturīga sakaru un informācijas infrastruktūra, lai apmainītos ar informāciju ar būtiskajām un svarīgajām vienībām un citām attiecīgajām ieinteresētajām personām. Šajā nolūkā dalībvalstis nodrošina, ka *CSIRT* sniedz ieguldījumu drošu informācijas apmaiņas rīku izmantošanā.

4. *CSIRT* sadarbojas un attiecīgā gadījumā saskaņā ar 26. pantu apmainās ar būtisko informāciju ar būtisko un svarīgo vienību uzticamām nozaru un starpnozaru kopienām.

5. *CSIRT* piedalās [...] **savstarpējās mācīšanās kārtās**, ko organizē saskaņā ar 16. pantu.

6. Dalībvalstis nodrošina savu *CSIRT* efektīvu, lietpratīgu un drošu sadarbību 13. pantā minētajā *CSIRT* tīklā.

7. Dalībvalstis nekavējoties paziņo Komisijai *CSIRT*, kas izraudzītas saskaņā ar 1. punktu, *CSIRT* koordinatoru, kas izraudzīts saskaņā ar 6. panta 1. punktu, un to attiecīgos uzdevumus, kas paredzēti saistībā ar vienībām, kuras minētas I un II pielikumā.

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

10. pants

Prasības* CSIRT *un to uzdevumi

1. *CSIRT* atbilst šādām prasībām:

   a) *CSIRT* nodrošina savu sakaru [...] **kanālu** plašu pieejamību, izvairoties no atsevišķu informācijas ķēdes punktu kļūdainas darbības, un tai ir vairāki saziņas līdzekļi, kas jebkurā laikā ļauj ar to sazināties un nodrošina saziņu ar citiem. *CSIRT* skaidri nosaka saziņas kanālus un dara tos zināmus ieinteresētajām personām un sadarbības partneriem;

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

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

d) *CSIRT* ir pietiekams darbinieku skaits, lai nodrošinātu pieejamību jebkurā brīdī;

e) *CSIRT* ir nodrošinātas ar rezerves sistēmām un dublēšanas darba telpu, lai nodrošinātu pakalpojumu nepārtrauktību;

f) *CSIRT* ir iespēja piedalīties starptautiskos sadarbības tīklos.

2. *CSIRT* uzdevumi ir šādi:

a) kiberdraudu, neaizsargātības un incidentu uzraudzība valsts līmenī;

b) agrīnu brīdinājumu, trauksmju, paziņojumu sniegšana un informācijas izplatīšana būtiskajām un svarīgajām vienībām, kā arī **kompetentajām iestādēm un** citām ieinteresētajām personām par kiberdraudiem, neaizsargātību un incidentiem;

c) reaģēšana uz incidentiem;

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

e) **[...]** tīklu un informācijas sistēmu proaktīvas skenēšanas nodrošināšana [...], **lai noteiktu neaizsargātību, kurai var būt būtiska ietekme, ar nosacījumu, ka ielaušanās tīklā un informācijas sistēmās vai to darbības negatīva ietekmēšana netiek veikta bez attiecīgās vienības piekrišanas**;

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

fa) attiecīgā gadījumā darbošanās koordinatora statusā koordinētas neaizsargātības atklāšanas procesa nolūkā, ievērojot 6. panta 1. punktu, kas jo īpaši ietver mijiedarbības veicināšanu starp ziņotāju vienībām, iespējamās neaizsargātības īpašnieku un IKT produktu ražotāju vai IKT pakalpojumu sniedzēju gadījumos, kad tas ir nepieciešams, attiecīgo vienību apzināšanu un saziņu ar tām, ziņotāju vienību atbalstīšanu, atklāšanas termiņu apspriešanu un vairākas organizācijas ietekmējošas neaizsargātības pārvaldību (vairāku pušu koordinēta neaizsargātības atklāšana).

3. *CSIRT* nodibina sadarbības attiecības ar attiecīgajiem dalībniekiem privātajā sektorā, lai labāk sasniegtu direktīvas mērķus.

3.a *CSIRT* var nodibināt sadarbības attiecības ar trešo valstu *CSIRT*. Šādas sadarbības ietvaros tās var apmainīties ar būtisku informāciju, tostarp personas datiem, saskaņā ar Savienības tiesību aktiem par datu aizsardzību.

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

a) incidentu risināšanas procedūrām;

b) kiberdrošības krīžu pārvaldību;

c) koordinētu neaizsargātības atklāšanu.

11. pants

Sadarbība valsts līmenī

1. Vienas un tās pašas dalībvalsts kompetentās iestādes, kas minētas 8. pantā, vienotais kontaktpunkts un *CSIRT* – ja tās ir atsevišķas struktūras – sadarbojas attiecībā uz šajā direktīvā noteikto pienākumu izpildi.

2. Dalībvalstis nodrošina, ka vai nu to kompetentās iestādes, vai arī to *CSIRT* saņem paziņojumus par incidentiem, nozīmīgiem kiberdraudiem un gandrīz notikušiem notikumiem, kurus iesniedz atbilstoši šai direktīvai. Ja dalībvalsts nolemj, ka tās *CSIRT* nesaņems minētos paziņojumus, *CSIRT* – ciktāl tas ir nepieciešams to uzdevumu izpildei – tiek piešķirta piekļuve datiem par incidentiem, kurus paziņojušas būtiskās vai svarīgās vienības atbilstoši 20. pantam.

3. Katra dalībvalsts nodrošina, ka tās kompetentās iestādes vai *CSIRT* informē tās vienoto kontaktpunktu par paziņojumiem, kas attiecas uz incidentiem, nozīmīgiem kiberdraudiem un gandrīz notikušiem notikumiem un kas sniegti atbilstoši šai direktīvai.

4. Ciktāl nepieciešams šajā direktīvā noteikto uzdevumu un pienākumu izpildei, dalībvalstis nodrošina atbilstīgu sadarbību starp kompetentajām iestādēm, ***CSIRT*****,** vienotajiem kontaktpunktiem un tiesībaizsardzības iestādēm, datu aizsardzības iestādēm un **kompetentajām** iestādēm, kas **izraudzītas** [...], ievērojot Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva[...]], **kompetentajām iestādēm saskaņā ar Komisijas Īstenošanas regulu 2019/1583, valsts regulatīvajām iestādēm saskaņā ar Direktīvu (ES) 2018/1972, valsts iestādēm, kas izraudzītas, ievērojot Regulas (ES) Nr. 910/2014 17. pantu,** [...] valsts finanšu iestādēm, kas izraudzītas saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) XXXX/XXXX [*DORA* regula], **kā arī kompetentajām iestādēm, kas izraudzītas saskaņā ar citiem nozarspecifiskiem Savienības tiesību aktiem,** minētajā dalībvalstī.

5. Dalībvalstis nodrošina, ka to kompetentās iestādes **saskaņā ar šo direktīvu un kompetentās iestādes, kas izraudzītas, ievērojot Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva]**, regulāri [...] **apmainās** ar informāciju [...] par **kritisko vienību apzināšanu,** kiberdrošības riskiem, kiberdraudiem **un incidentiem, kā arī riskiem, draudiem un incidentiem, kas nav saistīti ar kiberdrošību un** kas ietekmē būtiskās vienības, kuras identificētas kā kritiskas **[**vai kā vienības, kas ir līdzvērtīgas kritiskām vienībām**]**, ievērojot Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], kā arī par veiktajiem pasākumiem, [...] reaģējot uz šādiem riskiem un incidentiem. **Dalībvalstis arī nodrošina, ka kompetentās iestādes saskaņā ar šo direktīvu [...] un kompetentās iestādes, kas izraudzītas, ievērojot Regulu (ES) XXXX/XXXX [*DORA* regula], Direktīvu 2018/1972 un Regulu (ES) 910/2014, regulāri apmainās ar attiecīgo informāciju.**

Attiecībā uz uzticamības pakalpojumu sniedzējiem un [...] jo īpaši [...] gadījumos, kad uzraudzības pienākumi saskaņā ar šo direktīvu ir uzticēti citai iestādei, nevis uzraudzības struktūrām, kas izraudzītas saskaņā ar Regulu (ES) Nr. 910/2014, valstu kompetentās iestādes saskaņā ar šo direktīvu cieši un jau laikus sadarbojas, apmainoties ar attiecīgo informāciju, lai nodrošinātu efektīvu uzraudzību un uzticamības pakalpojumu sniedzēju atbilstību šajā direktīvā un Regulā [XXXX/XXXX] noteiktajām prasībām, **un attiecīgajā gadījumā valsts kompetentā iestāde saskaņā ar šo direktīvu bez nepamatotas kavēšanās paziņo *eIDAS* uzraudzības iestādei par jebkādu paziņotu nozīmīgu kiberdraudu vai incidentu, kas ietekmē uzticamības pakalpojumus.**

5.a Lai [...] vienkāršotu ziņošanu par incidentiem, dalībvalstis var izveidot vienotu kontaktpunktu visiem paziņojumiem, kas prasīti saskaņā ar šo direktīvu, kā arī attiecīgā gadījumā saskaņā ar Regulu (ES) 2016/679 un Direktīvu 2002/58/EK. Dalībvalstis var izmantot vienoto kontaktpunktu paziņojumiem, kas prasīti saskaņā ar citiem nozarspecifiskiem Savienības tiesību aktiem. Šis vienotais kontaktpunkts neietekmē Regulas (ES) 2016/679 un Direktīvas 2002/58/EK noteikumu piemērošanu, jo īpaši to noteikumu piemērošanu, kas attiecas uz neatkarīgām uzraudzības iestādēm.

III NODAĻA

***ES** sadarbība*

12. 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 6. punktā.

3. Sadarbības grupas sastāvā ir pārstāvji no dalībvalstīm, Komisijas un *ENISA*. Sadarbības grupas darbībās kā novērotājs piedalās Eiropas Ārējās darbības dienests. Sadarbības grupas darbībās **saskaņā ar Regulas (ES) XXXX/XXXX [*DORA* regulas] 42. panta 1. punktu** var piedalīties Eiropas uzraudzības iestādes (EUI) **un kompetentās iestādes, kas izraudzītas** saskaņā ar Regulu (ES) XXXX/XXXX [*DORA* regulu].

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

   Komisija nodrošina sekretariātu.

4. Sadarbības grupai ir šādi uzdevumi:

   a) dot norādījumus kompetentajām iestādēm par šīs direktīvas transponēšanu un īstenošanu**;**

   aa) dot norādījumus saistībā ar politikas izstrādi un īstenošanu attiecībā uz koordinētu neaizsargātības atklāšanu, kā minēts 5. panta 2. punkta c) apakšpunktā un 6. panta 1. punktā;

b) apmainīties ar paraugpraksi un informāciju saistībā ar šīs direktīvas īstenošanu, arī par kiberdraudiem, incidentiem, neaizsargātību, gandrīz notikušiem notikumiem, izpratnes veicināšanas iniciatīvām, apmācību, vingrinājumiem un prasmēm, spēju veidošanu, kā arī standartiem un tehniskajām specifikācijām;

c) apmainīties ar padomiem un sadarboties ar Komisiju jaunu kiberdrošības politikas iniciatīvu jomā;

d) apmainīties ar padomiem un sadarboties ar Komisiju saistībā ar Komisijas īstenošanas [...] aktu projektiem, ko pieņem atbilstoši šai direktīvai;

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

ea) apmainīties viedokļiem par tādu nozaru tiesību aktu īstenošanu, kuros ir kiberdrošības aspekti;

f) apspriest ziņojumus par [...] **savstarpējo mācīšanos**, kas minēta 16. panta 7. punktā;

g) apspriest **pieredzi, kas gūta** kopējās uzraudzības darbībās [...] pārrobežu lietās, kā minēts 34. pantā;

h) dot stratēģiskus norādījumus *CSIRT* tīklam **un *EU-CyCLONe*** par īpašām jaunām problēmām;

ha) apmainīties viedokļiem par turpmākiem politikas pasākumiem pēc plašapmēra kiberdrošības incidentiem, pamatojoties uz *CSIRT* tīkla un *EU–CyCLONe* pieredzē gūtajām atziņām;

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

j) organizēt regulāras kopīgas sanāksmes ar attiecīgajām privātā sektora ieinteresētajām personām visā Savienībā, lai apspriestu grupas veiktās darbības un apkopotu informāciju par jaunām politikas problēmām;

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

ka) izveidot savstarpējas mācīšanās mehānismu saskaņā ar šīs direktīvas 16. pantu.

5. Sadarbības grupa no *CSIRT* tīkla var pieprasīt tehnisku ziņojumu par atlasītiem tematiem.

6. Līdz … [24 mēneši pēc šīs direktīvas spēkā stāšanās dienas] un pēc tam reizi divos gados sadarbības grupa izstrādā darba programmu par darbībām, kas veicamas, lai īstenotu tās mērķus un uzdevumus. Saskaņā ar šo direktīvu pieņemtās pirmās programmas termiņu pielāgo saskaņā ar Direktīvu (ES) 2016/1148 pieņemtās pēdējās programmas termiņam.

7. Komisija var pieņemt īstenošanas aktus, ar kuriem nosaka procesuālo kārtību, kas nepieciešama sadarbības grupas darbībai. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 37. panta 2. punktā.

8. Sadarbības grupa regulāri un vismaz reizi gadā tiekas ar Kritisko vienību noturības grupu, kas izveidota ar Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], lai veicinātu stratēģisko sadarbību un **atvieglotu** informācijas apmaiņu.

13. pants

CSIRT *tīkls*

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

2. *CSIRT* tīkls sastāv no dalībvalstu *CSIRT***, kuras izraudzītas saskaņā ar 9. pantu,** un *CERT-EU* pārstāvjiem. Komisija piedalās *CSIRT* tīklā novērotāja statusā. *ENISA* nodrošina sekretariātu un aktīvi atbalsta sadarbību starp *CSIRT*.

3. *CSIRT* tīklam ir šādi uzdevumi:

   a) apmainīties ar informāciju par *CSIRT* spējām;

   b) apmainīties ar būtisku informāciju par incidentiem, gandrīz notikušiem notikumiem, kiberdraudiem, riskiem un neaizsargātību;

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

bb) dalīties tehniskajos risinājumos, kas atvieglo incidentu tehnisko risināšanu;

bc) apmainīties ar paraugpraksi, rīkiem un procesiem saistībā ar *CSIRT* uzdevumiem;

c) ja to lūdz kāda *CSIRT* tīkla [...] **locekle**, kuru varētu būt ietekmējis incidents, — apmainīties ar informāciju un apspriest informāciju par attiecīgo incidentu un saistītajiem kiberdraudiem, riskiem un neaizsargātību;

d) pēc *CSIRT* tīkla [...] **locekles** lūguma apspriest un, ja iespējams, īstenot saskaņotu reaģēšanu uz incidentu, kas ir identificēts attiecīgās dalībvalsts jurisdikcijā;

e) sniegt dalībvalstīm atbalstu pārrobežu incidentu risināšanā atbilstoši šai direktīvai;

f) sadarboties ar izraudzītajām *CSIRT*, kas minētas 6. pantā, **apmainīties ar tām ar paraugpraksi** un sniegt tām palīdzību attiecībā uz tādas [...] koordinētas neaizsargātības atklāšanas pārvaldību, kura ietekmē vairākus IKT produktu ražotājus vai IKT pakalpojumu sniedzējus un IKT procesu nodrošinātājus, kas iedibināti dažādās dalībvalstīs;

g) apspriest un apzināt operatīvās sadarbības turpmākos veidus, arī attiecībā uz:

i) kiberdraudu un incidentu kategorijām;

ii) agrīniem brīdinājumiem;

iii) savstarpēju palīdzību;

iv) koordinēšanas principiem un kārtību, reaģējot uz pārrobežu riskiem un incidentiem;

v) ieguldījumu valsts plānā reaģēšanai uz kiberdrošības incidentiem un krīzēm, kas minēts 7. panta 3. punktā, **pēc kādas dalībvalsts lūguma**;

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

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

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

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

l) apspriest [...] **savstarpējas mācīšanās** ziņojumus, kas minēti 16. panta 7. punktā;

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

4. Šīs direktīvas 35. pantā minētās pārskatīšanas nolūkā *CSIRT* tīkls līdz [24 mēneši pēc šīs direktīvas spēkā stāšanās dienas] un pēc tam reizi divos gados novērtē gūto progresu operatīvajā sadarbībā un sagatavo ziņojumu. Ziņojumā izdara secinājumus par rezultātiem, kas gūti 16. pantā minētajā [...] **savstarpējās mācīšanās procesā**, kura veikta saistībā ar valstu *CSIRT*, tostarp secinājumus un ieteikumus, kas jāīsteno atbilstoši šim pantam. Minēto ziņojumu iesniedz arī sadarbības grupai.

5. *CSIRT* tīkls sev pieņem reglamentu.

6. *CSIRT* tīkls sadarbojas ar *EU-CyCLONe*, pamatojoties uz saskaņotu procesuālo kārtību.

14. pants

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

1. Lai atbalstītu koordinētu plašapmēra kiberdrošības incidentu un krīžu pārvaldību operatīvā līmenī un nodrošinātu regulāru informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām un aģentūrām, ar šo tiek izveidots Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*).

2. *EU-CyCLONe* sastāvā ir pārstāvji no dalībvalstu **kiber**krīžu pārvaldības iestādēm, kas izraudzītas saskaņā ar 7. pantu [...]. **Komisija tīkla darbībās piedalās novērotāja statusā.** *ENISA* tīklam nodrošina sekretariātu un atbalsta drošu informācijas apmaiņu, **kā arī dod rīkus, kas vajadzīgi, lai, nodrošinot drošu informācijas apmaiņu, atbalstītu dalībvalstu sadarbību.**

Attiecīgā gadījumā *EU-CyCLONe* var aicināt savā darbā piedalīties attiecīgo ieinteresēto personu pārstāvjus.

3. *EU-CyCLONe* uzdevumi ir šādi:

a) paaugstināt sagatavotības līmeni plašapmēra **kiberdrošības** incidentu un krīžu pārvaldībai;

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

ba) izvērtēt attiecīgo plašapmēra kiberdrošības incidentu sekas un ietekmi un ierosināt iespējamos riska mazināšanas pasākumus;

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

d) **pēc kādas dalībvalsts lūguma** apspriest **tās** valsts plānus reaģēšanai uz kiberdrošības incidentu un **krīzi**, kuri minēti [...] 7. panta **3. punktā**; [...]

4. *EU-CyCLONe* sev pieņem reglamentu.

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

6. *EU-CyCLONe* sadarbojas ar *CSIRT* tīklu, pamatojoties uz saskaņotu procesuālo kārtību.

7. *EU-CyCLONe* līdz [24 mēneši pēc šīs direktīvas spēkā stāšanās dienas] iesniedz Eiropas Parlamentam un Padomei ziņojumu, kurā izvērtēts tā darbs.

14.a pants

Starptautiskā sadarbība

Attiecīgā gadījumā Savienība saskaņā ar LESD 218. pantu var noslēgt starptautiskus nolīgumus ar trešām valstīm vai starptautiskām organizācijām, ļaujot tām saskaņā ar Savienības tiesību aktiem par datu aizsardzību piedalīties dažās sadarbības grupas, *CSIRT* tīkla un *EU-CyCLONe* darbībās un organizējot šo dalību.

15. pants

Ziņojums par situāciju kiberdrošības jomā Savienībā

1. *ENISA*, sadarbojoties ar Komisiju **un sadarbības grupu**, izdod divgadu ziņojumu par situāciju kiberdrošības jomā Savienībā. Ziņojumā [...] **jo īpaši** [...] iekļauj:

   aa) Savienības līmeņa kiberdrošības riska novērtējumu, kurā ir ņemta vērā apdraudējuma aina;

   a) [...] kiberdrošības spēju attīstības **novērtējumu** publiskajā un privātajā sektorā visā Savienībā;

   b) [...]

   c) **saskaņotu novērtējumu [...], kura pamatā** ir **kvantitatīvi un kvalitatīvi** kiberdrošības rādītāji, kas nodrošina **pārskatu** par kiberdrošības spēju brieduma līmeni, **tostarp par nozarspecifiskām spējām**.

2. Ziņojumā iekļauj īpašus politiskus ieteikumus kiberdrošības līmeņa paaugstināšanai Savienībā un konstatējumu kopsavilkumu par attiecīgo periodu no aģentūras ES kiberdrošības tehniskās situācijas ziņojumiem, ko izdevusi *ENISA* saskaņā ar Regulas (ES) 2019/881 7. panta 6. punktu.

16. pants

Savstarpēja mācīšanās

1. **Lai nostiprinātu savstarpēju uzticēšanos, panāktu augstu kopējo kiberdrošības līmeni, kā arī lai stiprinātu dalībvalstu kiberdrošības spējas un politiku, kas ir vajadzīgas efektīvai šīs direktīvas īstenošanai, sadarbības grupa, ar Komisijas atbalstu** un apspriedusies ar *ENISA*, **un attiecīgā gadījumā ar *CSIRT* tīklu**, vēlākais, **24 [...]** mēnešus pēc šīs direktīvas stāšanās spēkā izveido [...] **objektīvas, nediskriminējošas un taisnīgas savstarpējās mācīšanās sistēmas metodiku attiecībā uz to**, kā dalībvalstis **īsteno šo direktīvu**. **Dalība savstarpējas mācīšanās procesā ir brīvprātīga. Sistēma sastāv no novērtēšanas kārtām**, [...] ko veic kiberdrošības eksperti no dalībvalstīm [...], un tajā aplūko **vienu vai vairākus** šādus aspektus:

   i) 18. un 20. pantā minēto kiberdrošības riska pārvaldības prasību un ziņošanas pienākumu īstenošanu [...];

   ii) spējas [...], ieskaitot pieejamos [...] resursus [...], un **8. pantā minēto** valsts kompetento iestāžu **un 9. pantā minēto *CSIRT*** uzdevumu izpildi [...];

[...]

i**ii**[...]) 34. pantā minētās savstarpējās palīdzības **īstenošanu** [...];

iv) šīs direktīvas 26. pantā minētā informācijas apmaiņas satvara **īstenošanu** [...].

2. **Kritēriji, pēc kuriem dalībvalstīm ir jāizraugās eksperti, kas ir tiesīgi piedalīties savstarpējas mācīšanās kārtās, ir** [...] objektīvi, nediskriminējoši, taisnīgi un pārredzami [...], **un tie ir iekļauti 1. punktā minētajā metodikā**. *ENISA* un Komisija [...] **var** izraudzīties ekspertus, kuri novērotāja statusā piedalās [...] **savstarpējas mācīšanās kārtās**. [...]

3. [...] .

3.a Pirms savstarpējas mācīšanās kārtu sākšanas dalībvalstis var veikt to aspektu pašnovērtējumu, uz kuriem attiecas konkrētā savstarpējas mācīšanās kārta, un šo pašnovērtējumu iesniegt 2. punktā minētajiem izraudzītajiem ekspertiem.

4. **Savstarpējā mācīšanās** [...] **var** būt [...] **fiziski** vai virtuāli apmeklējumi uz vietas un apmaiņa no tālienes. Ievērojot labas sadarbības principu, dalībvalstis [...], **kas piedalās savstarpējas mācīšanās procesā**, izraudzītajiem ekspertiem [...] sniedz novērtēšanai nepieciešamo informāciju**, neskarot valsts vai Savienības tiesību aktus par konfidenciālas vai klasificētas informācijas aizsardzību vai tādu būtisku valsts funkciju saglabāšanu kā valsts drošība.** Visu [...] **savstarpējas mācīšanās** procesā iegūto informāciju izmanto tikai šim mērķim. Eksperti, kuri piedalās **savstarpējas mācīšanās procesā**[...], neizpauž trešām personām nekādu sensitīvu vai konfidenciālu informāciju, kas iegūta [...] **minētajā kontekstā**. **Dalībvalsts, kas piedalās savstarpējas mācīšanās procesā, var iebilst pret konkrētu ekspertu izraudzīšanos, balstoties uz pienācīgi pamatotiem iemesliem, kas paziņoti sadarbības grupai.**

5. Tie aspekti, kas jau reiz ir [...] **izskatīti kādā savstarpējas mācīšanās kārtā**, attiecībā uz iesaistītajām [...] dalībvalstīm vairs netiek izskatīti turpmākās [...] **savstarpējas mācīšanās kārtās četrus** gadus pēc **minētās savstarpējas mācīšanās kārtas** beigām, **ja vien attiecīgā dalībvalsts to nelūdz vai nepiekrīt sadarbības grupas priekšlikumam** to darīt.

6. [...]

7. Eksperti, kuri piedalās [...] **savstarpējas mācīšanās kārtās**, sagatavo ziņojumus par **novērtēšanā** konstatēto un secināto. **Dalībvalstīm par attiecīgi saviem ziņojumu projektiem ir atļauts iesniegt komentārus, ko pievieno ziņojumam. Galīgos** ziņojumus iesniedz [...] sadarbības grupai [...]; **dalībvalstis var pieņemt lēmumu par attiecīgi savu ziņojumu publiskošanu.**

IV NODAĻA

Kiberdrošības riska pārvaldības un ziņošanas pienākumi

I IEDAĻA

Kiberdrošības riska pārvaldība un ziņošana

17. pants

Pārvalde

1. Dalībvalstis nodrošina, ka būtisku un svarīgu vienību pārvaldes struktūras apstiprina kiberdrošības riska pārvaldības pasākumus, ko minētās vienības veikušas, lai izpildītu 18. panta prasības, [...] **pārrauga** tā īstenošanu, un [...] **no tām var prasīt atbildību** par to, ka vienības nav izpildījušas šajā pantā noteiktos pienākumus.

   Šā punkta piemērošana neskar dalībvalsts tiesību aktus par atbildības noteikumiem valsts iestādēs, kā arī par valsts ierēdņu un ievēlētu un ieceltu amatpersonu atbildību.

2. Dalībvalstis nodrošina, ka [...] **no pārvaldības struktūras locekļiem tiek prasīts** regulāri piedalīties mācībās, kurās iegūst pietiekamas zināšanas un prasmes, lai izprastu un novērtētu kiberdrošības riskus un pārvaldības praksi, kā arī to ietekmi uz vienības darbībām.

18. pants

Kiberdrošības riska pārvaldības pasākumi

1.**a** **Šajā direktīvā piemēro "visu apdraudējumu" pieeju, kurā ir ietverta tīklu un informācijas sistēmu un to fiziskās vides aizsardzība pret visiem notikumiem, kas varētu apdraudēt uzglabāto, nosūtīto vai apstrādāto datu vai tīklu un informācijas sistēmu piedāvāto vai ar to starpniecību pieejamo pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti.**

1. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības veic atbilstīgus un samērīgus tehniskos un organizatoriskos pasākumus, lai pārvaldītu riskus [...] to tīklu un informācijas sistēmu drošībai, ko tās izmanto savu pakalpojumu sniegšanā. Ņemot vērā jaunākos tehniskos sasniegumus **un īstenošanas izmaksas**, ar minētajiem pasākumiem nodrošina radītajam riskam atbilstošu tīklu drošības un informācijas sistēmu līmeni. **Novērtējot minēto pasākumu samērīgumu, pienācīgi ņem vērā to, cik lielā mērā vienība ir pakļauta riskiem, cik tā ir liela un cik liela ir iespēja, ka radīsies incidenti, un cik smagi incidenti. Ņemot vērā to, cik liels un kāds risks tiek radīts sabiedrībai tādu incidentu gadījumā, kas skar būtiskas vai svarīgas vienības, kiberdrošības riska pārvaldības pasākumi, ko piemēro svarīgām vienībām, var būt ne tik stingri kā tie, ko piemēro būtiskām vienībām.**

2. Pasākumos, kas minēti 1. punktā, ietver vismaz:

a) riska analīzes un informācijas sistēmu drošības politiku;

b) incidentu risināšanu (incidentu novēršana, atklāšana, [...] reaģēšana uz tiem **un atgūšanās no**[...] incidentiem);

c) darbības nepārtrauktības 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, piemēram, datu uzglabāšanas un apstrādes pakalpojumu vai pārvaldītu drošības pakalpojumu sniedzējiem;

e) drošību tīklu un informācijas sistēmu ieguvē, attīstīšanā un uzturēšanā, tostarp rīcību neaizsargātības gadījumā un atklāšanā;

f) politikas nostādnes un procedūras [...], ar ko novērtē kiberdrošības riska pārvaldības pasākumu efektivitāti;

g) **politiku attiecībā uz** kriptogrāfijas un šifrēšanas izmantošanu;

ga) cilvēkresursu drošību, piekļuves kontroles politiku un aktīvu pārvaldību.

3. Dalībvalstis nodrošina, ka, apsverot atbilstīgus pasākumus, kas minēti 2. punkta d) apakšpunktā, vienībām **ir jāņem** vērā [...] neaizsargātība, kas raksturīga katram **tiešajam** piegādātājam un pakalpojumu sniedzējam, un vispārējo savu piegādātāju un pakalpojumu sniedzēju produktu kvalitāti un to kiberdrošības praksi, ieskaitot to drošās attīstības procedūras. **Dalībvalstis nodrošina arī to, lai, apsverot 2. punkta d) apakšpunktā minētos piemērotos pasākumus, no vienībām tiktu prasīts ņemt vērā saskaņā ar 19. panta 1. punktu veikto koordinēto riska novērtējumu rezultātus.**

4. Dalībvalstis nodrošina, ka tad, ja vienība konstatē, ka attiecīgi tās pakalpojumi vai uzdevumi neatbilst 2. punktā noteiktajām prasībām, tā nekavējoties veic visus nepieciešamos korektīvos pasākumus, lai nodrošinātu attiecīgā pakalpojuma atbilstību.

5. Komisija var pieņemt īstenošanas aktus, lai **šā panta** 2. punktā minētajiem elementiem noteiktu tehniskās un metodiskās specifikācijas, **kā arī vajadzības gadījumā – nozaru specifiku**. **Komisija līdz [18 mēneši pēc šīs direktīvas stāšanās spēkā] pieņem īstenošanas aktus, lai 24. panta 1. punktā minētajām vienībām un uzticamības pakalpojumu sniedzējiem, kas minēti I pielikuma 8. punktā, noteiktu tehniskās un metodiskās specifikācijas. Minētos īstenošanas aktus pieņem saskaņā ar 37. panta 2. punktā minēto pārbaudes procedūru.** Gatavojot [...] **šādus īstenošanas** aktus, Komisija[...], ciktāl iespējams, **ievēro** starptautiskos un Eiropas standartus, kā arī attiecīgās tehniskās specifikācijas **un ar sadarbības grupu un *ENISA* apmainās ar padomiem par īstenošanas akta projektu saskaņā ar12. panta 4. punkta d) apakšpunktu**.

6. [...]

19. pants

ES koordinētie kritisko piegādes ķēžu riska novērtējumi

1. Sadarbības grupa kopā ar Komisiju un *ENISA* attiecībā uz īpašiem kritiskiem IKT pakalpojumiem, sistēmām vai produktu piegādes ķēdēm var veikt koordinētus drošības riska novērtējumus, ņemot vērā tehniskus un attiecīgā gadījumā netehniskus riska faktorus.

2. Komisija pēc apspriešanās ar sadarbības grupu un *ENISA* identificē īpašos kritiskos IKT pakalpojumus, sistēmas vai produktus, par kuriem var veikt 1. punktā minēto koordinēto riska novērtējumu.

20. pants

Ziņošanas pienākumi

1. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās paziņo kompetentajām iestādēm vai *CSIRT* saskaņā ar 3. un 4. punktu par ikvienu incidentu, kam ir būtiska ietekme uz to pakalpojumu sniegšanu. Attiecīgā gadījumā minētās vienības bez nepamatotas kavēšanās informē savus pakalpojumu saņēmējus par **šiem** incidentiem, kas varētu nelabvēlīgi ietekmēt konkrētā pakalpojuma sniegšanu. Dalībvalstis nodrošina, ka minētās vienības cita starpā paziņo visu informāciju, kas ļauj kompetentajām iestādēm vai CSIRT noteikt incidenta pārrobežu ietekmi. **Pati paziņošanas darbība ziņotājai vienībai nerada lielāku atbildību.**

2. [...]

   Attiecīgā gadījumā [...] **būtiskās un svarīgās** vienības bez nepamatotas kavēšanās savus pakalpojumu saņēmējus, kurus varētu skart ievērojami kiberdraudi, informē par visiem pasākumiem vai tiesiskās aizsardzības līdzekļiem, ko minētie saņēmēji var veikt, reaģējot uz konkrētajiem draudiem. Attiecīgā gadījumā vienības arī informē minētos saņēmējus par pašiem draudiem. **Pati** paziņošanas **darbība** ziņotājai vienībai nerada lielāku atbildību.

3. Incidentu uzskata par nozīmīgu, ja:

a) incidents ir izraisījis vai var izraisīt **smagu** [...] **pakalpojuma** darbības traucējumu vai finansiālus zaudējumus attiecīgajai vienībai;

b) incidents ir ietekmējis vai var ietekmēt citas fiziskas vai juridiskas personas, izraisot ievērojamus materiālus vai nemateriālus zaudējumus.

4. Dalībvalstis nodrošina, lai 1. punktā noteiktās paziņošanas nolūkos attiecīgās vienības kompetentajām iestādēm vai *CSIRT* iesniegtu :

a) bez nepamatotas kavēšanās un katrā ziņā 24 stundu laikā no brīža, kad uzzinājušas par incidentu, — sākotnēju paziņojumu **agrīna brīdinājuma veidā**, kurā attiecīgā gadījumā norāda, vai incidentu ir izraisījusi, domājams, nelikumīga vai ļaunprātīga rīcība;

b) pēc kompetentās iestādes vai *CSIRT* pieprasījuma — starpposma ziņojumu par attiecīgajiem statusa atjauninājumiem;

c) **galīgu** ziņojumu ne vēlāk kā mēnesi pēc a) apakšpunktā minētā **sākotnējā paziņojuma** iesniegšanas, tajā iekļaujot vismaz:

i) sīku incidenta, tā smaguma un ietekmes aprakstu;

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

iii) piemērotos un notiekošos riska mazināšanas pasākumus.

Dalībvalstis nodrošina, ka pienācīgi pamatotos gadījumos un pēc vienošanās ar kompetentajām iestādēm vai *CSIRT* attiecīgā vienība var atkāpties no a) un c) apakšpunktā noteiktajiem termiņiem. **Atkāpi no c) apakšpunktā minētā termiņa var jo īpaši pamatot gadījumos, kad incidents joprojām turpinās.**

5. Valsts kompetentās iestādes vai *CSIRT* [...] **bez nepamatotas kavēšanās** 24 stundu laikā no 4. punkta a) apakšpunktā minētā sākotnējā paziņojuma saņemšanas sniedz ziņotājai vienībai atbildi, kurā iekļauj sākotnējo atgriezenisko saiti par incidentu un — pēc vienības pieprasījuma — norādījumus par iespējamo riska mazināšanas pasākumu īstenošanu. Ja *CSIRT* nesaņem 1. un 2. punktā minēto paziņojumu, minētos norādījumus sniedz kompetentā iestāde, sadarbojoties ar *CSIRT*. Ja attiecīgā vienība lūdz papildu tehnisko atbalstu, *CSIRT* to sniedz. Ja ir aizdomas, ka incidents ir noziedzīgs, valsts kompetentās iestādes vai CSIRT arī dod norādījumus par incidenta paziņošanu tiesībaizsardzības iestādēm.

6. Attiecīgā gadījumā, īpaši tad, ja 1. punktā minētais incidents skar divas vai vairākas dalībvalstis, kompetentā iestāde *CSIRT* vai **vienotais kontaktpunkts** informē citas skartās dalībvalstis un *ENISA* par incidentu. **Šādā informācijā iekļauj vismaz šā panta 4. punktā paredzētos elementus.** To darot, kompetentās iestādes, *CSIRT* un vienotie kontaktpunkti saskaņā ar Savienības tiesību aktiem vai valsts tiesību aktiem, kas atbilst Savienības tiesību aktiem, nodrošina vienības drošību un komerciālās intereses, kā arī sniegtās informācijas konfidencialitāti.

7. Ja ir nepieciešams informēt sabiedrību, lai novērstu incidentu vai risinātu notiekošu incidentu, vai incidenta atklāšana citādi ir sabiedrības interesēs, kompetentā iestāde vai CSIRT un attiecīgā gadījumā citu iesaistīto dalībvalstu kompetentās iestādes vai CSIRT pēc apspriešanās ar attiecīgo vienību informē sabiedrību par incidentu vai pieprasa, lai to dara vienība.

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

9. Vienotais kontaktpunkts [...] **reizi sešos mēnešos** iesniedz *ENISA* kopsavilkuma ziņojumu, kurā iekļauj anonimizētus un apkopotus datus par incidentiem, nozīmīgiem kiberdraudiem un gandrīz notikušiem notikumiem, par kuriem paziņots saskaņā ar [...] 1. punktu un 27. pantu. Lai veicinātu salīdzināmas informācijas sniegšanu, *ENISA* var izdot tehniskus norādījumus par kopsavilkuma ziņojumā iekļautās informācijas parametriem. ***ENISA* reizi sešos mēnešos informē sadarbības grupu un *CSIRT* tīklu par saviem konstatējumiem saistībā ar saņemtajiem paziņojumiem.**

10. Kompetentās iestādes kompetentajām iestādēm, kuras izraudzītas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], sniedz informāciju par incidentiem un kiberdraudiem, ko saskaņā ar 1. un 2. punktu paziņojušas būtiskās vienības, kas identificētas kā kritiskas vienības, **[**vai vienības, kas ir līdzvērtīgas kritiskajām vienībām,**]** atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva].

11. Komisija var pieņemt īstenošanas aktus, kuros sīkāk nosaka atbilstoši 1. un 2. punktam iesniegtajā ziņojumā iekļaujamās informācijas veidu, ziņojuma formātu un paziņošanas procedūru. Komisija var pieņemt īstenošanas aktus, lai precizētu, kuros gadījumos incidentu uzskata par nozīmīgu, kā minēts 3. punktā. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 37. panta 2. punktā.

21. pants

Eiropas kiberdrošības sertifikācijas shēmu izmantošana

1. Lai pierādītu atbilstību konkrētām 18. panta prasībām, dalībvalstis var **no vienībām prasīt, lai tās izmantotu konkrētus IKT produktus, [...] pakalpojumus un [...] procesus, kuri ir sertificēti** atbilstoši īpašām Eiropas kiberdrošības sertifikācijas shēmām, kas pieņemtas saskaņā ar Regulas (ES) 2019/881 49. pantu. **IKT** produktus, pakalpojumus un procesus, uz kuriem attiecas sertifikācija, var izstrādāt būtiska vai svarīga vienība, vai tos var iepirkt no trešām personām.

2. Komisija var [...] pieņemt **īstenošanas** aktus, ar ko nosaka, kurām būtisko **vai svarīgo** vienību kategorijām ir **jāizmanto konkrēti sertificēti IKT produkti, pakalpojumi un procesi vai** jāsaņem sertifikāts, [...] saskaņā ar ko ir **pieņemtas** [...] Eiropas kiberdrošības sertifikācijas shēmas, **ievērojot Regulas (ES) 2019/881 49. pantu**.[...] **Minētos īstenošanas aktus pieņem saskaņā ar 37. panta 2. punktā minēto pārbaudes procedūru. Gatavojot šādus īstenošanas aktus, Komisija saskaņā ar Regulas (ES) 2019/881 56. pantu:**

   i) ņem vērā to, kā minētie pasākumi savu izmaksu ziņā ietekmē šādu IKT produktu, pakalpojumu vai procesu ražotājus, sniedzējus vai nodrošinātājus un to lietotājus, un to, kādus sociālus vai ekonomiskus ieguvumus iecerētais augstākais drošības līmenis rada konkrētajiem IKT produktiem, pakalpojumiem vai procesiem, kā arī to alternatīvu pieejamībai tirgū;

   ii) veic atklātu, pārredzamu un iekļaujošu apspriešanos ar visām attiecīgajām ieinteresētajām personām un dalībvalstīm;

(i) ņem vērā jebkādus īstenošanas termiņus, pārejas pasākumus un laikposmus, jo īpaši attiecībā uz to, kā pasākumi var ietekmēt IKT produktu, pakalpojumu un procesu ražotājus, sniedzējus vai nodrošinātājus, vai lietotājus, tostarp MVU;

(ii) ņem vērā attiecīgo dalībvalstu tiesību aktu spēkā esamību un īstenošanu.

3. Gadījumos, kad **šā panta** 2. punkta nolūkos nav pieejama neviena piemērota Eiropas kiberdrošības sertifikācijas shēma, Komisija var prasīt, lai *ENISA*, ievērojot Regulas (ES) 2019/881 48. panta 2. punktu, sagatavotu kandidātshēmu **vai pārskatītu kādu pastāvošu Eiropas kiberdrošības sertifikācijas shēmu**.

22. pants

Standartizācija

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

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

23. pants

Domēnu nosaukumu un reģistrācijas datu datubāzes

1. Lai veicinātu DNS drošību, stabilitāti un noturību, dalībvalstis nodrošina, ka ALD **nosaukumu** reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, ar pienācīgu rūpību savāc un uztur precīzus **[...]** un pilnīgus domēnu nosaukumu reģistrācijas datus speciālā datubāzē **saskaņā ar** [...] Savienības datu aizsardzības tiesību aktiem par datiem, kas ir persondati.

2. Dalībvalstis nodrošina, ka 1. punktā minētajās domēnu nosaukumu reģistrācijas datu datubāzēs ir ietverta attiecīga informācija, kas ļauj identificēt domēnu nosaukumu turētājus un kontaktpunktus, kuri pārvalda ALD nosaukumus, un sazināties ar tiem**, tostarp vismaz šādi dati:**

   a) domēna nosaukums,

   b) reģistrācijas datums,

   c) reģistrētāja dati, to skaitā

      i) attiecībā uz fiziskām personām – vārds, uzvārds un e-pasta adrese,

      ii) attiecībā uz juridiskām personām – nosaukums un e-pasta adrese.

3. Dalībvalstis nodrošina, ka ALD **nosaukumu** reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, ir ieviesuši politiku un procedūras, lai nodrošinātu, ka datubāzēs ir iekļauta precīza un pilnīga informācija. Dalībvalstis nodrošina, ka šāda politika un procedūras tiek publiskotas.

4. Dalībvalstis nodrošina, ka ALD **nosaukumu** reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, bez nepamatotas kavēšanās pēc domēna nosaukuma reģistrācijas publicē domēnu reģistrācijas datus, kas nav persondati.

5. Dalībvalstis nodrošina, ka ALD **nosaukumu** reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, sniedz leģitīmiem piekļuves prasītājiem pēc to likumīgiem un pienācīgi pamatotiem pieprasījumiem piekļuvi īpašiem domēnu nosaukumu reģistrācijas datiem, ievērojot Savienības datu aizsardzības tiesību aktus. Dalībvalstis nodrošina, ka ALD **nosaukumu** reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD, bez nepamatotas kavēšanās **un jebkurā gadījumā 72 stundu laikā** atbild uz visiem piekļuves pieprasījumiem. Dalībvalstis nodrošina, ka politika un procedūras šādu datu izpaušanai tiek publiskotas.

II iedaļa

Jurisdikcija un reģistrācija

24. pants

Jurisdikcija un teritorialitāte

1.a Saskaņā ar šo direktīvu uzskata, ka vienības ir tās dalībvalsts jurisdikcijā, kurā tās sniedz savus pakalpojumus. Uzskata, ka vienības, kas minētas I pielikuma 1.–7. punktā un 10. punktā, uzticamības pakalpojumu sniedzēji un interneta plūsmu apmaiņas punktu nodrošinātāji, kas minēti I pielikuma 8. punktā, un vienības, kas minētas II pielikuma 1.–5. punktā, ir tās dalībvalsts jurisdikcijā, kuras teritorijā tie ir iedibināti.

1. DNS pakalpojumu sniedzējus, ALD nosaukumu reģistrus [...] **un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD**, mākoņdatošanas pakalpojumu sniedzējus, datu centru pakalpojumu sniedzējus, [...] satura piegādes tīklu nodrošinātājus, **pārvaldītu pakalpojumu sniedzējus un pārvaldītu drošības pakalpojumu sniedzējus,** kas minēti I pielikuma 8. **un 8.a** punktā, kā arī digitālo pakalpojumu sniedzējus, kas minēti II pielikuma 6. punktā, uzskata par tādiem, kas ir tās dalībvalsts jurisdikcijā, kurā atrodas to galvenais iedibinājums Savienībā.

2. Šīs direktīvas nolūkos vienības, kas minētas 1. punktā, uzskata par vienībām, kuru galvenais iedibinājums Savienībā ir tajā dalībvalstī, kurā **galvenokārt** tiek pieņemti lēmumi saistībā ar kiberdrošības riska pārvaldības pasākumiem. Ja **nevar noteikt vietu, kur galvenokārt tiek pieņemti šādi lēmumi, vai** ja šādus lēmumus nepieņem nevienā iedibinājumā Savienībā, tad uzskata, ka galvenais iedibinājums ir tajā dalībvalstī, kurā vienības ir iedibinātas ar vislielāko darbinieku skaitu Savienībā. **Ja pakalpojumus sniedz uzņēmumu grupa, tad par galveno iedibinājumu uzskata uzņēmumu grupas galveno iedibinājumu.**

3. Ja 1. punktā minētā vienība nav iedibināta Savienībā, bet piedāvā pakalpojumus Savienībā, tad tā izraugās pārstāvi Savienībā. Minētais pārstāvis ir iedibināts vienā no tām dalībvalstīm, kurās tiek piedāvāti pakalpojumi. Uzskata, ka šāda vienība ir tās dalībvalsts jurisdikcijā, kurā ir iedibināts pārstāvis. Ja nav izraudzīta pārstāvja Savienībā atbilstoši šim pantam, jebkura dalībvalsts, kurā vienība sniedz pakalpojumus, var veikt tiesiskas darbības pret vienību sakarā ar neatbilstību šajā direktīvā noteiktajiem pienākumiem.

4. Vienības veiktā pārstāvja izraudzīšanās, kā minēts 1. punktā, neskar tiesiskās darbības, ko var ierosināt pret pašu vienību.

4.a Dalībvalstis, kas ir saņēmušas savstarpējas palīdzības lūgumu attiecībā uz 1. punktā minētajām vienībām, var minētā lūguma robežās veikt pienācīgus uzraudzības un izpildes pasākumus attiecībā uz attiecīgo vienību, kas to teritorijā sniedz pakalpojumus vai kam tur ir tīkls un informācijas sistēma.

25. pants

Dažu digitālās infrastruktūras vienību un digitālo pakalpojumu sniedzēju reģistrs

1. [...] **Dalībvalstis nodrošina, lai no 24. panta 1. punktā minētajām** vienībām, **kuru galvenais iedibinājums ir to teritorijā vai, ja tās nav iedibinātas Savienībā, kuru izraudzītais pārstāvis Savienībā ir iedibināts to teritorijā, tiktu prasīts** [...] līdz [vēlākais,12 mēneši pēc direktīvas stāšanās spēkā] [...] iesniegt **kompetentajām iestādēm** šādu informāciju:

a) vienības nosaukums;

aa) vienības veids kā šīs direktīvas I un II pielikumā;

b) tās galvenā iedibinājuma adrese un citu tās juridisko iedibinājumu adrese Savienībā vai, ja vienība Savienībā nav iedibināta, tad atbilstoši 24. panta 3. punktam izraudzītā tās pārstāvja iedibinājuma adrese Savienībā;

c) jaunākā kontaktinformācija, ieskaitot vienību **un to pārstāvju** e-pasta adreses un tālruņa numurus;

d) dalībvalstis, kurās vienība sniedz pakalpojumu.

Attiecīgā gadījumā šo informāciju iesniedz, izmantojot 2.a pantā minēto valsts mehānismu[...] patstāvīgai paziņošanai.

2. **Dalībvalstis nodrošina, lai** [...] vienības, kas minētas 1. punktā, [...] **paziņotu arī** par visām izmaiņām informācijā, ko tās iesniegušas atbilstoši 1. punktam, nekavējoties un katrā ziņā trīs mēnešu laikā no attiecīgo izmaiņu stāšanās spēkā.

3. [...] **Dalībvalstu vienotie kontaktpunkti 1. un 2. punktā minēto informāciju** [...] nodod [...] ***ENISA***. [...]

3.a Pamatojoties uz informāciju, kas saņemta saskaņā ar šā panta 3. punktu, *ENISA* izveido un uztur 1. punktā minēto vienību reģistru. Pēc dalībvalstu pieprasījuma *ENISA* dod iespēju attiecīgajām kompetentajām iestādēm piekļūt reģistram, vienlaikus attiecīgā gadījumā nodrošinot nepieciešamās garantijas, lai aizsargātu informācijas konfidencialitāti.

4. [...]

V NODAĻA

Informācijas apmaiņa

26. pants

Kiberdrošības informācijas apmaiņas pasākumi

1. [...] Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības **brīvprātīgi** var savstarpēji apmainīties ar būtisku kiberdrošības informāciju, ieskaitot informāciju, kas attiecas uz kiberdraudiem, **gandrīz notikušiem notikumiem**, neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem, ja šāda informācijas apmaiņa:

   a) ir paredzēta, lai novērstu vai atklātu incidentus vai reaģētu uz tiem, vai mazinātu to riskus;

b) veicina kiberdrošības līmeni, it īpaši – palielinot informētību attiecībā uz kiberdraudiem, ierobežojot vai traucējot kiberdraudu izplatīšanos, atbalstot virkni aizsardzības spēju, neaizsargātības izlabošanu un atklāšanu, draudu atklāšanas metodes, seku mazināšanas stratēģijas vai reaģēšanas un seku novēršanas posmus.

2. Dalībvalstis nodrošina, ka informācijas apmaiņa notiek būtisko un svarīgo vienību [...] kopienās. Šādu apmaiņu īsteno, veicot informācijas apmaiņas pasākumus attiecībā uz informācijas iespējami sensitīvo raksturu.

3. Dalībvalstis [...] **var** pieņemt noteikumus, kuros precizē 2. punktā minēto informācijas apmaiņas pasākumu procedūru, operatīvos elementus (tostarp speciālu IKT platformu izmantošanu), saturu un nosacījumus. Šādos noteikumos [...] **var** arī sīkāk aprakstīt publisku iestāžu iesaistīšanos šādos pasākumos, kā arī operatīvos elementus, tostarp speciālu IT platformu izmantošanu. Dalībvalstis piedāvā atbalstu šādu pasākumu piemērošanā atbilstoši to politikas nostādnēm, kas minētas 5. panta 2. punkta g) apakšpunktā.

4. Būtiskās un svarīgās vienības informē kompetentās iestādes par savu dalību 2. punktā minētajos informācijas apmaiņas pasākumos, tiklīdz tās iesaistās šādos pasākumos, vai attiecīgā gadījumā — par izstāšanos no šādas dalības, tiklīdz izstāšanās stājas spēkā.

5. [...] *ENISA* atbalsta 2. punktā minēto kiberdrošības informācijas apmaiņas pasākumu izveidi, nodrošinot paraugpraksi un sniedzot norādījumus.

27. pants

Brīvprātīga būtiskas informācijas paziņošana

1. Neskarot 20. pantu, dalībvalstis nodrošina, lai būtiskas un svarīgas vienības var kompetentajām iestādēm vai *CSIRT* brīvprātīgi paziņot par jebkādiem attiecīgiem incidentiem, kiberdraudiem vai gandrīz notikušiem notikumiem.

2. Dalībvalstis nodrošina, ka, neskarot 3. pantu, vienības, uz kurām neattiecas šīs direktīvas darbības joma, var brīvprātīgi iesniegt paziņojumus par nozīmīgiem incidentiem, kiberdraudiem vai gandrīz notikušiem notikumiem. Apstrādājot paziņojumus, dalībvalstis rīkojas saskaņā ar 20. pantā noteikto procedūru. Dalībvalstis obligātos paziņojumus var apstrādāt, nosakot tiem prioritāti pār brīvprātīgajiem paziņojumiem. **Neskarot noziedzīgu nodarījumu izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem,** [...] brīvprātīgās paziņošanas rezultātā ziņotājai vienībai netiek uzlikti nekādi papildu pienākumi, kas uz to neattiektos, ja tā nebūtu iesniegusi minēto paziņojumu.

3. Brīvprātīgos paziņojumus apstrādā tikai tad, ja šāda apstrāde nerada nesamērīgu vai nepamatotu slogu attiecīgajai dalībvalstij.

VI NODAĻA

Uzraudzība un izpilde

28. pants

Vispārīgi uzraudzības un izpildes aspekti

1. Dalībvalstis nodrošina, ka kompetentās iestādes efektīvi uzrauga atbilstību šai direktīvai [...], it īpaši 18.**,** [...] 20 **un 23.** pantā noteiktajiem pienākumiem, un veic nepieciešamos pasākumus, lai nodrošinātu atbilstību tiem. **Dalībvalstis var atļaut kompetentajām iestādēm piešķirt prioritāti uzraudzībai, kuras pamatā ir uz risku balstīta pieeja.**

2. Pievēršoties incidentiem, kuru rezultātā notiek persondatu aizsardzības pārkāpumi, kompetentās iestādes strādā ciešā sadarbībā ar datu aizsardzības iestādēm, **kompetentām iestādēm, kuras izraudzītas, ievērojot Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], uzraudzības struktūrām, kuras izraudzītas, ievērojot Regulu (ES) Nr. 910/2014, un citām kompetentām iestādēm, kuras izraudzītas saskaņā ar nozarspecifiskiem Savienības tiesību aktiem**. [...]

3. Neskarot valsts tiesisko regulējumu un iestāžu sistēmu, dalībvalstis nodrošina, ka, uzraugot valsts pārvaldes vienību atbilstību šai direktīvai un piemērojot iespējamās sankcijas par neatbilstību, kompetentajām iestādēm ir atbilstīgas pilnvaras veikt šādus uzdevumus operatīvi neatkarīgi no uzraudzītajām vienībām. Dalībvalstis var lemt par piemērotu, samērīgu un efektīvu uzraudzības un izpildes pasākumu noteikšanu attiecībā uz šīm vienībām saskaņā ar valsts regulējumu un tiesisko kārtību.

29. pants

Uzraudzība un izpilde attiecībā uz būtiskajām vienībām

1. Dalībvalstis nodrošina, ka uzraudzības vai izpildes pasākumi, kas noteikti būtiskajām vienībām attiecībā uz šajā direktīvā noteiktajiem pienākumiem, ir iedarbīgi, samērīgi un atturoši, ņemot vērā katra atsevišķa gadījuma apstākļus.

2. Dalībvalstis nodrošina, ka kompetentās iestādes, kad tās īsteno savus uzraudzības uzdevumus attiecībā uz būtiskajām vienībām, **ievēro uz risku balstītu pieeju un** tām ir pilnvaras minētajām vienībām piemērot **vismaz**:

   a) pārbaudes uz vietas un attālinātu uzraudzību, arī pārbaudes izlases veidā;

   b) regulāru **drošības** revīziju;

   c) mērķtiecīgas drošības revīzijas, kas balstītas uz riska novērtējumiem vai ar risku saistītu pieejamo informāciju;

   d) drošības skenēšanu, pamatojoties uz objektīviem, nediskriminējošiem, taisnīgiem un pārredzamiem riska novērtēšanas kritērijiem**, ja tas nepieciešams tehnisku iemeslu dēļ, sadarbojoties ar attiecīgo vienību**;

   e) tādas informācijas pieprasījumus, kas nepieciešama, lai novērtētu vienības pieņemtos kiberdrošības pasākumus, tostarp dokumentētas kiberdrošības politikas nostādnes[...];

   f) pieprasījumus, lai piekļūtu datiem, dokumentiem vai jebkurai informācijai, kas nepieciešama to uzraudzības pienākumu izpildei;

   g) pieprasījumus par pierādījumiem, ka tiek īstenotas kiberdrošības politikas nostādnes, piemēram, kvalificēta revidenta veikto drošības revīziju rezultātiem un attiecīgajiem pamatpierādījumiem.

2.a Pildot šā panta 2. punktā paredzētos uzraudzības uzdevumus, kompetentās iestādes var izveidot uzraudzības metodiku, kas ļauj noteikt prioritātes attiecībā uz šādiem uzdevumiem, ievērojot uz risku balstītu pieeju.

3. Īstenojot savas pilnvaras atbilstoši 2. punkta e)–g) apakšpunktam, kompetentās iestādes norāda pieprasījuma mērķi un precizē prasīto informāciju.

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

a) izdot brīdinājumus par vienību neatbilstību šajā direktīvā noteiktajiem pienākumiem;

b) izdot saistošus norādījumus vai rīkojumu, pieprasot, lai minētās vienības izlabo konstatētos trūkumus vai šajā direktīvā noteikto pienākumu pārkāpumus;

c) uzdot minētajām iestādēm izbeigt rīcību, kas nav saderīga ar šajā direktīvā noteiktajiem pienākumiem, un atturēties no tādas rīcības atkārtošanas;

d) uzdot minētajām vienībām nodrošināt savu riska pārvaldības pasākumu un/vai ziņošanas pienākumu atbilstību 18. un 20. pantā paredzētajiem noteikumiem noteiktā veidā un termiņā;

e) uzdot minētajām vienībām informēt fizisko(-ās) vai juridisko(-ās) personu(-as), kam tās sniedz pakalpojumus vai veic darbības, kuras var ietekmēt nozīmīgi kiberdraudi, par **apdraudējuma raksturu, kā arī** par visiem iespējamajiem aizsardzības vai novēršanas pasākumiem, ko attiecīgā(-ās) fiziskā(-ās) vai juridiskā(-ās) persona(-as) var veikt, reaģējot uz šādiem draudiem;

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

g) [...]

h) uzdot minētajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos vērojama neatbilstība šajā direktīvā noteiktajiem pienākumiem**, ja šāda publiskošana nerada kaitējumu attiecīgajai vienībai**;

i) [...]

j) piemērot vai pieprasīt, lai attiecīgās struktūras vai tiesas saskaņā ar valsts tiesību aktiem piemēro administratīvu naudas sodu atbilstoši 31. pantam, tādējādi papildinot vai aizstājot pasākumus, kas minēti šā punkta a)–i) apakšpunktā, atkarībā no katra atsevišķa gadījuma apstākļiem.

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

a) apturēt vai pieprasīt, lai sertifikācijas vai apstiprināšanas struktūra **vai tiesas saskaņā ar valsts tiesību aktiem** aptur sertifikāciju vai atļauju attiecībā uz visiem būtiskās vienības sniegtajiem pakalpojumiem vai veiktajām darbībām vai to daļu;

b) piemērot vai pieprasīt, lai attiecīgās struktūras vai tiesas saskaņā ar valsts tiesību aktiem piemēro pagaidu aizliegumu jebkurai personai, kura īsteno vadības pienākumus galvenās izpildpersonas vai juridiskā pārstāvja līmenī minētajā vienībā, un jebkurai citai fiziskai personai, kura ir atbildīga par pārkāpumu, īstenot vadības funkcijas konkrētajā vienībā.

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

Šajā punktā paredzētās sankcijas 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 pārstāve, pamatojoties uz pilnvarām to pārstāvēt, pilnvarām pieņemt lēmumus tās vārdā vai pilnvarām īstenot kontroli pār to, ir pilnvaras nodrošināt vienības atbilstību šajā direktīvā noteiktajiem pienākumiem. Dalībvalstis nodrošina, ka minētās fiziskās personas var tikt sauktas pie atbildības, ja viņas pārkāpj savus pienākumus nodrošināt atbilstību šajā direktīvā noteiktajiem pienākumiem. **Attiecībā uz valsts pārvaldes vienībām – šis noteikums neskar dalībvalstu tiesību aktus attiecībā uz valsts ierēdņu un ievēlētu un ieceltu amatpersonu atbildību.**

7. Veicot jebkuru no izpildes darbībām vai piemērojot jebkuru no sankcijām atbilstoši 4. un 5. punktam, kompetentās iestādes ievēro aizstāvības tiesības un ņem vērā katra atsevišķā gadījuma apstākļus, un vismaz pienācīgi ņem vērā:

   a) pārkāpuma nopietnumu un pārkāpto noteikumu svarīgumu. Pārkāpumi, kas jāuzskata par nopietniem, cita starpā ir šādi: atkārtoti pārkāpumi, tādu incidentu nepaziņošana vai neizlabošana, kam ir ievērojama traucējumus izraisoša ietekme, trūkumu neizlabošana saskaņā ar kompetento iestāžu saistošiem norādījumiem, šķēršļu likšana revīzijām vai uzraudzības darbībām, ko uzdevusi kompetentā iestāde pēc pārkāpuma konstatēšanas, nepatiesas vai ļoti neprecīzas informācijas sniegšana saistībā ar riska pārvaldības prasībām vai ziņošanas pienākumiem, kas noteikti 18. un 20. pantā;

b) pārkāpumu ilgumu, tostarp atkārtotu pārkāpumu elementu;

c) izraisīto faktisko kaitējumu vai radušos zaudējumus, vai iespējamo kaitējumu vai zaudējumus, kas būtu varējuši rasties, ciktāl tos var noteikt. Izvērtējot šo aspektu, cita starpā ņem vērā faktiskos vai iespējamos finansiālos vai ekonomiskos zaudējumus, ietekmi uz citiem pakalpojumiem, skarto vai iespējami skarto lietotāju skaitu;

d) to, vai pārkāpums izdarīts tīši vai neuzmanības dēļ;

e) pasākumus, ko vienība veikusi, lai novērstu vai mazinātu kaitējumu un/vai zaudējumus;

f) apstiprinātu rīcības kodeksu vai apstiprinātu sertifikācijas mehānismu ievērošanu;

g) to, cik lielā mērā pie atbildības sauktā(-ās) fiziskā(-ās) vai juridiskā(-ās) persona(-as) sadarbojas ar kompetentajām iestādēm.

8. Kompetentās iestādes sīki argumentē savus izpildes lēmumus. Pirms šādu lēmumu pieņemšanas kompetentās iestādes informē attiecīgās vienības par saviem sākotnējiem konstatējumiem un atvēl vienībām saprātīgu termiņu apsvērumu iesniegšanai**, izņemot tūlītēja apdraudējuma gadījumā**.

9. Dalībvalstis nodrošina, ka to kompetentās iestādes **saskaņā ar šo direktīvu**, kad tās īsteno savas uzraudzības un izpildes pilnvaras, kuru mērķis ir nodrošināt, lai būtiska vienība, kas saskaņā ar Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva] identificēta kā kritiska, **[**vai vienība, kas ir līdzvērtīga kritiskai vienībai**]**, ievērotu šajā direktīvā noteiktos pienākumus, informē attiecīgās kompetentās iestādes **tajā pašā** [...] dalībvalstī [...], kuras izraudzītas, ievērojot Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva]. **Attiecīgā gadījumā** [...] kompetentās iestādes saskaņā ar Direktīvu (ES) XXX/XXX [Kritisko vienību noturības direktīva][...], **var pieprasīt** kompetentajām iestādēm **saskaņā ar šo direktīvu** [...] īstenot savas uzraudzības un izpildes **pilnvaras attiecībā uz** būtisku vienību, kas ietilpst šīs direktīvas darbības jomā un kas arī ir identificēta kā kritiska **[**vai līdzvērtīga**]** **saskaņā ar Direktīvu (ES) XXXX/XXXX [Kritisko vienību noturības direktīva].**

10. Dalībvalstis nodrošina, ka to kompetentās iestādes saskaņā ar šo direktīvu informē Pārraudzības forumu, ievērojot Regulas (ES) XXXX/XXXX [*DORA*] 29. panta 1. punktu, kad tās īsteno savas uzraudzības un izpildes pilnvaras, kuru mērķis ir nodrošināt, lai būtiska vienība, kas, ievērojot Regulas (ES) XXXX/XXXX [*DORA*] 28. pantu, ir izraudzīta par kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, ievērotu šajā direktīvā noteiktos pienākumus.

10.a Dalībvalstis nodrošina, ka to kompetentās iestādes saskaņā ar šo direktīvu informē attiecīgās kompetentās iestādes, kas izraudzītas, ievērojot Regulu (ES) Nr. 910/2014, kad tās īsteno savas uzraudzības un izpildes pilnvaras, kuru mērķis ir nodrošināt, lai vienība, kas izraudzīta par uzticamības pakalpojumu sniedzējiem, ievērojot Regulu (ES) Nr. 910/2014, pildītu šajā direktīvā noteiktos pienākumus.

30. pants

Uzraudzība un izpilde attiecībā uz svarīgām vienībām

1. Saņemot pierādījumus vai norādes, **vai informāciju** par to, ka svarīga vienība, **iespējams**, nepilda šajā direktīvā un jo īpaši tās 18. un 20. pantā noteiktos pienākumus, dalībvalstis nodrošina, ka kompetentās iestādes rīkojas, nepieciešamības gadījumā īstenojot *ex post* uzraudzības pasākumus.

2. Dalībvalstis nodrošina, ka kompetentās iestādes, kad tās pilda savus uzraudzības uzdevumus attiecībā uz svarīgām vienībām, **ievēro uz risku balstītu pieeju un** tām ir pilnvaras minētajām vienībām piemērot **vismaz**:

   a) pārbaudes uz vietas un attālinātu *ex post* uzraudzību;

   b) mērķtiecīgas drošības revīzijas, kas balstītas uz riska novērtējumiem vai ar risku saistītu pieejamo informāciju;

   c) drošības skenēšanu, pamatojoties uz objektīviem, **nediskriminējošiem**, taisnīgiem un pārredzamiem riska novērtēšanas kritērijiem, **ja tas nepieciešams tehnisku iemeslu dēļ, sadarbojoties ar attiecīgo vienību**;

   d) tādas informācijas pieprasījumus, kas nepieciešama, lai novērtētu veiktos kiberdrošības pasākumus[...];

   e) pieprasījumus piekļūt datiem, dokumentiem un/vai informācijai, kas nepieciešama uzraudzības pienākumu izpildei;

   ea) pieprasījumus sniegt pierādījumus par to, ka tiek īstenotas kiberdrošības politikas nostādnes, piemēram, kvalificēta revidenta veikto drošības revīziju rezultātus un attiecīgos pamatpierādījumus.

2.a Pildot šā panta 2. punktā paredzētos uzraudzības uzdevumus, kompetentās iestādes var izveidot uzraudzības metodiku, kas ļauj noteikt prioritātes attiecībā uz šādiem uzdevumiem, ievērojot uz risku balstītu pieeju.

3. Īstenojot savas pilnvaras atbilstoši 2. punkta d) –**ea)** apakšpunktam, kompetentās iestādes norāda pieprasījuma mērķi un precizē prasīto informāciju.

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

a) izdot brīdinājumus par vienību neatbilstību šajā direktīvā noteiktajiem pienākumiem;

b) izdot saistošus norādījumus vai rīkojumu, pieprasot, lai minētās vienības izlabo konstatētos trūkumus vai šajā direktīvā noteikto pienākumu pārkāpumu;

c) uzdot minētajām iestādēm izbeigt rīcību, kas nav saderīga ar šajā direktīvā noteiktajiem pienākumiem, un atturēties no tādas rīcības atkārtošanas;

d) uzdot minētajām vienībām nodrošināt savu riska pārvaldības pasākumu vai ziņošanas pienākumu atbilstību 18. un 20. pantā paredzētajiem noteikumiem noteiktā veidā un termiņā;

e) uzdot minētajām vienībām informēt fizisko(-ās) vai juridisko(-ās) personu(-as), kam tās sniedz pakalpojumus vai veic darbības, kuras var ietekmēt nozīmīgi kiberdraudi, par **apdraudējuma raksturu, kā arī** par visiem iespējamajiem aizsardzības vai novēršanas pasākumiem, ko attiecīgā(-ās) fiziskā(-ās) vai juridiskā(-ās) persona(-as) var veikt, reaģējot uz šādiem draudiem;

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

g) uzdot minētajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos vērojama neatbilstība šajā direktīvā noteiktajiem pienākumiem**, ja šāda publiskošana nerada kaitējumu attiecīgajai vienībai**;

h) [...]

i) piemērot vai pieprasīt, lai attiecīgās struktūras vai tiesas saskaņā ar valsts tiesību aktiem piemēro administratīvu naudas sodu atbilstoši 31. pantam, tādējādi papildinot vai aizstājot pasākumus, kas minēti šā punkta a)–h) apakšpunktā, atkarībā no katra atsevišķa gadījuma apstākļiem.

5. Uzraudzības un izpildes pasākumiem, kas paredzēti šajā pantā attiecībā uz [...] svarīgajām vienībām [...], piemēro arī 29. panta 6.–8. punktu.

31. pants

Vispārīgi nosacījumi administratīvo naudas sodu piemērošanai būtiskajām un svarīgajām vienībām

1. Dalībvalstis nodrošina, ka administratīvo naudas sodu piemērošana būtiskajām un svarīgajām vienībām atbilstoši šim pantam saistībā ar šajā direktīvā noteikto pienākumu pārkāpumiem katrā atsevišķā gadījumā ir iedarbīga, samērīga un atturoša.

2. Administratīvos naudas sodus atkarībā no katra individuālā gadījuma apstākļiem piemēro, ar tiem papildinot vai aizstājot pasākumus, kas minēti 29. panta 4. punkta a)–i) apakšpunktā, 29. panta 5. punktā un 30. panta 4. punkta a)–h) apakšpunktā.

3. Izlemjot, vai piemērot administratīvu naudas sodu, un lemjot par tā summu, katrā individuālā gadījumā pienācīgi ņem vērā vismaz 29. panta 7. punktā paredzētos elementus.

4. Dalībvalstis nodrošina, ka par 18. vai 20. pantā noteikto pienākumu pārkāpumiem, ko veic **būtiskās vienības**, saskaņā ar šā panta 2. un 3. punktu piemēro administratīvus naudas sodus, kuru maksimālais apjoms ir vismaz **4**[...] 000 000 EUR vai **– juridiskas personas gadījumā –** [...] 2 % no tā uzņēmuma kopējā gada apgrozījuma visā pasaulē, pie kura pieder būtiskā [...] vienība, iepriekšējā finanšu gadā atkarībā no tā, kura no summām ir lielāka.

4.a Dalībvalstis nodrošina, ka par 18. vai 20. pantā noteikto pienākumu pārkāpumiem, ko veic svarīgās vienības, saskaņā ar šā panta 2. un 3. punktu piemēro administratīvus naudas sodus, kuru maksimālais apjoms ir vismaz 2 000 000 EUR vai – juridiskas personas gadījumā – 1 % no tā uzņēmuma kopējā gada apgrozījuma visā pasaulē, pie kura pieder svarīgā vienība, iepriekšējā finanšu gadā atkarībā no tā, kura no summām ir lielāka.

5. Dalībvalstis var paredzēt pilnvaras piemērot periodiskus soda maksājumus, lai būtiskajai vai svarīgajai vienībai liktu izbeigt pārkāpumu, saskaņā ar kompetentās iestādes iepriekšēju lēmumu.

6. Neskarot 29. un 30. pantā noteiktās kompetento iestāžu pilnvaras, katra dalībvalsts var pieņemt noteikumus par to, vai un līdz kādam apjomam administratīvos naudas sodus var piemērot valsts pārvaldes vienībām, kas minētas 4. panta 23. punktā, ievērojot šajā direktīvā paredzētos pienākumus.

6.a Ja dalībvalsts tiesību sistēmā nav paredzēti administratīvi naudas sodi, dalībvalstis nodrošina, ka šo pantu var piemērot tā, ka naudas sodu ierosina kompetentā iestāde un piemēro valsts kompetentās tiesas, vienlaikus nodrošinot, ka minētie tiesību aizsardzības līdzekļi ir efektīvi un tiem ir tāda pati iedarbība kā kompetento iestāžu piemērotiem administratīviem naudas sodiem. Jebkurā gadījumā uzliktie naudas sodi ir efektīvi, samērīgi un atturoši. Minētās dalībvalstis līdz [...] paziņo Komisijai to tiesību aktu noteikumus, ko tās pieņem, ievērojot šo punktu, un nekavējoties paziņo Komisijai par jebkuru turpmāku grozošo aktu vai jebkuriem turpmākiem šo noteikumu grozījumiem.

32. pants

Pārkāpumi, kas ietver persondatu aizsardzības pārkāpumu

1. Ja kompetentajām iestādēm **uzraudzības un izpildes gaitā** [...] **kļūst zināms**, ka būtiskas vai svarīgas vienības izdarīts **šīs direktīvas** 18. un 20. pantā noteikto pienākumu pārkāpums **var** ietvert [...] persondatu aizsardzības pārkāpumu, kas definēts Regulas (ES) 2016/679 4. panta 12. punktā un ko paziņo atbilstoši minētās regulas 33. pantam, tās **bez liekas kavēšanās** informē uzraudzības iestādes, kas ir kompetentas atbilstoši minētās regulas 55. un 56. pantam [...].

2. Ja uzraudzības iestādes, kas ir kompetentas saskaņā ar Regulas (ES) 2016/679 55. un 56. pantu, nolemj īstenot savas pilnvaras saskaņā ar minētās regulas 58. panta **2.** punkta i) apakšpunktu un piemērot administratīvu naudas sodu, **šīs direktīvas 8. pantā minētās** kompetentās iestādes nepiemēro administratīvu naudas sodu par [...] šīs direktīvas 31. panta pārkāpumu**, kas izdarīts ar to pašu rīcības aktu**. Tomēr kompetentās iestādes var piemērot izpildes darbības vai īstenot sankciju piemērošanas pilnvaras, kas paredzētas šīs direktīvas 29. panta 4. punkta a)–i) apakšpunktā, 29. panta 5. punktā un 30. panta 4. punkta a)–h) apakšpunktā.

3. Ja uzraudzības iestāde, kas ir kompetenta atbilstoši Regulai (ES) 2016/679, veic darbību citā dalībvalstī, kas nav kompetentās iestādes dalībvalsts, kompetentā iestāde var informēt uzraudzības iestādi, kas veic darbību minētajā dalībvalstī.

33. pants

Sodi

1. Dalībvalstis paredz noteikumus par sodiem, kas piemērojami par to valsts tiesību normu pārkāpumiem, kuras pieņemtas, ievērojot šo direktīvu, un veic visus nepieciešamos pasākumus, lai nodrošinātu to piemērošanu. Paredzētie sodi ir efektīvi, samērīgi un atturoši.

2. Dalībvalstis, vēlākais, [divus] gadus pēc šīs direktīvas stāšanās spēkā informē Komisiju par minētajiem noteikumiem un pasākumiem un bez nepamatotas kavēšanās informē to par visiem turpmākajiem grozījumiem, kas tos skar.

34. pants

Savstarpēja palīdzība

1. Ja būtiska vai svarīga vienība sniedz pakalpojumus vairāk nekā vienā dalībvalstī vai [...] **sniedz pakalpojumus vienā vai vairākās** dalībvalstī**s**, bet tās tīklu un informācijas sistēmas atrodas vienā vai vairākās citās dalībvalstīs, **attiecīgo** dalībvalst**u** kompetentā**s** iestāde**s** vajadzības gadījumā sadarbojas un cita citai palīdz. Minētā sadarbība ietver vismaz turpmāk minēto:

a) kompetentās iestādes, kas piemēro uzraudzības vai izpildes pasākumus dalībvalstī, ar vienotā kontaktpunkta starpniecību informē un konsultē pārējo attiecīgo dalībvalstu kompetentās iestādes par veiktajiem uzraudzības un izpildes pasākumiem [...];

b) kompetentā iestāde vai pieprasīt, lai cita kompetentā iestāde veic [...] uzraudzības vai izpildes pasākumus;

c) kompetentā iestāde, saņemot pamatotu lūgumu no citas kompetentās iestādes, sniedz otrai kompetentajai iestādei palīdzību, **kas ir proporcionāla pašas rīcībā esošajiem resursiem**, lai uzraudzības vai izpildes pasākumus [...] varētu īstenot efektīvi, iedarbīgi un konsekventi. Šāda savstarpējā palīdzība var ietvert informācijas pieprasījumus un uzraudzības pasākumus, tostarp pieprasījumus veikt pārbaudes uz vietas vai attālinātu uzraudzību, vai mērķtiecīgas drošības revīzijas. Kompetentā iestāde, kam adresēts lūgums sniegt palīdzību, nedrīkst atteikt šo palīdzību, ja vien pēc informācijas apmaiņas ar pārējām attiecīgajām iestādēm [...] netiek konstatēts [...], ka vai nu iestāde nav kompetenta sniegt lūgto palīdzību vai **tai nav nepieciešamo resursu**, vai lūgtā palīdzība nav samērīga ar kompetentās iestādes veiktajiem uzraudzības uzdevumiem [...], **vai arī lūgums attiecas uz informāciju vai ietver darbības, kas ir pretrunā attiecīgās dalībvalsts valsts drošībai vai sabiedriskajai drošībai, vai aizsardzībai**.

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

VII NODAĻA

Pārejas un nobeiguma noteikumi

35. pants

Pārskatīšana

Komisija periodiski pārskata šīs direktīvas darbību un iesniedz ziņojumu Eiropas Parlamentam un Padomei. Ziņojumā galvenokārt novērtē I un II pielikumā minēto nozaru, apakšnozaru un vienību lieluma un veida nozīmīgumu ekonomikas darbībai un sabiedrībai saistībā ar kiberdrošību. [...] **Pārskatīšanas** nolūkā [...] Komisija ņem vērā [...] *CSIRT* tīkla ziņojumus par operatīvā līmenī [...] gūto pieredzi. Pirmo ziņojumu iesniedz līdz … [54 mēneši pēc šīs direktīvas spēkā stāšanās dienas].

36. pants

[...]

[...]

[...]

37. pants

Komiteju procedūra

1. Komisijai palīdz komiteja. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 nozīmē.

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

3. Ja komitejas atzinums jāsaņem rakstiskā procedūrā, minēto procedūru izbeidz, nepanākot rezultātu, ja atzinuma sniegšanas termiņā tā nolemj komitejas priekšsēdētājs vai to pieprasa kāds komitejas loceklis.

38. pants

Transponēšana

1. Dalībvalstis **līdz** … [[...] **24** mēneši pēc šīs direktīvas spēkā stāšanās dienas **]** pieņem un publicē [...] normatīvos un administratīvos aktus, kas vajadzīgi, lai izpildītu šīs direktīvas prasības. Dalībvalstis par to tūlīt informē Komisiju. Tās minētos aktus piemēro no ... [nākamā diena pēc pirmajā daļā minētā datuma].

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

39. pants

Grozījums Regulā (ES) Nr. 910/2014

Regulas (ES) Nr. 910/2014 19. pantu [...] svītro **no... [šīs direktīvas transponēšanas termiņa datums].**

40. pants

Grozījums Direktīvā (ES) 2018/1972

Direktīvas (ES) 2018/1972 40. un 41. pantu [...] svītro **no... [šīs direktīvas transponēšanas termiņa datums].**

41. pants

Atcelšana

Direktīvu (ES) 2016/1148 atceļ no .... [šīs direktīvas transponēšanas termiņa datums].

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

42. pants

Stāšanās spēkā

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

43. pants

Adresāti

Šī direktīva ir adresēta dalībvalstīm.

Briselē,

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

I PIELIKUMS

NOZARES, APAKŠNOZARES UN VIENĪBU VEIDI

Nozare	Apakšnozare	Vienības veids
1. Enerģētika	a) Elektroenerģija	– Elektroenerģijas uzņēmumi, kas minēti Direktīvas (ES) 2019/944 2. panta 57. punktā un izpilda "piegādes" funkciju, uz kuru norādīts minētās direktīvas ([39]) 2. panta 12. punktā.
		– Sadales sistēmu operatori, kas minēti Direktīvas (ES) 2019/944 2. panta 29. punktā
		– Pārvades sistēmu operatori, kas minēti Direktīvas (ES) 2019/944 2. panta 35. punktā
		– Ražotāji, kas minēti Direktīvas (ES) 2019/944 2. panta 38. punktā
		— Nominēti elektroenerģijas tirgus operatori, kas minēti Regulas (ES) 2019/943 [40] 2. panta 8. punktā
		– Elektroenerģijas tirgus dalībnieki, kas minēti Regulas (ES) 2019/943 2. panta 25. punktā un sniedz agregēšanas, pieprasījumreakcijas vai enerģijas uzkrāšanas pakalpojumus, kuri minēti Direktīvas (ES) 2019/944 2. panta

[39] 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.).

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

		18., 20. un 59. punktā
	b) Centralizēta siltumapgāde un aukstumapgāde	– Centralizēta siltumapgāde vai aukstumapgāde, kas minēta 2. panta 19. punktā Direktīvā (ES) 2018/2001 ([41]) par no atjaunojamajiem energoresursiem iegūtas enerģijas izmantošanas veicināšanu
	c) Nafta	– Naftas pārvades cauruļvadu operatori
		– Naftas ražošanas operatori, pārstrādes un attīrīšanas iekārtas, uzglabāšana un pārvade
		— Centrālās krājumu uzturēšanas struktūras, kas minētas Padomes Direktīvas 2009/119/EK ([42]) 2. panta f) punktā
	d) Gāze	– Piegādes uzņēmumi, kas minēti Direktīvas (ES) 2009/73/EK([43]) 2. panta 8. punktā
		– Sadales sistēmu operatori, kas minēti Direktīvas 2009/73/EK 2. panta 6. punktā
		– Pārvades sistēmu operatori, kas minēti Direktīvas 2009/73/EK 2. panta 4. punktā

41 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.).

42 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.).

43 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.).

		– Uzglabāšanas sistēmu operatori, kas minēti Direktīvas 2009/73/EK 2. panta 10. punktā
		– SDG sistēmu operatori, kas minēti 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
2. Transports	a) Gaisa transports	– Gaisa pārvadātāji, kas minēti Regulas (EK) Nr. 300/2008 ([44]) 3. panta 4. punktā **un ko izmanto komerciāliem mērķiem**
		– Lidostas administrācijas, kas minētas Direktīvas 2009/12/EK ([45]) 2. panta 2. punktā, lidostas, kas minētas direktīvas 2. panta 1. punktā, tostarp pamatlidostas, kas uzskaitītas Regulas (ES) Nr. 1315/2013 ([46]) II pielikuma 2. iedaļā, un vienības, kas nodarbojas ar tādu palīgiekārtu ekspluatāciju, kuras atrodas lidostās

[44] 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.).

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

[46] 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.).

		– Satiksmes pārvaldības kontroles operatori, kas sniedz gaisa satiksmes vadības (ATC) pakalpojumus, kā minēts Regulas (EK) Nr. 549/2004 ([47]) 2. panta 1. punktā
	b) Dzelzceļa transports	– Infrastruktūras pārvaldītāji, kas minēti Direktīvas 2012/34/ES ([48]) 3. panta 2. punktā
		– Dzelzceļa pārvadājumu uzņēmumi, kas minēti Direktīvas 2012/34/ES 3. panta 1. punktā, tostarp apkalpes vietas operatori, kas minēti Direktīvas 2012/34/ES 3. panta 12. punktā
	c) Ūdens transports	– Iekšējo, jūras un piekrastes ūdens transporta pasažieru un kravu pārvadājumu uzņēmumi, kā attiecībā uz jūras transportu minēts Regulas (EK) Nr. 725/2004 ([49]) I pielikumā, neietverot atsevišķus kuģus, kurus ekspluatē minētie uzņēmumi
		– Tādu ostu pārvaldības struktūras, kas minētas Direktīvas 2005/65/EK ([50]) 3. panta 1. punktā, tostarp to ostas iekārtas, kas minētas Regulas (EK) Nr. 725/2004 2. panta 11. punktā, un vienības, kas ekspluatē rūpnīcas un iekārtas, kuras atrodas ostās

[47] 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.).

[48] 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.).

[49] 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.).

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

		– Tādu kuģu satiksmes dienestu operatori, kas minēti Direktīvas 2002/59/EK [51] 3. panta o) punktā
	d) Autotransports	– Par autoceļiem atbildīgās iestādes, kas minētas Komisijas Deleģētās regulas (ES) 2015/962 ([52]) 2. panta 12. punktā un atbild par satiksmes pārvaldības kontroli, **izņemot publiskas vienības, attiecībā uz kurām satiksmes pārvaldība vai intelektisko transporta sistēmu operatori ir tikai nebūtiska to vispārējās darbības daļa**
		– Tādu intelektisko transporta sistēmu operatori, kas minētas Direktīvas 2010/40/ES ([53]) 4. panta 1. punktā
3. Banku pakalpojumi		— Kredītiestādes, kas minētas Regulas (ES) Nr. 575/2013 ([54]) 4. panta 1. punktā**, [izņemot tās, kuras minētas Direktīvas 2013/36/ES 2. panta 5. punkta 8) apakšpunktā un uz kurām attiecas atbrīvojums saskaņā ar Regulas XX [*DORA*] 2. panta 4. punktu]**

[51] 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.).

[52] 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.).

[53] 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.).

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

4. Finanšu tirgus infrastruktūras		– Tādu tirdzniecības vietu operatori, kas minētas Direktīvas 2014/65/ES ([55]) 4. panta 24. punktā
		– Centrālie darījumu partneri (CCP), kas minēti Regulas (ES) Nr. 648/2012 ([56]) 2. panta 1. punktā
5. Veselība		— Veselības aprūpes sniedzēji, kas minēti Direktīvas 2011/24/ES ([57]) 3. panta g) punktā
		— ES references laboratorijas, kas minētas Regulas XXXX/XXXX par nopietniem pārrobežu veselības apdraudējumiem [58] 15. pantā
		— Vienības, kas veic izpētes un izstrādes darbības attiecībā uz zālēm, kas minētas Direktīvas 2001/83/EK ([59]) 1. panta 2. punktā — Vienības, kas ražo farmaceitiskās pamatvielas un farmaceitiskos preparātus, kuri minēti *NACE* 2. red. 21. nodaļas C sadaļā — Vienības, kas ražo medicīniskās

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

[56] 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.).

[57] 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.).

[58] [Eiropas Parlamenta un Padomes regula par nopietniem pārrobežu veselības apdraudējumiem un ar ko atceļ Lēmumu Nr. 1082/2013/ES; atsauce jāatjaunina, tiklīdz būs pieņemts priekšlikums COM(2020) 727 final]

[59] 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.).

		ierīces, kuras uzskata par kritiski svarīgām sabiedrības veselības ārkārtas situācijas laikā (“sabiedrības veselības ārkārtas situācijas kritiski svarīgo ierīču saraksts”) un kuras minētas Regulas XXXX [60] 20. pantā
6. Dzeramais ūdens		Tāda dzeramā ūdens piegādātāji un izplatītāji, kas definēts Padomes Direktīvas 98/83/EK [61] 2. panta 1. punkta a) apakšpunktā, bet izņemot izplatītājus, kuriem dzeramā ūdens izplatīšana ir tikai **nebūtiska** daļa no to veiktās patēriņa preču un pārējo preču izplatīšanas vispārējās darbības [...]
7. Notekūdeņi		Uzņēmumi, kas savāc, utilizē vai attīra komunālos, sadzīves un rūpnieciskos notekūdeņus, kā minēts Padomes Direktīvas ([62]) 91/271/EEK 2. panta 1.–3. punktā**, bet izņemot uzņēmumus, kuriem komunālo, sadzīves un rūpniecisko notekūdeņu savākšana, utilizēšana vai attīrīšana ir tikai nebūtiska to vispārējās darbības daļa.** [...]
8. Digitālā infrastruktūra		**–** Interneta plūsmu apmaiņas punktu nodrošinātāji
		– DNS pakalpojumu sniedzēji**, izņemot saknes nosaukuma serveru operatorus**
		— ALD nosaukumu reģistri

[60] [Eiropas Parlamenta un Padomes regula par pastiprinātu Eiropas Zāļu aģentūras lomu attiecībā uz zālēm un medicīniskajām ierīcēm krīžgatavības un krīžu pārvaldības kontekstā; atsauce jāatjaunina, tiklīdz būs pieņemts priekšlikums COM(2020) 725 final]

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

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

		– Mākoņdatošanas pakalpojumu sniedzēji
		– Datu centru pakalpojumu sniedzēji
		– Satura piegādes tīklu nodrošinātāji
		– Uzticamības pakalpojumu sniedzēji, kas minēti Regulas (ES) Nr. 910/2014 ([63]) 3. panta 19. punktā
		– Publisko elektronisko sakaru tīklu, kas minēti Direktīvas (ES) 2018/1972 ([64]) 2. panta 8. punktā, nodrošinātāji vai elektronisko sakaru pakalpojumu, kas minēti Direktīvas (ES) 2018/1972 2. panta 4. punktā, sniedzēji, ja to pakalpojumi ir publiski pieejami
8.a IKT pakalpojumu pārvaldība **(B2B)**		— **Pārvaldītu pakalpojumu sniedzēji (*MSP*)** — **Pārvaldītu drošības pakalpojumu sniedzēji (*MSSP*)**

63 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.).

64 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.).

9. Valsts pārvaldes **vienības**		— Centrālo valdību valsts pārvaldes vienības, **ko definējusi dalībvalsts saskaņā ar valsts tiesību aktiem** — [...][65][...] — [...]
10. Kosmoss		— Zemes infrastruktūras, kas pieder dalībvalstīm vai privātpersonām vai ko pārvalda un ekspluatē dalībvalstis vai privātpersonas, operatori, kas atbalsta kosmosā izvietotu pakalpojumu sniegšanu, izņemot Direktīvas (ES) 2018/1972 2. panta 8. punktā minēto publisko elektronisko sakaru tīklu nodrošinātājus

65 [...]

II PIELIKUMS

NOZARES, APAKŠNOZARES UN VIENĪBU VEIDI

Nozare	Apakšnozare	Vienības veids
1. Pasta un kurjeru pakalpojumi		Tādu pasta pakalpojumu sniedzēji, kas minēti Direktīvas 97/67/EK ([66]) 2. panta 1.[...] punktā, **tostarp** [...] kurjeru pakalpojumu sniedzēji
2. Atkritumu apsaimniekošana		Uzņēmumi, kas veic atkritumu apsaimniekošanu, kā minēts Direktīvas 2008/98/EK ([67]) 3. panta 9. punktā, taču izņemot uzņēmumus, kuriem atkritumu apsaimniekošana nav to galvenā saimnieciskā darbība

[66] 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.)**, kas grozīta ar Eiropas Parlamenta un Padomes Direktīvu 2008/6/EK (2008. gada 20. februāris), ar ko Direktīvu 97/67/EK groza attiecībā uz Kopienas pasta pakalpojumu iekšējā tirgus pilnīgu izveidi (OV L 52, 27.2.2008, 3. lpp.)**.

[67] 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.).

3. Ķīmisko vielu izgatavošana, ražošana un izplatīšana		Uzņēmumi, kas veic vielu un [...] **maisījumu** izgatavošanu [...] un izplatīšanu un kas minēti Regulas (EK) Nr. 1907/2006 ([68]) 3. panta [...], 9. un 14. punktā, **un uzņēmumi, kas veic minētās regulas 3. panta 3. punktā minēto izstrādājumu ražošanu no vielām vai maisījumiem.**
4. Pārtikas ražošana, pārstrāde un izplatīšana		Pārtikas uzņēmumi, kas minēti Regulas (EK) Nr. 178/2002 ([69]) 3. panta 2. punktā **un kas nodarbojas ar izplatīšanu vairumtirdzniecībā un rūpniecisko ražošanu un pārstrādi**
5. Ražošana	a) Medicīnisko ierīču un *in vitro* diagnostikas medicīnisko ierīču ražošana	Vienības, kas ražo medicīniskas ierīces, kuras minētas Regulas (ES) 2017/745 ([70]) 2. panta 1. punktā, un vienības, kas ražo *in vitro* diagnostikas medicīniskas ierīces, kuras minētas Regulas (ES) 2017/746 ([71]) 2. panta 2. punktā, izņemot vienības, kas ražo 1. pielikuma 5. punktā minētās medicīniskās ierīces.

68 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.).

69 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.).

70 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/EK un 93/42/EEK (OV L 117, 5.5.2017., 1. lpp.).

71 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.).

	b) Datoru, elektronisko un optisko iekārtu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. 26. nodaļas C sadaļā
	c) Elektrisko iekārtu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. 27. nodaļas C sadaļā
	d) Citur neklasificētu iekārtu, mehānismu un darba mašīnu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. 28. nodaļas C sadaļā
	e) Automobiļu, piekabju un puspiekabju ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. 29. nodaļas C sadaļā
	f) Citu transportlīdzekļu ražošana	Uzņēmumi, kas veic kādu no saimnieciskajām darbībām, kuras minētas *NACE* 2. red. 30. nodaļas C sadaļā
6. Digitālo pakalpojumu sniedzēji		– Tiešsaistes tirdzniecības vietu nodrošinātāji
		– Tiešsaistes meklētājprogrammu nodrošinātāji
		– Sociālās tīklošanās pakalpojumu platformu nodrošinātāji