Eiropas Parlaments
2019-2024

Pilsoņu brīvību, tieslietu un iekšlietu komiteja

2020/0359(COD)

15.10.2021

ATZINUMS

Sniegusi Pilsoņu brīvību, tieslietu un iekšlietu komiteja

Rūpniecības, pētniecības un enerģētikas komitejai

par priekšlikumu Eiropas Parlamenta un Padomes direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Atzinuma sagatavotājs (*): *Lukas Mandl*

(*) Iesaistītā komiteja — Reglamenta 57. pants

PA_Legam

ĪSS PAMATOJUMS

Priekšlikums Eiropas Parlamenta un Padomes direktīvai par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā, ar ko atceļ Direktīvu (ES) 2016/1148 (*NIS2* direktīva)[1], ir daļa no plašāka iniciatīvu kopuma Savienības līmenī, kuru mērķis ir palielināt publisko un privāto struktūru noturību pret apdraudējumiem. Priekšlikuma mērķis ir novērst nepilnības spēkā esošajos tiesību aktos un ļaut struktūrām, uz kurām attiecas tā darbības joma, labāk reaģēt uz jaunajām problēmām, kuras Komisija konstatējusi savā ietekmes novērtējumā, kas ietvēra plašu apspriešanos ar ieinteresētajām personām. Šīs problēmas jo īpaši ietver arvien lielāku iekšējā tirgus digitalizāciju un mainīgo drošības apdraudējumu ainu.

Priekšlikuma juridiskais pamats ir LESD 114. pants, t.i., iekšējais tirgus. Tomēr no LIBE viedokļa ir svarīgi uzsvērt, ka pasākumi, kas tīklu un informācijas sistēmām noteikti ar *NIS2* direktīvu, ne tikai kalpo iekšējā tirgus pienācīgas darbības nodrošināšanai. **Direktīvai būtu arī jāpalīdz veicināt Savienības drošību kopumā**, cita starpā izvairoties no dalībvalstu atšķirīgās neaizsargātības pret kiberdrošības riskiem.

Šajā nolūkā ir būtiski **novērst pastāvošās atšķirības starp dalībvalstīm**, kas izriet no dalībvalstu atšķirīgām tiesību aktu interpretācijām. Šā iemesla dēļ referents atzinīgi vērtē ar regulu ieviesto vienoto nosacījumu, lai noteiktu struktūras, uz kurām attiecas direktīvas darbības joma. Ir sagatavoti papildu ierosinājumi, lai novērstu atšķirības īstenošanā, jo īpaši, lai liktu Komisijai pieņemt pamatnostādnes par *lex specialis* īstenošanu un MVU piemērojamos kritērijus (kuriem būtu arī jānodrošina juridiskā skaidrība un jāizvairās no nevajadzīga sloga), un pieprasīt Sadarbības grupai sīkāk precizēt netehniskos faktorus, kas jāņem vērā piegādes ķēdes riska novērtējumos. Turklāt tiek uzsvērts, ka sadarbībai starp kompetentajām iestādēm ir jānotiek gan dalībvalstu iekšienē, gan *starp* tām reāllaikā.

Ziņojuma projektā ir ņemti vērā arī vairāki **ieteikumi, ko EDAU sniedzis** savā atzinumā par kiberdrošības stratēģiju un *NIS* 2.0 direktīvu[2]. Vissvarīgākais ir tas, ka gan apsvērumos, gan teksta rezolutīvajā daļā ir precizēts, ka jebkāda personas datu apstrāde saskaņā ar *NIS2* direktīvu neskar Regulu (ES) 2016/679 (VDAR)[3] un Direktīvu 2002/58/EK[4] (e-privātums). Ņemot vērā jēdziena „tīklu un informācijas sistēmu drošība" šaurāko darbības jomu (attiecas tikai uz tehnoloģiju aizsardzību) salīdzinājumā ar „kiberdrošību" (attiecas arī uz darbībām lietotāju aizsardzībai), iepriekšējo terminu lieto tikai tad, ja konteksts ir tīri tehnisks. Attiecībā uz domēnu nosaukumiem un reģistrācijas datiem ir ierosināti precizējumi attiecībā uz 1) juridisko pamatu „attiecīgās informācijas" publicēšanai identifikācijas un saziņas nolūkos, 2) to datu jomas reģistrācijas datu kategorijām, uz kuriem attiecas publicēšana (pamatojoties

[1] 2020/0359(COD).

[2] Atzinums Nr. 5/2021: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.

[3] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 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) (Dokuments attiecas uz EEZ), *OV L 119, 4.5.2016., 1.–88. lpp.*

[4] Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK 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.–47. lpp*.).

uz *ICANN* ieteikumu), un 3) struktūrām, kas varētu būt „likumīgi piekļuves meklētāji". Juridiskajā tekstā ir arī precizēts, ka priekšlikums neietekmē jurisdikcijas noteikšanu un datu aizsardzības uzraudzības iestāžu kompetences saskaņā ar VDAR. Visbeidzot, ir nodrošināts plašāks juridiskais pamats attiecīgās informācijas sadarbībai un apmaiņai starp kompetentajām iestādēm saskaņā ar priekšlikumu un citām attiecīgajām uzraudzības iestādēm, jo īpaši uzraudzības iestādēm saskaņā ar VDAR.

Citas izmaiņas, ko Komisijas priekšlikumā ieviesa LIBE komitejas referents, ir šādas:

- Lai nodrošinātu saskaņotību starp *NIS2* direktīvu un ierosināto direktīvu par kritisko vienību noturību (*ECI*)[5], dažu noteikumu formulējums tika saskaņots ar *ECI* priekšlikuma formulējumu. Saskaņā ar līdzīgām izmaiņām, kas paredzētas *ECI* direktīvai, kurai būtu jāaptver tās pašas nozares, uz kurām attiecas *NIS2* direktīva, ir ierosināts darbības jomā iekļaut „pārtikas ražošanu, pārstrādi un izplatīšanu".
- Attiecībā uz personas datiem ir precizēts, ka *CSIRT* veiktai tīklu un informācijas sistēmu skenēšanai būtu jāatbilst ne tikai Regulai (ES) 2016/679 (VDAR)[6], bet arī Direktīvai 2002/58/EK[7] (e-privātums). Personas datu starptautiskai nosūtīšanai saskaņā ar šo direktīvu būtu jāatbilst VDAR V nodaļai.
- Sadarbības grupai būtu jātiekas divas reizes, nevis reizi gadā, lai izvērtētu aktuālākās norises kiberdrošības jomā. Sadarbības grupas darbībās kā novērotājam būtu jāpiedalās EDAK.
- *ENISA* būtu jāpublisko gada ziņojums, nevis divgadu ziņojums par situāciju kiberdrošības jomā Savienībā. Ziņojumā būtu jāņem vērā arī kiberdrošības incidentu ietekme uz personas datu aizsardzību Savienībā.
- Incidentu paziņošanas termiņš ir saskaņots ar VDAR noteikto termiņu ziņošanai par pārkāpumiem, proti, 72 stundas.
- Lai gan būtisku un svarīgu struktūru ziņošanai par faktiskajiem kiberdrošības incidentiem patiešām vajadzētu būt obligātai, paziņošanai par kiberdraudiem vajadzētu būt brīvprātīgai, lai ierobežotu administratīvo slogu un izvairītos no pārmērīgas ziņošanas. Lai incidentu uzskatītu par būtisku, tam būtu bijis jārada faktisks kaitējums un jāietekmē citas fiziskas un juridiskas personas – nepietiek ar tādu kaitējumu vai sekām, kas ir „iespējamas".
- Apstākļi, kas jāņem vērā, lemjot par sankcijām pēc kiberdrošības noteikumu pārkāpuma, ir saskaņoti ar VDAR. Tā kā tas būtu pretrunā pašreizējai atbildības praksei Savienības tiesību aktos, nevajadzētu būt iespējai uz laiku aizliegt fiziskām personām veikt vadības funkcijas.
- Lai novērstu kaitējumu reputācijai, subjektiem nevajadzētu būt pienākumam publiskot tos aspektus, kas saistīti ar neatbilstību šīs direktīvas prasībām vai to fizisko vai juridisko personu identitāti, kuras ir atbildīgas par pārkāpumu.

[5] 2020/0365(COD).

[6] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 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) (Dokuments attiecas uz EEZ), *OV L 119, 4.5.2016., 1.–88. lpp.*

[7] Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK 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.–47. lpp*.).

GROZĪJUMI

Pilsoņu brīvību, tieslietu un iekšlietu komiteja aicina par jautājumu atbildīgo Rūpniecības, pētniecības un enerģētikas komiteju ņemt vērā šādus grozījumus:

Grozījums Nr. 1

Direktīvas priekšlikums
1. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(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 ***drošībā un tās*** ekonomikas un sabiedrības efektīvā darbībā.
[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.).	[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.).

Grozījums Nr. 2

Direktīvas priekšlikums
2. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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	(2) Kopš Direktīvas (ES) 2016/1148 stāšanās spēkā ir panākts ievērojams progress Savienības kiberdrošības noturības līmeņa paaugstināšanā. Minētās direktīvas pārskatīšana apliecināja, ka direktīva ir bijusi kā katalizators

institucionālajai un regulatīvajai pieejai attiecībā uz kiberdrošību Savienībā, bruģējot ceļu būtiskām pārmaiņām domāšanas veidā. Direktīva ir nodrošinājusi valstu regulējumu pabeigšanu, nosakot valsts kiberdrošības stratēģijas, veidojot valstu spējas un īstenojot regulatīvus pasākumus, kas aptver būtiskas infrastruktūras un dalībniekus, kurus noteikusi katra dalībvalsts. Tā ir arī veicinājusi sadarbību Savienības līmenī, izveidojot sadarbības 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.	institucionālajai un regulatīvajai pieejai attiecībā uz kiberdrošību Savienībā, bruģējot ceļu būtiskām pārmaiņām domāšanas veidā. Direktīva ir nodrošinājusi valstu regulējumu pabeigšanu, nosakot valsts kiberdrošības stratēģijas, veidojot valstu spējas un īstenojot regulatīvus pasākumus, kas aptver būtiskas infrastruktūras un dalībniekus, kurus noteikusi katra dalībvalsts. Tā ir arī veicinājusi sadarbību Savienības līmenī, izveidojot sadarbības grupu un valstu datordrošības incidentu reaģēšanas vienību tīklu ("CSIRT tīkls"). Neraugoties uz šiem sasniegumiem, Direktīvas (ES) 2016/1148 pārskatīšanā ir konstatētas nepilnības, kas liedz tai efektīvi risināt pašreizējās un jaunās kiberdrošības problēmas. ***Turklāt tiešsaistes darbību paplašināšanās saistībā ar Covid-19 pandēmiju ir uzskatāmi parādījusi kiberdrošības nozīmi, kas ir būtiska, lai ES iedzīvotāji varētu uzticēties inovācijai un savienojamībai, kā arī plaša mēroga izglītībai un apmācībai šajā jomā. Tāpēc Komisijai būtu jāatbalsta dalībvalstis kiberdrošības izglītības programmu izstrādē, lai ļautu svarīgām un nozīmīgām vienībām pieņemt darbā kiberdrošības ekspertus, kas ļautu tām izpildīt no šīs direktīvas izrietošos pienākumus.***
[12] Direktīvas (ES) 2016/1148 11. pants.	[12] Direktīvas (ES) 2016/1148 11. pants.
[13] Direktīvas (ES) 2016/1148 12. pants.	[13] Direktīvas (ES) 2016/1148 12. pants.

Grozījums Nr. 3

Direktīvas priekšlikums
3. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(3) Tīklu un informācijas sistēmas ir kļuvušas par būtisku ikdienas dzīves iezīmi, ko raksturo ātra digitālā pārveide un sabiedrības savstarpējā savienotība, tai	(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***.

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***, mūsu demokrātijas darbībai, mūsu vērtībām un brīvībām, kas ir visas mūsu sabiedrības pamatā***. Tāpēc sagatavotība kiberdrošības jomā un ***šīs jomas*** efektivitāte tagad ***Savienības drošībai un*** iekšējā tirgus ***pareizai*** darbībai ir ***svarīgāka*** nekā jebkad ***agrāk, ņemot vērā visā Savienībā notiekošo ikdienas darbību digitalizāciju. Tādēļ ir nepieciešama ciešāka sadarbība starp iestādēm gan valstu iekšienē, gan dalībvalstu starpā, kā arī starp valstu iestādēm un atbildīgajām Savienības struktūrām.***

Grozījums Nr. 4

Direktīvas priekšlikums
5. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(5) Visas šīs atšķirības sadrumstalo iekšējo tirgu un tām var būt prejudiciāla ietekme uz tā darbību, jo īpaši ietekmējot pakalpojumu pārrobežu sniegšanu un kiberdrošības noturības līmeni, jo tiek piemēroti atšķirīgi standarti. Šīs direktīvas mērķis ir novērst šādas plašas atšķirības starp dalībvalstīm, jo īpaši izklāstot minimālos noteikumus attiecībā uz koordinēta tiesiskā regulējuma darbību, nosakot mehānismus efektīvai atbildīgo iestāžu sadarbībai katrā dalībvalstī, atjauninot to nozaru un darbību sarakstu,	(5) Visas šīs atšķirības sadrumstalo iekšējo tirgu un tām var būt prejudiciāla ietekme uz tā darbību, jo īpaši ietekmējot pakalpojumu pārrobežu sniegšanu un kiberdrošības noturības līmeni, jo tiek piemēroti atšķirīgi standarti. ***Galu galā šīs atšķirības var palielināt dažu dalībvalstu neaizsargātību pret kiberdrošības apdraudējumiem, radot iespējamu plašāku ietekmi visā Savienībā, gan attiecībā uz iekšējo tirgu, gan uz tā drošību kopumā.*** Šīs direktīvas mērķis ir novērst šādas plašas atšķirības starp

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.

dalībvalstīm, jo īpaši izklāstot minimālos noteikumus attiecībā uz koordinēta tiesiskā regulējuma darbību, nosakot mehānismus efektīvai atbildīgo iestāžu sadarbībai ***reāllaikā*** katrā dalībvalstī ***un starp dalībvalstu kompetentajām iestādēm***, 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.

Grozījums Nr. 5

Direktīvas priekšlikums
6. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(6) Šī direktīva neietekmē dalībvalstu spēju veikt nepieciešamos pasākumus, lai nodrošinātu savu būtisko drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrisko drošību un lai ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem atbilstoši Savienības tiesību aktiem. Saskaņā ar LESD 346. pantu dalībvalstīm nav jāsniedz informācija, kuras izpaušana būtu pretrunā to būtiskajām sabiedriskās drošības interesēm. Šajā kontekstā svarīgi ir valstu un Savienības noteikumi par klasificētas informācijas aizsardzību, vienošanās par neizpaušanu un neformālas vienošanās par informācijas neizpaušanu, piemēram, Gaismas signālu protokols[14].	(6) Šī direktīva neietekmē dalībvalstu spēju veikt nepieciešamos pasākumus, lai nodrošinātu savu būtisko ***nacionālo*** drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrisko drošību un lai ļautu ***novērst,*** izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem atbilstoši Savienības tiesību aktiem. Saskaņā ar LESD 346. pantu dalībvalstīm nav jāsniedz informācija, kuras izpaušana būtu pretrunā to būtiskajām sabiedriskās drošības interesēm. Šajā kontekstā svarīgi ir valstu un Savienības noteikumi par klasificētas informācijas aizsardzību, vienošanās par neizpaušanu un neformālas vienošanās par informācijas neizpaušanu, piemēram, Gaismas signālu protokols[14].
[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).	[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).

Grozījums Nr. 6

Direktīvas priekšlikums
8. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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. Dalībvalstīm nebūtu jānosaka prasība izveidot to vienību sarakstu, kuras atbilst šim vispārpiemērojamam ar lielumu saistītajam kritērijam.	(8) ***Dalībvalstu atbildība saskaņā*** ar Direktīvu (ES) 2016/1148***,*** dalībvalstīm bija pienākums noteikt, kuras vienības atbilst kritērijiem, lai tās uzskatītu par pamatpakalpojumu sniedzējiem ("identifikācijas process")***, un tas noveda pie lielām atšķirībām*** starp dalībvalstīm ***šajā sakarībā. Neskarot šajā direktīvā paredzētos īpašos izņēmumus***, būtu jāievieš vienots kritērijs to vienību noteikšanai, kuras ir šīs direktīvas piemērošanas jomā***, lai novērstu šīs atšķirības, kā arī nodrošinātu juridisko noteiktību attiecībā uz riska pārvaldības prasībām un visu attiecīgo vienību ziņošanas pienākumiem***. 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. Dalībvalstīm nebūtu jānosaka prasība izveidot to vienību sarakstu, kuras atbilst šim vispārpiemērojamam ar lielumu saistītajam kritērijam.
[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.).	[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.).

Grozījums Nr. 7

Direktīvas priekšlikums
8.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(8a) Ņemot vērā atšķirības valstu publiskās pārvaldes sistēmās, dalībvalstis saglabā savas lēmumu pieņemšanas spējas attiecībā uz to vienību izraudzīšanu, uz kurām attiecas šī direktīva.

Grozījums Nr. 8

Direktīvas priekšlikums
9. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(9) ***Tomēr šī*** direktīva būtu jāattiecina arī uz mazām vienībām vai mikrovienībām, kas atbilst noteiktiem kritērijiem, kuri norāda uz būtisku lomu dalībvalstu tautsaimniecībā vai sabiedrībā vai konkrētās nozarēs vai pakalpojumu veidos. Dalībvalstīm vajadzētu būt atbildīgām par šādu vienību saraksta izveidi un būtu jāiesniedz saraksts Komisijai.	(9) ***Šī*** direktīva būtu jāattiecina arī uz mazām vienībām vai mikrovienībām, kas atbilst noteiktiem kritērijiem, kuri norāda uz būtisku lomu dalībvalstu tautsaimniecībā vai sabiedrībā vai konkrētās nozarēs vai pakalpojumu veidos***, balstoties uz riska novērtējumu, tostarp vienībām, kas noteiktas kā kritiskas vienības, vai vienībām, kas ir līdzvērtīgas kritiskām vienībām saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) XXX/XXX[1a]***. Dalībvalstīm vajadzētu būt atbildīgām par šādu vienību saraksta izveidi un būtu jāiesniedz saraksts Komisijai. _____ ***[1a] Eiropas Parlamenta un Padomes XXXX. gada XX. xxxx direktīva (ES) [XXX/XXX] par kritisko vienību noturību (OV ...).***

Grozījums Nr. 9

Direktīvas priekšlikums
10. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(10) ***Komisija*** kopā ar sadarbības grupu	(10) ***Komisijai*** kopā ar sadarbības grupu

var izdot pamatnostādnes par ***mikrouzņēmumiem*** un ***mazajiem uzņēmumiem*** piemērojamo kritēriju īstenošanu.

būtu jāizdod pamatnostādnes par ***mikrovienībām*** un ***mazajām vienībām*** piemērojamo kritēriju īstenošanu.

Grozījums Nr. 10

Direktīvas priekšlikums
12. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(12) Īpaši nozaru tiesību akti un instrumenti var palīdzēt nodrošināt augstu kiberdrošības līmeni, vienlaikus pilnībā ņemot vērā šo nozaru specifiku un sarežģītību. Ja saskaņā ar konkrētas nozares Savienības tiesību aktu būtiskajām vai svarīgajām vienībām ir jāpieņem kiberdrošības riska pārvaldības pasākumi vai jāpaziņo incidenti vai nozīmīgi kiberdraudi, kam ir vismaz līdzvērtīga ietekme uz šajā direktīvā noteiktajiem pienākumiem, būtu jāpiemēro minētie īpašie nozaru noteikumi, tai skaitā par uzraudzību un izpildi. ***Komisija var izdot*** pamatnostādnes par lex specialis īstenošanu. Šī direktīva neliedz pieņemt konkrētu nozaru Savienības papildu aktus, kuros pievēršas kiberdrošības riska pārvaldības pasākumiem un incidentu paziņojumiem. Šī direktīva neskar esošās īstenošanas pilnvaras, kas piešķirtas Komisijai vairākās nozarēs, tai skaitā transporta un enerģētikas nozarē.	(12) Īpaši nozaru tiesību akti un instrumenti var palīdzēt nodrošināt augstu kiberdrošības līmeni, vienlaikus pilnībā ņemot vērā šo nozaru specifiku un sarežģītību. Ja saskaņā ar konkrētas nozares Savienības tiesību aktu būtiskajām vai svarīgajām vienībām ir jāpieņem kiberdrošības riska pārvaldības pasākumi vai jāpaziņo incidenti vai nozīmīgi kiberdraudi, kam ir vismaz līdzvērtīga ietekme uz šajā direktīvā noteiktajiem pienākumiem, būtu jāpiemēro minētie īpašie nozaru noteikumi, tai skaitā par uzraudzību un izpildi. ***Komisijai būtu jāizdod*** pamatnostādnes par lex specialis īstenošanu. Šī direktīva neliedz pieņemt konkrētu nozaru Savienības papildu aktus, kuros pievēršas kiberdrošības riska pārvaldības pasākumiem un incidentu paziņojumiem. Šī direktīva neskar esošās īstenošanas pilnvaras, kas piešķirtas Komisijai vairākās nozarēs, tai skaitā transporta un enerģētikas nozarē.

Grozījums Nr. 11

Direktīvas priekšlikums
14. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(14) Ņemot vērā saikni starp kiberdrošību un vienību fizisko drošību, Eiropas Parlamenta un Padomes Direktīvā (ES) XXX/XXX[17] un šajā	(14) Ņemot vērā saikni starp kiberdrošību un vienību fizisko drošību, Eiropas Parlamenta un Padomes Direktīvā (ES) XXX/XXX[17] un šajā

direktīvā būtu jānodrošina saskaņota pieeja. Lai to panāktu, dalībvalstīm būtu jānodrošina, ka kritiskās vienības un tām līdzvērtīgas vienības atbilstoši Direktīvai (ES) XXX/XXX tiek uzskatītas par būtiskām vienībām atbilstoši šai direktīvai. Dalībvalstīm būtu arī jānodrošina, ka to 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. Iestādēm būtu jāsadarbojas un jāapmainās ar informāciju atbilstoši abām direktīvām, jo īpaši ***saistībā ar*** kritisko vienību noteikšanu, kiberdraudiem, kiberdrošības riskiem, incidentiem, kas ietekmē kritiskās vienības, kā arī kiberdrošības pasākumiem, ko veikušas ***kritiskās vienības***. Ja to pieprasa kompetentās iestādes atbilstoši Direktīvai (ES) XXX/XXX, kompetentajām iestādēm atbilstoši šai direktīvai vajadzētu būt iespējām ***īstenot savas uzraudzības un izpildes pilnvaras attiecībā uz būtisku vienību***, kas identificēta kā kritiska. Abu veidu iestādēm šajā nolūkā būtu jāsadarbojas un jāapmainās ar informāciju.	direktīvā būtu jānodrošina saskaņota pieeja***, kad vien iespējams un lietderīgi***. Lai to panāktu, dalībvalstīm būtu jānodrošina, ka kritiskās vienības un tām līdzvērtīgas vienības atbilstoši Direktīvai (ES) XXX/XXX tiek uzskatītas par būtiskām vienībām atbilstoši šai direktīvai. Dalībvalstīm būtu arī jānodrošina, ka to kiberdrošības stratēģijās ir paredzēts politikas satvars uzlabotai koordinācijai starp ***kompetentajām iestādēm kādā no dalībvalstīm vai starp tām*** atbilstoši šai direktīvai un kompetento iestādi atbilstoši Direktīvai (ES) XXX/XXX saistībā ar informācijas apmaiņu par ***kiberincidentiem*** un kiberdraudiem un uzraudzības uzdevumu īstenošanu. Iestādēm ***dalībvalstīs un starp dalībvalstīm*** būtu jāsadarbojas un jāapmainās ar informāciju atbilstoši abām direktīvām, jo īpaši ***attiecībā uz*** kritisko vienību noteikšanu, kiberdraudiem, kiberdrošības riskiem, incidentiem, kas ietekmē kritiskās vienības, kā arī kiberdrošības pasākumiem, ko veikušas ***šajā direktīvā minētās kompetentās iestādes un kas ir nozīmīgi kritiskām vienībām***. Ja to pieprasa kompetentās iestādes atbilstoši Direktīvai (ES) XXX/XXX, kompetentajām iestādēm atbilstoši šai direktīvai vajadzētu būt iespējām ***novērtēt tādas būtiskas vienības kiberdrošību***, kas identificēta kā kritiska. Abu veidu iestādēm šajā nolūkā būtu jāsadarbojas un jāapmainās ar informāciju ***reāllaikā***.
[17] [ierakstīt pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]	[17] [ierakstīt pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

Grozījums Nr. 12

Direktīvas priekšlikums
18. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(18) Pakalpojumus, ko piedāvā datu centru pakalpojumu sniedzēji, ne vienmēr var sniegt mākoņpakalpojuma 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 mākoņpakalpojumi. 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.	(18) Pakalpojumus, ko piedāvā datu centru pakalpojumu sniedzēji, ne vienmēr var sniegt mākoņpakalpojuma veidā. Tas nozīmē, ka datu centri var nebūt daļa no mākoņdatošanas infrastruktūras. Lai pārvaldītu visus riskus ***kiberdrošībai***, šī direktīva būtu jāattiecina arī uz tādu datu centru pakalpojumu sniedzējiem, kuri nav mākoņpakalpojumi. Šajā direktīvā termins "datu centra pakalpojums" būtu jāattiecina uz tāda pakalpojuma sniegšanu, kas ietver struktūras vai struktūru grupas, kuras paredzētas tāda informācijas 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.

Grozījums Nr. 13

Direktīvas priekšlikums
20. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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	(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, ***pārtikas ražošana, pārstrāde un izplatīšana,*** veselība, konkrēti valsts pārvaldes aspekti, kā arī kosmoss, ciktāl tas attiecas uz tādu konkrētu pakalpojumu sniegšanu, kuri ir atkarīgi no virszemes infrastruktūrām, ko

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.	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 ***pandēmijas laikā notikušie intensīvie uzbrukumi informācijas sistēmām*** ir ***parādījuši*** mūsu arvien vairāk savstarpēji atkarīgās sabiedrības neaizsargātību, neraugoties uz zemas varbūtības riskiem. ***Tāpēc ir vajadzīgas papildu investīcijas kiberdrošības jomā.***

Grozījums Nr. 14

Direktīvas priekšlikums
20.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(20a) Ir būtiski palielināt informētību par kiberdrošību un kibernoturību visās kritiski svarīgās un nozīmīgās vienībās, tostarp valsts pārvaldes struktūrās.

Grozījums Nr. 15

Direktīvas priekšlikums
21. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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	(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.	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 ***un nodrošināt, ka tās rīcībā ir pietiekami resursi, lai efektīvi un produktīvi veiktu savus uzdevumus***.

Grozījums Nr. 16

Direktīvas priekšlikums
22. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(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 ***kiberdrošību*** un pārrobežu sadarbību Savienības līmenī.

Grozījums Nr. 17

Direktīvas priekšlikums
23. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(23) Kompetentajām iestādēm vai CSIRT būtu efektīvi un lietpratīgi jāsaņem paziņojumi par incidentiem no vienībām. Būtu jānosaka vienotajiem kontaktpunktiem pienākums pārsūtīt incidentu paziņojumus citu ***skarto*** dalībvalstu vienotajiem kontaktpunktiem. Dalībvalstu iestāžu līmenī, lai nodrošinātu vienu vienotu kontaktpunktu katrā dalībvalstī, vienotajiem kontaktpunktiem arī būtu jāsaņem attiecīgā informācija par incidentiem saistībā ar finanšu sektora vienībām no kompetentajām iestādēm atbilstoši Regulai XXXX/XXXX, un tiem būtu jāspēj šo informāciju attiecīgā	(23) Kompetentajām iestādēm vai CSIRT būtu efektīvi un lietpratīgi jāsaņem paziņojumi par incidentiem no vienībām. Būtu jānosaka vienotajiem kontaktpunktiem pienākums pārsūtīt incidentu paziņojumus ***reāllaikā visu*** citu dalībvalstu vienotajiem kontaktpunktiem. Dalībvalstu iestāžu līmenī, lai nodrošinātu vienu vienotu kontaktpunktu katrā dalībvalstī, vienotajiem kontaktpunktiem arī būtu jāsaņem attiecīgā informācija par incidentiem saistībā ar finanšu sektora vienībām no kompetentajām iestādēm atbilstoši Regulai XXXX/XXXX, un tiem būtu jāspēj šo informāciju attiecīgā

gadījumā pārsūtīt attiecīgajām valsts kompetentajām iestādēm vai CSIRT saskaņā ar šo regulu.	gadījumā pārsūtīt attiecīgajām valsts kompetentajām iestādēm vai CSIRT saskaņā ar šo regulu.

Grozījums Nr. 18

Direktīvas priekšlikums
25. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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. Dalībvalstīm būtu jāizvirza mērķis nodrošināt vienlīdzīgu tehnisko spēju līmeni visām nozaru CSIRT. Dalībvalstis var lūgt Eiropas Savienības Kiberdrošības aģentūras (ENISA) palīdzību valsts CSIRT attīstīšanā.	(25) Attiecībā uz persondatiem CSIRT saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679[19] ***un Direktīvu 2002/58/EK***, ja to pieprasa vienības atbilstoši šai direktīvai un to vārdā, būtu jāspēj nodrošināt to pakalpojumu sniegšanai ***informācijas sistēmu*** un ***izmantotā tīkla tvēruma drošības*** skenēšanu***, lai noteiktu, mazinātu vai novērstu konkrētus draudus***. Dalībvalstīm būtu jāizvirza mērķis nodrošināt vienlīdzīgu tehnisko spēju līmeni visām nozaru CSIRT. Dalībvalstis var lūgt Eiropas Savienības Kiberdrošības aģentūras (ENISA) palīdzību valsts CSIRT attīstīšanā. ***Turklāt kiberdrošības riskus nekad nevajadzētu izmantot kā aizbildinājumu pamattiesību pārkāpumiem.***
[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.).	[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.).

Grozījums Nr. 19

Direktīvas priekšlikums
27. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(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 ***vai rada nopietnus riskus sabiedrības drošībai dažās dalībvalstīs vai Savienībai kopumā***. Ņemot vērā šādu incidentu plašo tvērumu un to, ka vairākumā gadījumu tiem ir pārrobežu raksturs, dalībvalstīm un attiecīgajām Savienības iestādēm, struktūrām un aģentūrām būtu jāsadarbojas tehniskā, operatīvā un politiskā līmenī, lai pienācīgi koordinētu reaģēšanu visā Savienībā. ***Dalībvalstīm būtu jāuzrauga, kā tiek īstenoti ES noteikumi, jāsniedz savstarpējs atbalsts pārrobežu problēmu gadījumā, jāveido strukturētāks dialogs ar privāto sektoru un jāsadarbojas, lai novērstu drošības riskus un apdraudējumus, kas saistīti ar jaunajām tehnoloģijām, kā tas bija 5G tehnoloģijas gadījumā.***
[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.).	[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.).

Grozījums Nr. 20

Direktīvas priekšlikums
33. apsvērums

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

Grozījums Nr. 21

Direktīvas priekšlikums
34. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(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 ***jāpieaicina būtiskās*** Savienības struktūras un aģentūras, kas iesaistītas kiberdrošības politikā, ***jo īpaši Eiropols***, Eiropas Savienības Aviācijas drošības ***aģentūra*** (EASA) un Eiropas Savienības Kosmosa programmas ***aģentūra*** (EUSPA), lai tās piedalītos tās darbā.

Grozījums Nr. 22

Direktīvas priekšlikums
36. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(36) Attiecīgā gadījumā Savienībai saskaņā ar LESD 218. pantu būtu jānoslēdz starptautiski nolīgumi ar trešām valstīm vai starptautiskām organizācijām, ļaujot tām piedalīties un organizējot to dalību atsevišķās sadarbības grupas un CSIRT tīkla darbībās. ***Šādos nolīgumos*** būtu ***jānodrošina pienācīga datu aizsardzība***.	(36) Attiecīgā gadījumā Savienībai saskaņā ar LESD 218. pantu būtu jānoslēdz starptautiski nolīgumi ar trešām valstīm vai starptautiskām organizācijām, ļaujot tām piedalīties un organizējot to dalību atsevišķās sadarbības grupas un CSIRT tīkla darbībās. ***Ciktāl personas dati tiek nosūtīti trešai valstij vai starptautiskai organizācijai,*** būtu ***jāpiemēro Regulas (ES) 2016/679 V nodaļa***.

Grozījums Nr. 23

Direktīvas priekšlikums
37. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(37) Dalībvalstīm būtu jāsniedz ieguldījums Ieteikumā (ES) 2017/1584 noteiktā ES satvara reaģēšanai kiberdrošības krīzēs izveidošanā, izmantojot esošos sadarbības tīklus, jo īpaši Kiberkrīžu sadarbības organizāciju tīklu (EU-CyCLONe), CSIRT tīklu un sadarbības grupu. EU-CyCLONe un CSIRT tīklam būtu jāsadarbojas, pamatojoties uz procedūrām, kas nosaka šādas sadarbības procesuālo kārtību. EU-CyCLONe reglamentā būtu jāprecizē kārtība, kādā tīklam būtu jādarbojas, cita starpā paredzot uzdevumus, sadarbības veidus, mijiedarbību ar citiem attiecīgiem dalībniekiem un veidnes informācijas apmaiņai, kā arī saziņas līdzekļus. Attiecībā uz krīžu pārvaldību Savienības līmenī attiecīgajām pusēm būtu jāpaļaujas uz integrētajiem krīzes situāciju politiskās reaģēšanas (IPCR) mehānismiem. Šim nolūkam Komisijai būtu jāizmanto krīzes augstlīmeņa starpnozaru koordinācijas process ARGUS. Ja krīzei ir nozīmīgs ārējās politikas vai kopīgās drošības un aizsardzības politikas (KDAP) aspekts, būtu jāiedarbina Eiropas Ārējās darbības	(37) Dalībvalstīm būtu jāsniedz ieguldījums Ieteikumā (ES) 2017/1584 noteiktā ES satvara reaģēšanai kiberdrošības krīzēs izveidošanā, izmantojot esošos sadarbības tīklus, jo īpaši Kiberkrīžu sadarbības organizāciju tīklu (EU-CyCLONe), CSIRT tīklu un sadarbības grupu. EU-CyCLONe un CSIRT tīklam būtu jāsadarbojas, pamatojoties uz procedūrām, kas nosaka šādas sadarbības procesuālo kārtību. EU-CyCLONe reglamentā būtu jāprecizē kārtība, kādā tīklam būtu jādarbojas, cita starpā paredzot uzdevumus, sadarbības veidus, mijiedarbību ar citiem attiecīgiem dalībniekiem un veidnes informācijas apmaiņai, kā arī saziņas līdzekļus. Attiecībā uz krīžu pārvaldību Savienības līmenī attiecīgajām pusēm būtu jāpaļaujas uz integrētajiem krīzes situāciju politiskās reaģēšanas (IPCR) mehānismiem. Šim nolūkam Komisijai būtu jāizmanto krīzes augstlīmeņa starpnozaru koordinācijas process ARGUS. Ja ***krīze skar divas vai vairākas dalībvalstis un ir aizdomas, ka tai ir krimināltiesisks raksturs, būtu jāapsver iespēja aktivizēt ES***

dienesta (EĀDD) mehānisms reaģēšanai krīzes situācijās (CRM).	***Tiesībaizsardzības ārkārtas reaģēšanas protokolu. 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).

Grozījums Nr. 24

Direktīvas priekšlikums
45. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(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 ***un jāziņo par visiem iespējamajiem kiberuzbrukumiem, ko tās atklāj***.

Grozījums Nr. 25

Direktīvas priekšlikums
46.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(46a) Īpaša uzmanība būtu jāpievērš tam, ka IKT pakalpojumi, sistēmas vai produkti, uz kuriem izcelsmes valstī attiecas īpašas prasības, varētu būt

	šķērslis ES privātuma un datu aizsardzības tiesību aktu ievērošanai. Attiecīgā gadījumā šādu riska novērtēšanas ietvaros būtu jāapspriežas ar EDAK. Brīvā un atklātā pirmkoda programmatūra, kā arī atklātā pirmkoda aparatūra varētu sniegt milzīgus ieguvumus kiberdrošības jomā, jo īpaši attiecībā uz funkciju pārredzamību un pārbaudāmību. Tā kā tas varētu palīdzēt novērst un mazināt konkrētus riskus piegādes ķēdēs, to izmantošanai saskaņā ar EDAU atzinumu Nr. 5/2021[1a] būtu pēc iespējas jādod priekšroka.
	[1a] Eiropas Datu aizsardzības uzraudzītāja Atzinums Nr. 5/2021 par kiberdrošības stratēģiju un TID 2.0 direktīvu, 2021. gada 11. marts.

***Grozījums Nr.* 26**

Direktīvas priekšlikums
47. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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	(47) Piegādes ķēžu riska novērtējumos, ievērojot attiecīgās nozares iezīmes, būtu jāņem vērā gan tehniski, gan attiecīgā gadījumā netehniski faktori, ***kuri būtu jāprecizē koordinācijas grupai, un jāietver*** 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

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.	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.

Grozījums Nr. 27

Direktīvas priekšlikums
48.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(48a) Mazajiem un vidējiem uzņēmumiem (MVU) bieži vien trūkst mēroga un resursu, lai apmierinātu plašās un arvien pieaugošās kiberdrošības vajadzības savstarpēji tik saistītajā pasaulē, jo palielinās attālinātā darba apjoms. Tāpēc dalībvalstīm savās valsts kiberdrošības stratēģijās būtu jāparedz norādes un atbalsts MVU.

Grozījums Nr. 28

Direktīvas priekšlikums
50. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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	(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 būtu arī jānodrošina radītajam riskam ***atbilstīgs kiberdrošības*** 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

starppersonu sakaru pakalpojumiem, kuros izmanto numurus un kuros netiek īstenota faktiska kontrole pār signālu pārraidi.

pakalpojumiem, kuros izmanto numurus un kuros netiek īstenota faktiska kontrole pār signālu pārraidi.

Grozījums Nr. 29

Direktīvas priekšlikums
52. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(52) Attiecīgā gadījumā vienībām ***būtu jāinformē*** to pakalpojumu saņēmēji par īpašiem un nozīmīgiem draudiem un par pasākumiem, kurus tās var veikt, lai mazinātu izrietošo risku, kas tām rodas. Prasībai informēt lietotājus par šādiem apdraudējumiem nebūtu jāatbrīvo vienības no pienākuma par saviem līdzekļiem veikt atbilstīgus un steidzamus pasākumus, lai izlabotu vai likvidētu jebkurus kiberdraudus un atjaunotu normālu pakalpojuma drošības līmeni. Šāda informācija par drošības apdraudējumiem būtu jāsniedz saņēmējiem bez maksas.	(52) Attiecīgā gadījumā vienībām ***vajadzētu būt iespējai informēt*** to pakalpojumu saņēmēji par īpašiem un nozīmīgiem draudiem un par pasākumiem, kurus tās var veikt, lai mazinātu izrietošo risku, kas tām rodas. Prasībai informēt lietotājus par šādiem apdraudējumiem nebūtu jāatbrīvo vienības no pienākuma par saviem līdzekļiem veikt atbilstīgus un steidzamus pasākumus, lai izlabotu vai likvidētu jebkurus kiberdraudus un atjaunotu normālu pakalpojuma drošības līmeni. Šāda informācija par drošības apdraudējumiem būtu jāsniedz saņēmējiem bez maksas.

Grozījums Nr. 30

Direktīvas priekšlikums
53. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(53) Jo īpaši publisko elektronisko sakaru tīklu nodrošinātājiem vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem būtu ***jāīsteno integrēta drošība un drošība pēc noklusējuma un tiem vajadzētu būt iespējai informēt*** pakalpojumu ***saņēmējus*** par konkrētiem un nozīmīgiem kiberdraudiem un par pasākumiem, ko tie var veikt, lai aizsargātu to ***ierīču un*** sakaru drošību, izmantojot, piemēram, konkrētu veidu programmatūru vai šifrēšanas tehnoloģijas. ***Lai palielinātu aparatūras un programmatūras drošību, pakalpojumu sniedzēji būtu jāmudina***

	izmantot atklātā pirmkoda programmatūru, kā arī atklātā pirmkoda aparatūru.

Grozījums Nr. 31

Direktīvas priekšlikums
54. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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***.	(54) Lai garantētu elektronisko sakaru tīklu un pakalpojumu drošību, ***kā arī pamattiesību attiecībā uz datu aizsardzību un privātumu aizsardzību,*** 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 ***atbildību nodrošināt*** dalībvalstu būtisko drošības interešu un sabiedrības aizsardzību un ļautu ***novērst*** un atklāt noziedzīgus nodarījumus un sodīt par tiem atbilstoši Savienības ***un valsts*** tiesību aktiem. Risinājumos par likumīgu piekļuvi informācijai pilnīgi šifrētos sakaros būtu jāsaglabā šifrēšanas efektivitāte privātuma un sakaru drošības aizsardzībā***. Nekas šajā regulā nebūtu jāuzskata par mēģinājumu vājināt pilnīgu (end-to-end) šifrēšanu, izmantojot slepenpiekļuvi (backdoors) vai līdzīgus risinājumus, jo šifrēšanas nepilnības var izmantot ļaunprātīgos nolūkos. Jebkurš pasākums, kura mērķis ir vājināt šifrēšanu vai apiet tehnoloģijas arhitektūru, var nopietni apdraudēt ar to saistītās efektīvās aizsardzības spējas. Lai nodrošinātu šīs tehnoloģijas efektivitāti un tās plašāku izmantošanu, jebkādu neatļautu atšifrēšanu vai elektronisko sakaru uzraudzību drīkstētu veikt tikai tiesu iestādes. Ir svarīgi, lai dalībvalstis risinātu problēmas, ar kurām saskaras tiesu iestādes un neaizsargātības pētnieki.***

	Dažās dalībvalstīs vienības un fiziskas personas, kas pēta ievainojamību, ir pakļautas krimināltiesiskai atbildībai un civiltiesiskai atbildībai. Tādēļ dalībvalstis tiek mudinātas izdot pamatnostādnes par to, kā nesākt kriminālvajāšanu un nesaukt pie atbildības par pētījumiem informācijas drošības jomā.

Grozījums Nr. 32

Direktīvas priekšlikums
56. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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, dalībvalstīm būtu jāizveido vienots kontaktpunkts ***visiem paziņojumiem, kas jāsniedz*** saskaņā ar šo direktīvu un arī citiem Savienības tiesību aktiem, piemēram, Regulu (ES) 2016/679 un Direktīvu 2002/58/EK. ENISA kopā ar sadarbības grupu būtu jāizstrādā vienotas ziņojumu veidnes, pieņemot pamatnostādnes, ar kurām vienkāršo un racionalizē ziņojamo informāciju, ko pieprasa Savienības tiesību akti, un mazina slogus uzņēmumiem.	(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, dalībvalstīm būtu jāizveido vienots kontaktpunkts 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 ***un Eiropas Datu aizsardzības kolēģiju*** būtu jāizstrādā vienotas ziņojumu veidnes, pieņemot pamatnostādnes, ar kurām vienkāršo un racionalizē ziņojamo informāciju, ko pieprasa Savienības tiesību akti, un mazina slogus uzņēmumiem.

Grozījums Nr. 33

Direktīvas priekšlikums
57. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(57) Ja ir aizdomas, ka incidents ir	(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.	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 ***Eiropola Eiropas Kibernoziedzības apkarošanas centrs (***EC3***)*** un ENISA veicina koordināciju starp dažādu dalībvalstu kompetentajām iestādēm un tiesībaizsardzības iestādēm.

Grozījums Nr. 34

Direktīvas priekšlikums
58. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(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 ***Regulai (ES) 2016/679 un*** Direktīvai 2002/58/EK.

Grozījums Nr. 35

Direktīvas priekšlikums
59. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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	(59) Lai garantētu DNS drošību, stabilitāti un noturību, kas savukārt veicina vienādi augsta līmeņa kiberdrošību Savienībā, ir svarīgi uzturēt precīzas un pilnīgas domēna nosaukuma 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.

dati") datubāzes un nodrošināt likumīgu piekļuvi šādiem datiem. Ja tiek apstrādāti persondati, šādā apstrādē ievēro ***piemērojamos*** Savienības datu aizsardzības tiesību aktus.

Grozījums Nr. 36

Direktīvas priekšlikums
62. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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 ***leģitīmo piekļuves prasītāju*** pieprasījumiem izpaust ***domēnu nosaukumu*** reģistrācijas datus. ALD reģistriem un vienībām, kas tiem sniedz ***domēnu nosaukumu*** reģistrācijas pakalpojumus, būtu jānosaka politika un procedūras reģistrācijas datu, tai skaitā pakalpojumu līmeņa līgumu, publicēšanai un izpaušanai, lai izpildītu 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. Lai veicinātu saskaņotu praksi visā iekšējā tirgū, Komisija var	(62) ***Lai izpildītu juridisku pienākumu, kas noteikts Regulas (ES) 2016/679 6. panta 1. punkta c) apakšpunktā un 6. panta 3. punktā, ALD*** reģistriem un vienībām, kas tiem sniedz ***domēna nosaukuma*** reģistrācijas pakalpojumus, būtu jādara publiski pieejami ***konkrēti domēna nosaukuma*** reģistrācijas dati, ***kas norādīti dalībvalsts tiesību aktos, kuri uz tiem attiecas***, piemēram, ***domēna nosaukums un juridiskās personas nosaukums***. ALD reģistriem un vienībām, kas sniedz ***domēna nosaukuma*** reģistrācijas pakalpojumus saistībā ar ALD, būtu arī jānodrošina leģitīmiem piekļuves prasītājiem***, it īpaši šajā direktīvā norādītajām kompetentām iestādēm vai Regulā (ES) 2016/679 noradītajām uzraudzības iestādēm, atbilstīgi to pilnvarām*** likumīga piekļuve īpašiem ***domēna nosaukuma*** reģistrācijas datiem par fiziskām personām. Dalībvalstīm būtu jānodrošina, ka ALD reģistri un vienības, kas tiem sniedz ***domēna nosaukuma*** reģistrācijas pakalpojumus, bez ***liekas*** kavēšanās atbild uz ***likumīgiem un pienācīgi pamatotiem*** pieprasījumiem***, ko iesniegušas publiskās iestādes, tostarp šajā direktīvā norādītās kompetentās iestādes, kompetentās iestādes, kas saskaņā ar Savienības vai valsts tiesību aktiem ir atbildīgas par noziedzīgu nodarījumu novēršanu, izmeklēšanu vai kriminālvajāšanu, vai Regulā (ES) 2016/679 norādītās***

pieņemt pamatnostādnes par šādām procedūrām, neskarot Eiropas Datu aizsardzības kolēģijas kompetences.

uzraudzības iestādes, izpaust ***domēna nosaukuma*** reģistrācijas datus. ALD reģistriem un vienībām, kas tiem sniedz ***domēna nosaukuma*** 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. Lai veicinātu saskaņotu praksi visā iekšējā tirgū, Komisija var pieņemt pamatnostādnes par šādām procedūrām, neskarot Eiropas Datu aizsardzības kolēģijas kompetences.

_____

_____

[25] EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/679 14. apsvērums: "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".

Grozījums Nr. 37

Direktīvas priekšlikums
63. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(63) ***Visām*** būtiskajām un svarīgajām vienībām atbilstoši šai direktīvai vajadzētu būt tās dalībvalsts jurisdikcijā, kurā tās sniedz pakalpojumus. Ja vienība sniedz pakalpojumus vairāk nekā vienā dalībvalstī, tai vajadzētu būt katras attiecīgās dalībvalsts atsevišķā un vienlaicīgā jurisdikcijā. Šo dalībvalstu kompetentajām iestādēm būtu jāsadarbojas, jāsniedz savstarpēja palīdzība un attiecīgā gadījumā jāveic kopīgas uzraudzības	(63) ***Šīs direktīvas mērķiem visām*** būtiskajām un svarīgajām vienībām atbilstoši šai direktīvai vajadzētu būt tās dalībvalsts jurisdikcijā, kurā tās sniedz pakalpojumus. Ja vienība sniedz pakalpojumus vairāk nekā vienā dalībvalstī, tai vajadzētu būt katras attiecīgās dalībvalsts atsevišķā un vienlaicīgā jurisdikcijā. Šo dalībvalstu kompetentajām iestādēm būtu ***jāvienojas par veidojošām klasifikācijām, pēc***

darbības.

iespējas jāsadarbojas, ***reāllaikā*** jāsniedz savstarpēja palīdzība un attiecīgā gadījumā jāveic kopīgas uzraudzības darbības.

Grozījums Nr. 38

Direktīvas priekšlikums
64. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(64) Lai ņemtu vērā DNS pakalpojumu sniedzēju, ALD nosaukumu reģistru, satura piegādes tīklu nodrošinātāju, mākoņpakalpojumu sniedzēju, datu centru pakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju pakalpojumu un darbību pārrobežu raksturu, tikai vienai dalībvalstij vajadzētu būt jurisdikcijai pār šīm vienībām. Jurisdikcija būtu jāpiedēvē tai dalībvalstij, kurā attiecīgajai vienībai ir tās galvenā darījumdarbības vieta Savienībā. Darījumdarbības 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 darījumdarbības vietu un tāpēc nav izšķirošs kritērijs galvenās darījumdarbības vietas noteikšanai. Par galveno darījumdarbības vietu būtu jāuzskata vieta, kur Savienībā tiek pieņemti ar kiberdrošības riska pārvaldības pasākumiem saistīti lēmumi. Parasti tā ir vieta, kur atrodas uzņēmumu centrālā administrācija Savienībā. Ja šādus lēmumus nepieņem Savienībā, būtu jāuzskata, ka galvenā darījumdarbības vieta ir dalībvalstīs, kurās vienībai ir darījumdarbības vieta ar vislielāko darbinieku skaitu Savienībā. Ja	(64) Lai ņemtu vērā DNS pakalpojumu sniedzēju, ALD nosaukumu reģistru, satura piegādes tīklu nodrošinātāju, mākoņpakalpojumu sniedzēju, datu centru pakalpojumu sniedzēju un digitālo pakalpojumu sniedzēju pakalpojumu un darbību pārrobežu raksturu, tikai vienai dalībvalstij vajadzētu būt jurisdikcijai pār šīm vienībām. ***Šīs direktīvas mērķiem*** jurisdikcija būtu jāpiedēvē tai dalībvalstij, kurā attiecīgajai vienībai ir tās galvenā darījumdarbības vieta Savienībā. Darījumdarbības 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 darījumdarbības vietu un tāpēc nav izšķirošs kritērijs galvenās darījumdarbības vietas noteikšanai. Par galveno darījumdarbības vietu būtu jāuzskata vieta, kur Savienībā tiek pieņemti ar kiberdrošības riska pārvaldības pasākumiem saistīti lēmumi. Parasti tā ir vieta, kur atrodas uzņēmumu centrālā administrācija Savienībā. Ja šādus lēmumus nepieņem Savienībā, būtu jāuzskata, ka galvenā darījumdarbības vieta ir dalībvalstīs, kurās vienībai ir darījumdarbības vieta ar vislielāko

pakalpojumus sniedz uzņēmumu grupa, par uzņēmumu grupas galveno uzņēmējdarbības vietu būtu jāuzskata kontrolējošā uzņēmuma galvenā darījumdarbības vieta.

darbinieku skaitu Savienībā. Ja pakalpojumus sniedz uzņēmumu grupa, par uzņēmumu grupas galveno uzņēmējdarbības vietu būtu jāuzskata kontrolējošā uzņēmuma galvenā darījumdarbības vieta.

Grozījums Nr. 39

Direktīvas priekšlikums
69. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(69) Persondatu ***apstrādei***, ciktāl tā ir stingri nepieciešama un samērīga, lai vienības, publiskās iestādes, *CERT*, *CSIRT* un drošības tehnoloģiju nodrošinātāji un pakalpojumu sniedzēji nodrošinātu tīklu un informācijas drošību, būtu jānotiek attiecīgā datu pārziņa leģitīmajās interesēs, kā minēts Regulā (ES) 2016/679. Tajā būtu jāietver pasākumi, kas saistīti ar incidentu novēršanu, atklāšanu, analīzi un reaģēšanu uz tiem, pasākumi, kas veicina informētību par īpašiem kiberdraudiem, informācijas apmaiņu neaizsargātības izlabošanas un koordinētas atklāšanas kontekstā, brīvprātīgu informācijas apmaiņu par minētajiem incidentiem, kā arī kiberdraudiem un neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem. Šādiem pasākumiem var būt vajadzīga ***šādu veidu*** persondatu apstrāde***:*** IP adreses, vienotie resursu vietrāži (URL), domēnu nosaukumi un e-pasta adreses.	(69) Persondatu ***apstrāde***, ciktāl tā ir stingri nepieciešama un samērīga, lai vienības, publiskās iestādes, *CERT*, *CSIRT* un drošības tehnoloģiju nodrošinātāji un pakalpojumu sniedzēji nodrošinātu tīklu un informācijas drošību, ***ir vajadzīga vienību atbilstībai to juridiskajām saistībām atbilstoši valsts tiesību aktiem, ar kuru transponē šo direktīvu, un tādēļ šādu datu apstrādi reglamentē Regulas (ES) 2016/679 6. panta 1. punkta c) apakšpunkts un 6. panta 3. punkts. Turklāt šādai apstrādei*** būtu jānotiek attiecīgā datu pārziņa leģitīmajās interesēs, kā minēts ***6. panta 1. punkta f) apakšpunktā*** Regulā (ES) 2016/679. Tajā būtu jāietver pasākumi, kas saistīti ar incidentu novēršanu, atklāšanu, analīzi un reaģēšanu uz tiem, pasākumi, kas veicina informētību par īpašiem kiberdraudiem, informācijas apmaiņu neaizsargātības izlabošanas un koordinētas atklāšanas kontekstā, brīvprātīgu informācijas apmaiņu par minētajiem incidentiem, kā arī kiberdraudiem un neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem. ***Daudzos gadījumos personas dati pēc kiberincidenta ir apdraudēti, tāpēc ES dalībvalstu kompetentajām iestādēm un datu aizsardzības iestādēm būtu jāsadarbojas un jāapmainās ar informāciju par visiem***

	būtiskajiem jautājumiem, lai vērstos pret jebkādiem personas datu aizsardzības pārkāpumiem. Šādiem pasākumiem var būt vajadzīga ***dažu*** persondatu ***kategoriju*** apstrāde***, tostarp*** IP adreses, vienotie resursu vietrāži (URL), domēnu nosaukumi un e-pasta adreses.

Grozījums Nr. 40

Direktīvas priekšlikums
71. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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) 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 ***nopietnība*** un ilgums, faktiskais izraisītais kaitējums vai zaudējumi vai iespējamais kaitējums vai zaudējumi, kas būtu varējuši rasties***, jebkādi attiecīgi iepriekšēji pārkāpumi, veids, kādā pārkāpums kļuvis zināms kompetentajai iestādei***, 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. ***Piemēroto*** 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.

Grozījums Nr. 41

Direktīvas priekšlikums
74. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(74) Dalībvalstīm būtu jāspēj pieņemt noteikumus par krimināLsodiem, ko piemēro, ja tiek pārkāptas valsts tiesību normas, ar kurām transponē šo direktīvu. Tomēr krimināLsodu piemērošanai par šādu valsts tiesību normu pārkāpumiem un saistītu administratīvu sodu piemērošanai nebūtu jāizraisa ne bis in idem principa pārkāpšana, kā to interpretējusi Tiesa.	(74) Dalībvalstīm būtu jāspēj pieņemt noteikumus par krimināLsodiem, ko piemēro, ja tiek pārkāptas valsts tiesību normas, ar kurām transponē šo direktīvu. ***Minētajos krimināLsodos būtu jāparedz arī iespēja atņemt ienākumus, kas gūti šīs regulas pārkāpumu rezultātā.*** 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.

Grozījums Nr. 42

Direktīvas priekšlikums
76. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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	(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 ***daļu no*** visiem būtiskas vienības sniegtajiem pakalpojumiem. Ņemot vērā šādu sankciju ***nopietnību*** 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

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.

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.

Grozījums Nr. 43

Direktīvas priekšlikums
77. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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.	(77) Ar šo direktīvu būtu jānosaka noteikumi par sadarbību starp ***šajā direktīvā norādītajām kompetentajām*** iestādēm ***un Regulā*** (ES) 2016/679 ***norādītajām uzraudzības iestādēm***, lai vērstos pret pārkāpumiem, kas saistīti ar persondatiem.

Grozījums Nr. 44

Direktīvas priekšlikums
79. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(79) Būtu jāievieš salīdzinošās izvērtēšanas mehānisms, ļaujot dalībvalstu izraudzītajiem ekspertiem novērtēt kiberdrošības politikas īstenošanu, tai skaitā dalībvalstu spēju līmeni un pieejamos resursus.	(79) Būtu jāievieš salīdzinošās izvērtēšanas mehānisms, ļaujot dalībvalstu izraudzītajiem ekspertiem novērtēt kiberdrošības politikas īstenošanu, tai skaitā dalībvalstu spēju līmeni un pieejamos resursus. ***ES būtu jāveicina***

	koordinēta reaģēšana uz plaša mēroga kiberincidentiem un krīzēm un jāpiedāvā palīdzība, lai palīdzētu atgūties pēc šādiem kiberuzbrukumiem.

Grozījums Nr. 45

Direktīvas priekšlikums
82.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(82a) Šī direktīva neattiecas uz Savienības iestādēm, birojiem, struktūrām un aģentūrām. Tomēr saskaņā ar šo direktīvu Savienības struktūras varētu uzskatīt par būtiskām vai svarīgām vienībām. Lai panāktu vienādu aizsardzības līmeni, izmantojot konsekventus un viendabīgus noteikumus, Komisijai līdz 2022. gada 31. decembrim būtu jāpublicē priekšlikums tiesību aktam par Savienības iestāžu, biroju, struktūru un aģentūru iekļaušanu ES mēroga kiberdrošības satvarā.

Grozījums Nr. 46

Direktīvas priekšlikums
84. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(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,	(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 ***un pilnībā ievērojot spēkā esošos Savienības tiesību aktus, kas reglamentē šos jautājumus. Uz jebkādu***

	personas datu apstrādi saskaņā ar šo direktīvu attiecas Regula (ES) 2016/679 un Direktīva 2002/58/EK to attiecīgajā piemērošanas jomā, tostarp to uzraudzības iestāžu uzdevumi un pilnvaras, kuras ir kompetentas uzraudzīt atbilstību minētajiem juridiskajiem instrumentiem.

Grozījums Nr. 47

Direktīvas priekšlikums
2. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Šī direktīva ir piemērojama publiskām un privātām vienībām, kas minētas kā būtiskas vienības I pielikumā un kā svarīgas vienības II pielikumā. Šī direktīva nav piemērojama vienībām, kas kvalificējamas kā mikrouzņēmumi un mazie uzņēmumi Komisijas Ieteikuma 2003/361/EK[28] nozīmē.	1. Šī direktīva ir piemērojama publiskām un privātām vienībām, kas minētas kā būtiskas vienības I pielikumā un kā svarīgas vienības II pielikumā. Šī direktīva nav piemērojama vienībām, kas kvalificējamas kā mikrouzņēmumi un mazie uzņēmumi Komisijas Ieteikuma 2003/361/EK[28] nozīmē. ***Nav piemērojams Komisijas Ieteikuma 2003/361/EK pielikuma 3. panta 4. punkts.***
[28] Komisijas Ieteikums 2003/361/EK (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).	[28] Komisijas Ieteikums 2003/361/EK (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

Grozījums Nr. 48

Direktīvas priekšlikums
2. pants – 2. punkts – ievaddaļa

Komisijas ierosinātais teksts	*Grozījums*
2. Tomēr šī direktīva ir piemērojama arī I un II pielikumā minētajām vienībām neatkarīgi no to lieluma, ja:	2. Tomēr šī direktīva ir piemērojama arī I un II pielikumā minētajām vienībām neatkarīgi no to lieluma ***un pamatojoties uz riska novērtējumu saskaņā ar 18. pantu***, ja:

Grozījums Nr. 49

Direktīvas priekšlikums
2. pants – 2. punkts – c apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(c) vienība ir vienīgais pakalpojuma sniedzējs ***dalībvalstī***;	(c) vienība ir vienīgais pakalpojuma sniedzējs ***valsts vai reģionālā līmenī***;

Grozījums Nr. 50

Direktīvas priekšlikums
2. pants – 2. punkts – d apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(d) vienības sniegtā pakalpojuma ***iespējamam*** traucējumam var būt ietekme uz sabiedrības aizsardzību, sabiedrisko drošību un sabiedrības veselību;	(d) vienības sniegtā pakalpojuma traucējumam var būt ietekme uz sabiedrības aizsardzību, sabiedrisko drošību un sabiedrības veselību;

Grozījums Nr. 51

Direktīvas priekšlikums
2. pants – 2. punkts – e apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(e) vienības sniegtā pakalpojuma ***iespējams*** traucējums var izraisīt sistēmiskus riskus, jo īpaši nozarēm, kurās šādam traucējumam var būt pārrobežu ietekme;	(e) vienības sniegtā pakalpojuma traucējums var izraisīt sistēmiskus riskus, jo īpaši nozarēm, kurās šādam traucējumam var būt pārrobežu ietekme;

Grozījums Nr. 52

Direktīvas priekšlikums
2. pants – 4.a punkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	4.a Jebkāda personas datu apstrāde saskaņā ar šo direktīvu atbilst Regulai (ES) 2016/679 un Direktīvai 2002/58/EK un aprobežojas ar to, kas ir absolūti

	nepieciešams un samērīgs šīs direktīvas mērķiem.

Grozījums Nr. 53

Direktīvas priekšlikums
2. pants – 5. punkts

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

Grozījums Nr. 54

Direktīvas priekšlikums
2. pants – 6.a punkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	6.a Komisija līdz 2021. gada 31. decembrim publicē priekšlikumu tiesību aktam par Savienības iestāžu, biroju, struktūru un aģentūru (EUI) iekļaušanu vispārējā ES mēroga kiberdrošības satvarā, lai panāktu vienādu aizsardzības līmeni, izmantojot konsekventus un viendabīgus noteikumus.

Grozījums Nr. 55

Direktīvas priekšlikums
4. pants – 1. daļa – 1. punkts – b apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(b) jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču ***grupa***, no kurām viena vai vairākas ierīces, ievērojot programmu, veic digitālu datu automātisku apstrādi***;***	(b) jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču ***kopums***, no kurām viena vai vairākas ierīces, ievērojot programmu, veic digitālu datu automātisku apstrādi***, un kuras ir integrētas IT sistēmā un tiek izmantotas to pakalpojumu sniegšanai, kuriem tās ir paredzētas.***

Grozījums Nr. 56

Direktīvas priekšlikums
4. pants – 1. daļa – 4. punkts

Komisijas ierosinātais teksts	*Grozījums*
(4) "valsts kiberdrošības stratēģija" ir saskaņots dalībvalsts satvars, kas paredz stratēģiskus mērķus un prioritātes attiecībā uz ***tīklu un informācijas sistēmu drošību*** attiecīgajā dalībvalstī;	(4) "valsts kiberdrošības stratēģija" ir saskaņots dalībvalsts satvars, kas paredz stratēģiskus mērķus un prioritātes attiecībā uz ***kiberdrošību*** attiecīgajā dalībvalstī;

Grozījums Nr. 57

Direktīvas priekšlikums
4. pants – 1. daļa – 12. punkts

Komisijas ierosinātais teksts	*Grozījums*
(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;	***svītrots***

Grozījums Nr. 58

Direktīvas priekšlikums
4. pants – 1. daļa – 22. punkts

Komisijas ierosinātais teksts	*Grozījums*
(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;	***svītrots***

Grozījums Nr. 59

Direktīvas priekšlikums
1. pants – 1. daļa – 24. punkts

Komisijas ierosinātais teksts	*Grozījums*
(24) "vienība" ir jebkura fiziska vai juridiska persona, kas izveidota un atzīta kā tāda atbilstoši tās darījumdarbības vietas valsts tiesību aktiem un kas var savā vārdā īstenot tiesības un uzņemties pienākumus;	(24) "vienība" ir jebkura fiziska ***persona*** vai ***jebkura*** juridiska persona, kas izveidota un atzīta kā tāda atbilstoši tās darījumdarbības vietas valsts tiesību aktiem un kas var savā vārdā īstenot tiesības un uzņemties pienākumus;

Grozījums Nr. 60

Direktīvas priekšlikums
5. pants – 1. punkts – a apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(a) dalībvalstu kiberdrošības stratēģijas mērķu un prioritāšu definīciju;	(a) dalībvalstu kiberdrošības stratēģijas mērķu un prioritāšu definīciju***, ņemot vērā to, kāda ir iedzīvotāju vispārējā informētība par kiberdrošību un cik drošas kopumā ir patērētāju savienotās ierīces;***

Grozījums Nr. 61

Direktīvas priekšlikums
5. pants – 1. punkts – f apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(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 par incidentiem un kiberdraudiem un uzraudzības uzdevumu īstenošanu.	(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], ***gan dalībvalstīs, gan starp tām,*** lai apmainītos ar informāciju par incidentiem un kiberdraudiem un uzraudzības uzdevumu īstenošanu.
[38] [ierakstīt pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]	[38] [ierakstīt pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

Grozījums Nr. 62

Direktīvas priekšlikums
5. pants – 2. punkts – b apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(b) pamatnostādnes par to, kā publiskajā iepirkumā iekļaut un noteikt ar kiberdrošību saistītas prasības IKT produktiem un pakalpojumiem;	(b) pamatnostādnes par to, kā publiskajā iepirkumā iekļaut un noteikt ar kiberdrošību saistītas prasības IKT produktiem un pakalpojumiem***, ietverot (bet ne tikai) šifrēšanas prasības un atklātā pirmkoda kiberdrošības produktu izmantošanas veicināšanu***;

Grozījums Nr. 63

Direktīvas priekšlikums
5. pants – 2. punkts – da apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(da) politika, kas saistīta ar drošības nolūkos īstenotu atklāto datu un atvērtā pirmkoda izmantošanas saglabāšanu, nodrošinot pārredzamību;

Grozījums Nr. 64

Direktīvas priekšlikums
5. pants – 2. punkts – db apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(db) politika, kas veicina tiešsaistes pakalpojumu lietotāju personas datu privātumu un drošību;

Grozījums Nr. 65

Direktīvas priekšlikums
5. pants – 2. punkts – e apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(e) politika kiberdrošības prasmju, izpratnes veidošanas, kā arī pētniecības un izstrādes iniciatīvu veicināšanai un attīstīšanai;	(e) politika kiberdrošības prasmju, izpratnes veidošanas, kā arī pētniecības un izstrādes iniciatīvu veicināšanai un attīstīšanai***, tostarp apmācības programmu izstrāde kiberdrošības jomā, lai nodrošinātu vienībām nepieciešamos speciālistus un tehniķus;***

Grozījums Nr. 66

Direktīvas priekšlikums
5. pants – 2. punkts – f apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(f) ***politika par atbalstu akadēmiskās*** un pētniecības ***iestādēm*** kiberdrošības ***rīku*** un ***drošas tīklu infrastruktūras attīstīšanā***;	(f) ***politika tādu akadēmisko*** un pētniecības ***iestāžu atbalstam, kuras sniedz ieguldījumu valsts*** kiberdrošības ***stratēģijā, izstrādājot*** un ***izvēršot kiberdrošības rīkus un drošu tīkla infrastruktūru, kas veicina valsts kiberdrošības stratēģijas īstenošanu, tostarp konkrētas rīcībpolitikas, ar kurām risina jautājumus, kas saistīti ar dzimumu pārstāvību un līdzsvaru šajā nozarē***;

Grozījums Nr. 67

Direktīvas priekšlikums
5. pants – 2. punkts – h apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(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.	(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 ***un to spēju reaģēt uz kiberdrošības incidentiem***.

Grozījums Nr. 68

Direktīvas priekšlikums
6. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. ENISA izstrādā un uztur Eiropas neaizsargātības reģistru. Šajā nolūkā ENISA izveido un uztur atbilstīgas informācijas sistēmas, politikas nostādnes un procedūras, jo īpaši lai svarīgās un būtiskās vienības un to tīklu un informācijas sistēmu piegādātāji varētu atklāt un reģistrēt neaizsargātību, kas saistīta ar IKT produktiem vai IKT pakalpojumiem, kā arī lai nodrošinātu visām ieinteresētajām personām piekļuvi reģistrā ietvertajai informācijai par neaizsargātību. Reģistrā jo īpaši iekļauj informāciju, kas raksturo neaizsargātību, ietekmēto IKT produktu vai IKT pakalpojumus un neaizsargātības smagumu, proti, apstākļus, kādos to var izmantot, saistītu ielāpu pieejamību un — ja nav pieejamu ielāpu — neaizsargātu produktu lietotājiem adresētus norādījumus par to, kā var mazināt no atklātās neaizsargātības izrietošos riskus.	2. ENISA izstrādā un uztur Eiropas neaizsargātības reģistru. Šajā nolūkā ENISA izveido un uztur atbilstīgas informācijas sistēmas, politikas nostādnes un procedūras, jo īpaši lai svarīgās un būtiskās vienības un to tīklu un informācijas sistēmu piegādātāji varētu atklāt un reģistrēt neaizsargātību, kas saistīta ar IKT produktiem vai IKT pakalpojumiem, kā arī lai nodrošinātu visām ieinteresētajām personām piekļuvi reģistrā ietvertajai informācijai par neaizsargātību. Reģistrā jo īpaši iekļauj informāciju, kas raksturo neaizsargātību, ietekmēto IKT produktu vai IKT pakalpojumus un neaizsargātības smagumu, proti, apstākļus, kādos to var izmantot, saistītu ielāpu pieejamību un — ja nav pieejamu ielāpu — neaizsargātu produktu lietotājiem adresētus norādījumus par to, kā var mazināt no atklātās neaizsargātības izrietošos riskus. ***Lai nodrošinātu reģistrā iekļautās informācijas drošību un pieejamību, ENISA piemēro progresīvākos drošības pasākumus un dara informāciju pieejamu mašīnlasāmos formātos, izmantojot attiecīgās saskarnes.***

Grozījums Nr. 69

Direktīvas priekšlikums
7. pants – 3. punkts – a apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(a) valsts sagatavotības pasākumu un darbību mērķus;	(a) valsts ***un – attiecīgā gadījumā un ja tas ir atbilstīgi – reģionālo un pārrobežu*** sagatavotības pasākumu un darbību mērķus;

Grozījums Nr. 70

Direktīvas priekšlikums
10. pants – 2. punkts – e apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(e) pēc vienības pieprasījuma — to pakalpojumu sniegšanā izmantoto tīklu un informācijas sistēmu ***proaktīvas*** skenēšanas nodrošināšana;	(e) pēc vienības pieprasījuma — to pakalpojumu sniegšanā izmantoto tīklu un informācijas sistēmu ***un tīklu tvēruma drošības*** skenēšanas nodrošināšana ***nolūkā apzināt, mazināt vai nepieļaut konkrētus draudus; personas datu apstrāde saistībā ar šādu skenēšanu attiecas tikai uz to, kas ir absolūti nepieciešams, un jebkurā gadījumā uz IP adresēm un URL;***

Grozījums Nr. 71

Direktīvas priekšlikums
11. pants – 4. punkts

Komisijas ierosinātais teksts	*Grozījums*
4. Ciktāl nepieciešams šajā direktīvā noteikto uzdevumu un pienākumu izpildei, dalībvalstis nodrošina atbilstīgu sadarbību starp kompetentajām iestādēm, vienotajiem kontaktpunktiem un tiesībaizsardzības iestādēm, datu aizsardzības iestādēm un iestādēm, kas atbild par kritiskajām infrastruktūrām atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], un valsts finanšu iestādēm, kas izraudzītas saskaņā	4. Ciktāl nepieciešams šajā direktīvā noteikto uzdevumu un pienākumu izpildei, dalībvalstis nodrošina atbilstīgu sadarbību starp kompetentajām iestādēm, vienotajiem kontaktpunktiem un tiesībaizsardzības iestādēm, datu aizsardzības iestādēm un iestādēm, kas atbild par kritiskajām infrastruktūrām atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], un valsts finanšu iestādēm, kas izraudzītas saskaņā

ar Eiropas Parlamenta un Padomes Regulu (ES) XXXX/XXXX[39] [DORA regula] minētajā dalībvalstī.	ar Eiropas Parlamenta un Padomes Regulu (ES) XXXX/XXXX[39] [DORA regula] minētajā dalībvalstī ***saskaņā ar to attiecīgajām kompetencēm***.
[39] [ierakstīt pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]	[39] [ierakstīt pilnu nosaukumu un atsauci uz publikāciju OV, kad zināms]

Grozījums Nr. 72

Direktīvas priekšlikums
11. pants – 5. punkts

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

Grozījums Nr. 73

Direktīvas priekšlikums
12. pants – 3. punkts – ievaddaļa

Komisijas ierosinātais teksts	*Grozījums*
3. Sadarbības grupas sastāvā ir pārstāvji no dalībvalstīm, Komisijas un ENISA. Sadarbības grupas darbībās kā novērotājs piedalās Eiropas Ārējās darbības dienests. Sadarbības grupas darbībās var piedalīties Eiropas uzraudzības iestādes (EUI) saskaņā ar	3. Sadarbības grupas sastāvā ir pārstāvji no dalībvalstīm, Komisijas un ENISA. Sadarbības grupas darbībās kā novērotājs piedalās Eiropas Ārējās darbības dienests***, Eiropola Eiropas Kibernoziedzības apkarošanas centrs un Eiropas Datu aizsardzības kolēģija***.

Regulas (ES) XXXX/XXXX [DORA regula] 17. panta 5. punkta c) apakšpunktu.	Sadarbības grupas darbībās var piedalīties Eiropas uzraudzības iestādes (EUI) saskaņā ar Regulas (ES) XXXX/XXXX [DORA regula] 17. panta 5. punkta c) apakšpunktu.

Grozījums Nr. 74

Direktīvas priekšlikums
12. pants – 3. punkts – 1. daļa

Komisijas ierosinātais teksts	*Grozījums*
Attiecīgā gadījumā sadarbības grupa var uzaicināt tās darbā piedalīties pārstāvjus ***no attiecīgajām ieinteresētajām personām***.	***Sadarbības grupa, ja tas nepieciešams tās uzdevumu veikšanai, uzaicina*** tās darbā piedalīties ***attiecīgo ieinteresēto personu*** pārstāvjus***, bet Eiropas Parlamentu — kā novērotāju***.

Grozījums Nr. 75

Direktīvas priekšlikums
12. pants – 8. punkts

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

Grozījums Nr. 76

Direktīvas priekšlikums
13. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. CSIRT tīkls sastāv no dalībvalstu CSIRT un CERT-EU pārstāvjiem. Komisija piedalās CSIRT tīklā novērotāja statusā. ENISA nodrošina sekretariātu un aktīvi atbalsta sadarbību starp CSIRT.	2. CSIRT tīkls sastāv no dalībvalstu CSIRT un CERT-EU pārstāvjiem. Komisija ***un Eiropola Eiropas Kibernoziedzības apkarošanas centrs*** piedalās CSIRT tīklā novērotāja statusā. ENISA nodrošina sekretariātu un aktīvi

atbalsta sadarbību starp CSIRT.

Grozījums Nr. 77

Direktīvas priekšlikums
14. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. EU-CyCLONe sastāvā ir pārstāvji no dalībvalstu krīžu pārvaldības iestādēm, kas izraudzītas saskaņā ar 7. pantu, Komisijas un ENISA. ENISA nodrošina tīkla sekretariātu un atbalsta drošu informācijas apmaiņu.	2. EU-CyCLONe sastāvā ir pārstāvji no dalībvalstu krīžu pārvaldības iestādēm, kas izraudzītas saskaņā ar 7. pantu, Komisijas un ENISA. ***EU-CyCLONe darbībās kā novērotājs piedalās Eiropola Eiropas Kibernoziedzības apkarošanas centrs.*** ENISA nodrošina tīkla sekretariātu un atbalsta drošu informācijas apmaiņu.

Grozījums Nr. 78

Direktīvas priekšlikums
14. pants – 6. punkts

Komisijas ierosinātais teksts	*Grozījums*
6. EU-CyCLONe sadarbojas ar CSIRT tīklu, pamatojoties uz saskaņotu procesuālo kārtību.	6. EU-CyCLONe sadarbojas ar CSIRT tīklu, pamatojoties uz saskaņotu procesuālo kārtību***, un ar tiesībaizsardzības iestādēm saskaņā ar ES tiesībaizsardzības iestāžu ārkārtas reaģēšanas protokolu***.

Grozījums Nr. 79

Direktīvas priekšlikums
15. pants – 1. punkts – ievaddaļa

Komisijas ierosinātais teksts	*Grozījums*
1. ENISA, sadarbojoties ar Komisiju, izdod ***divgadu*** ziņojumu par situāciju kiberdrošības jomā Savienībā. ***Ziņojumā*** īpaši iekļauj novērtējumu par:	1. ENISA, sadarbojoties ar Komisiju, izdod ***gada*** ziņojumu par situāciju kiberdrošības jomā Savienībā. ***Ziņojumu iesniedz mašīnlasāmā formātā un tajā*** īpaši iekļauj novērtējumu par:

Grozījums Nr. 80

Direktīvas priekšlikums
15. pants – 1. punkts – ca apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(ca) kiberdrošības incidentu ietekmi uz personas datu aizsardzību Savienībā.

Grozījums Nr. 81

Direktīvas priekšlikums
15. pants – 1. punkts – cb apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(cb) pārskatu par iedzīvotāju vispārējo kiberdrošības izpratnes un izmantošanas līmeni, kā arī par Savienības tirgū laisto patērētājiem paredzēto savienoto ierīču vispārējo drošības līmeni;

Grozījums Nr. 82

Direktīvas priekšlikums
17. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. Dalībvalstis nodrošina, ka pārvaldības struktūras locekļi regulāri apgūst īpašu apmācību, kurā iegūst pietiekamas zināšanas un prasmes, lai izprastu un novērtētu kiberdrošības riskus un pārvaldības praksi, kā arī to ietekmi uz vienības darbībām.	2. Dalībvalstis nodrošina, ka pārvaldības struktūras locekļi ***un par kiberdrošību atbildīgie speciālisti*** regulāri apgūst īpašu apmācību, kurā iegūst pietiekamas zināšanas un prasmes, lai izprastu un novērtētu ***pastāvīgi mainīgos*** kiberdrošības riskus un pārvaldības praksi, kā arī to ietekmi uz vienības darbībām.

Grozījums Nr. 83

Direktīvas priekšlikums
18. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Dalībvalstis nodrošina, ka būtiskās	1. Dalībvalstis nodrošina, ka būtiskās

un svarīgās vienības veic atbilstīgus un samērīgus tehniskos un organizatoriskos pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmu ***drošībai***, ko tās izmanto savu pakalpojumu sniegšanā. Ņemot vērā jaunākos tehniskos sasniegumus, ar minētajiem pasākumiem nodrošina radītajam riskam atbilstošu tīklu un informācijas sistēmu ***drošības*** līmeni.	un svarīgās vienības veic atbilstīgus un samērīgus tehniskos un organizatoriskos pasākumus, lai pārvaldītu riskus to tīklu un informācijas sistēmu ***kiberdrošībai***, ko tās izmanto savu pakalpojumu sniegšanā***, un lai nodrošinātu šo pakalpojumu nepārtrauktību un mazinātu riskus, kas rodas fizisku personu tiesībām, apstrādājot viņu personas datus.*** Ņemot vērā jaunākos tehniskos sasniegumus, ar minētajiem pasākumiem nodrošina radītajam riskam atbilstošu tīklu un informācijas sistēmu ***kiberdrošības*** līmeni.

Grozījums Nr. 84

Direktīvas priekšlikums
18. pants – 2. punkts – g apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(g) kriptogrāfijas un šifrēšanas izmantošanu.	(g) kriptogrāfijas un ***spēcīgas*** šifrēšanas izmantošanu.

Grozījums Nr. 85

Direktīvas priekšlikums
18. pants – 3. punkts

Komisijas ierosinātais teksts	*Grozījums*
3. Dalībvalstis nodrošina, ka, apsverot atbilstīgus pasākumus, kas minēti 2. punkta d) apakšpunktā, vienības ņem vērā neaizsargātību, kas raksturīga katram piegādātājam un pakalpojumu sniedzējam, un to piegādātāju un pakalpojumu sniedzēju produktu vispārējo kvalitāti un kiberdrošības praksi, ieskaitot to drošās attīstības procedūras.	3. Dalībvalstis nodrošina, ka, apsverot atbilstīgus ***un samērīgus*** pasākumus, kas minēti 2. punkta d) apakšpunktā, vienības ņem vērā neaizsargātību, kas raksturīga katram piegādātājam un pakalpojumu sniedzējam, un to piegādātāju un pakalpojumu sniedzēju produktu vispārējo kvalitāti un kiberdrošības praksi, ieskaitot to drošās attīstības procedūras. ***Kompetentās iestādes sniedz vienībām norādījumus par to praktisko un proporcionālu piemērošanu.***

Grozījums Nr. 86

Direktīvas priekšlikums

18. pants – 6.a punkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	6.a Dalībvalstis piešķir būtiskas vai svarīgas vienības nodrošinātas tīkla un informācijas sistēmas lietotājam tiesības iegūt no vienības informāciju par tehniskajiem un organizatoriskajiem pasākumiem, kas ieviesti, lai pārvaldītu tīklu un informācijas sistēmu drošībai radītos riskus. Dalībvalstis nosaka šo tiesību ierobežojumus.

Grozījums Nr. 87

Direktīvas priekšlikums
19. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Sadarbības grupa kopā ar Komisiju un ENISA ***var veikt*** īpašu kritisku IKT pakalpojumu, sistēmu vai produktu piegādes ķēžu koordinētus drošības riska novērtējumus, ņemot vērā tehniskus un attiecīgā gadījumā netehniskus riska faktorus.	1. Sadarbības grupa kopā ar Komisiju un ENISA ***veic*** īpašu kritisku IKT pakalpojumu, sistēmu vai produktu piegādes ķēžu koordinētus drošības riska novērtējumus, ņemot vērā tehniskus un attiecīgā gadījumā netehniskus riska faktorus.

Grozījums Nr. 88

Direktīvas priekšlikums
20. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās paziņo kompetentajām iestādēm vai CSIRT saskaņā ar 3. un 4. punktu par ikvienu incidentu, kam ir būtiska ietekme uz to pakalpojumu sniegšanu***. Attiecīgā gadījumā*** minētās vienības bez nepamatotas kavēšanās informē savus pakalpojumu saņēmējus par incidentiem, kas varētu nelabvēlīgi ietekmēt konkrētā pakalpojuma sniegšanu. Dalībvalstis nodrošina, ka minētās vienības cita starpā	1. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās***, bet jebkurā gadījumā 24 stundu laikā,*** paziņo kompetentajām iestādēm vai CSIRT saskaņā ar 3. un 4. punktu par ikvienu incidentu, kam ir būtiska ietekme uz to pakalpojumu sniegšanu***, un kompetentajām tiesībaizsardzības iestādēm, ja pastāv aizdomas vai ir zināms, ka šim starpgadījumam ir ļaunprātīgs nolūks.*** Minētās vienības bez nepamatotas

paziņo visu informāciju, kas ļauj kompetentajām iestādēm vai CSIRT noteikt incidenta pārrobežu ietekmi.	kavēšanās***, bet jebkurā gadījumā 24 stundu laikā,*** informē savus pakalpojumu saņēmējus par incidentiem, kas varētu nelabvēlīgi ietekmēt konkrētā pakalpojuma sniegšanu***, un sniedz informāciju, kas viņiem ļauj mazināt kiberuzbrukumu nelabvēlīgo ietekmi. Izņēmuma gadījumā, ja publiskošana var izraisīt papildu kiberuzbrukumus, minētās vienības paziņošanu var aizkavēt***. Dalībvalstis nodrošina, ka minētās vienības cita starpā paziņo visu informāciju, kas ļauj kompetentajām iestādēm vai CSIRT noteikt incidenta pārrobežu ietekmi.

Grozījums Nr. 89

Direktīvas priekšlikums
20. pants – 2. punkts – ievaddaļa

Komisijas ierosinātais teksts	*Grozījums*
2. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības bez nepamatotas kavēšanās informē kompetentās iestādes vai CSIRT par visiem nozīmīgajiem kiberdraudiem, ko minētās vienības identificējušas kā tādus, kuri būtu varējuši izraisīt nozīmīgu incidentu.	2. Dalībvalstis nodrošina, ka būtiskās un svarīgās vienības ***spēj informēt*** kompetentās iestādes vai *CSIRT* par visiem nozīmīgajiem kiberdraudiem, ko minētās vienības identificējušas kā tādus, kuri būtu varējuši izraisīt nozīmīgu incidentu.

Grozījums Nr. 90

Direktīvas priekšlikums
20. pants – 2. punkts – 1. daļa

Komisijas ierosinātais teksts	*Grozījums*
Attiecīgā gadījumā ***minētās vienības bez nepamatotas kavēšanās informē*** savus pakalpojumu saņēmējus, kurus varētu skart ievērojami kiberdraudi, par visiem pasākumiem vai tiesiskās aizsardzības līdzekļiem, ko minētie saņēmēji var veikt, reaģējot uz konkrētajiem draudiem. ***Attiecīgā gadījumā*** vienības arī informē minētos saņēmējus par pašiem draudiem. Paziņošana neuzliek ziņotājai vienībai	Attiecīgā gadījumā ***minētajām vienībām ir ļauts informēt*** savus pakalpojumu saņēmējus, kurus varētu skart ievērojami kiberdraudi, par visiem pasākumiem vai tiesiskās aizsardzības līdzekļiem, ko minētie saņēmēji var veikt, reaģējot uz konkrētajiem draudiem. ***Ja šāda informācija tiek sniegta,*** vienības arī informē minētos saņēmējus par pašiem draudiem. Paziņošana neuzliek ziņotājai

lielāku atbildību.	vienībai lielāku atbildību.

Grozījums Nr. 91

Direktīvas priekšlikums
20. pants – 4. punkts – c apakšpunkts – ievaddaļa

Komisijas ierosinātais teksts	*Grozījums*
(c) ***galīgu*** ziņojumu ne vēlāk kā mēnesi pēc a) apakšpunktā minētā ziņojuma iesniegšanas, tajā iekļaujot vismaz:	(c) ***visaptverošu*** ziņojumu ne vēlāk kā mēnesi pēc a) apakšpunktā minētā ziņojuma iesniegšanas, tajā iekļaujot vismaz:

Grozījums Nr. 92

Direktīvas priekšlikums
20. pants – 4. punkts – c apakšpunkts – ii punkts

Komisijas ierosinātais teksts	*Grozījums*
(ii) ***draudu*** veidu vai pamatcēloni, kas varētu būt izraisījis incidentu;	(ii) ***kiberdraudu*** veidu vai pamatcēloni, kas varētu būt izraisījis incidentu;

Grozījums Nr. 93

Direktīvas priekšlikums
20. pants – 4. punkts – c apakšpunkts – iii punkts

Komisijas ierosinātais teksts	*Grozījums*
(iii) piemērotos un notiekošos riska mazināšanas pasākumus.	(iii) piemērotos un notiekošos riska mazināšanas ***vai novēršanas*** pasākumus.

Grozījums Nr. 94

Direktīvas priekšlikums
20. pants – 6. punkts

Komisijas ierosinātais teksts	*Grozījums*
6. Attiecīgā gadījumā, īpaši tad, ja 1. punktā minētais incidents skar divas vai vairākas dalībvalstis, kompetentā iestāde vai CSIRT informē citas skartās	6. Attiecīgā gadījumā, īpaši tad, ja 1. punktā minētais incidents skar divas vai vairākas dalībvalstis, kompetentā iestāde vai CSIRT informē citas skartās

dalībvalstis un ENISA par incidentu. To darot, kompetentās iestādes, CSIRT un vienotie kontaktpunkti saskaņā ar Savienības tiesību aktiem vai valsts tiesību aktiem, kas atbilst Savienības tiesību aktiem, nodrošina vienības drošību un komerciālās intereses, kā arī sniegtās informācijas konfidencialitāti.	dalībvalstis un ENISA par incidentu. ***Ja incidents attiecas uz divām vai vairākām dalībvalstīm un ir aizdomas, ka tam ir krimināltiesisks raksturs, kompetentā iestāde vai CSIRT informē Eiropolu.*** 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.

Grozījums Nr. 95

Direktīvas priekšlikums
22. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
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.	2. ENISA ***pēc apspriešanās ar EDAK un*** 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.

Grozījums Nr. 96

Direktīvas priekšlikums
23. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Lai veicinātu DNS drošību, stabilitāti un noturību, dalībvalstis nodrošina, ka ALD ***reģistri un vienības, kas sniedz domēnu nosaukumu reģistrācijas pakalpojumus saistībā ar ALD,*** ar pienācīgu rūpību ***savāc*** un ***uztur precīzus*** un ***pilnīgus*** domēnu nosaukumu reģistrācijas ***datus speciālā datubāzē***, ievērojot Savienības datu aizsardzības tiesību aktus par datiem, kas ir persondati.	1. Lai veicinātu DNS drošību, stabilitāti un noturību, dalībvalstis nodrošina, ka ALD ***ir spēkā politikas nostādnes un procedūras, kuru mērķis ir garantēt, ka*** ar pienācīgu rūpību ***tiek vākti*** un ***uzturēti precīzi*** un ***pilnīgi*** domēnu nosaukumu reģistrācijas ***dati īpaši tam paredzētā datubāzes ierīcē***, ievērojot Savienības datu aizsardzības tiesību aktus par datiem, kas ir persondati. ***Dalībvalstis***

	nodrošina, ka šāda politika un procedūras tiek publiskotas.

Grozījums Nr. 97

Direktīvas priekšlikums
23. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
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.	2. Dalībvalstis nodrošina, ka 1. punktā minētajās ***domēna nosaukuma*** reģistrācijas datu datubāzēs ir ietverta ***nepieciešamā*** informācija, kas ļauj identificēt ***domēna nosaukuma*** turētājus***, proti, viņu vārdu, fizisko adresi, e-pasta adresi, kā arī viņu tālruņa numuru,*** un kontaktpunktus, kuri pārvalda ALD nosaukumus, un sazināties ar tiem.

Grozījums Nr. 98

Direktīvas priekšlikums
23. pants – 3. punkts

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

Pamatojums

Šī punkts ir iekļauts 23. pantā kā 1. punkts.

Grozījums Nr. 99

Direktīvas priekšlikums
23. pants – 4. punkts

Komisijas ierosinātais teksts	*Grozījums*
4. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz ***domēnu nosaukumu*** reģistrācijas pakalpojumus saistībā ar ALD, bez ***nepamatotas*** kavēšanās pēc domēna nosaukuma reģistrācijas publicē ***domēnu*** reģistrācijas datus, ***kas nav persondati***.	4. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz ***domēna nosaukuma*** reģistrācijas pakalpojumus saistībā ar ALD, ***saskaņā ar Regulas (ES) 2016/679 6. panta 1. punkta c) apakšpunktu un 6. panta 3. punktu un*** bez ***liekas*** kavēšanās pēc domēna nosaukuma reģistrācijas publicē ***konkrētus domēna nosaukuma*** reģistrācijas datus, ***piemēram, domēna nosaukumu un juridiskās personas vārdu***.

Grozījums Nr. 100

Direktīvas priekšlikums
23. pants – 5. punkts

Komisijas ierosinātais teksts	*Grozījums*
5. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz ***domēnu nosaukumu*** reģistrācijas pakalpojumus saistībā ar ALD, sniedz ***leģitīmiem piekļuves prasītājiem*** pēc to likumīgiem un pienācīgi pamatotiem pieprasījumiem piekļuvi īpašiem domēnu nosaukumu reģistrācijas datiem, ievērojot Savienības datu aizsardzības tiesību aktus. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz ***domēnu nosaukumu*** reģistrācijas pakalpojumus saistībā ar ALD, bez nepamatotas kavēšanās atbild uz visiem piekļuves pieprasījumiem. Dalībvalstis nodrošina, ka politika un procedūras šādu datu izpaušanai tiek publiskotas.	5. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz ***domēna nosaukuma*** reģistrācijas pakalpojumus saistībā ar ALD, sniedz ***publiskajām iestādēm, tostarp šajā direktīvā paredzētajām kompetentajām iestādēm, kompetentajām iestādēm, kas saskaņā ar Savienības vai valsts tiesību aktiem ir atbildīgas par noziedzīgu nodarījumu novēršanu, izmeklēšanu vai kriminālvajāšanu, vai Regulā (ES) 2016/679 paredzētajām uzraudzības iestādēm*** pēc to likumīgiem un pienācīgi pamatotiem pieprasījumiem piekļuvi īpašiem domēna nosaukuma reģistrācijas datiem, ievērojot Savienības datu aizsardzības tiesību aktus. Dalībvalstis nodrošina, ka ALD reģistri un vienības, kas sniedz ***domēna nosaukuma*** reģistrācijas pakalpojumus saistībā ar ALD, bez nepamatotas kavēšanās atbild uz visiem ***likumīgiem un pienācīgi pamatotiem*** piekļuves pieprasījumiem. Dalībvalstis nodrošina, ka politika un procedūras šādu datu izpaušanai tiek publiskotas.

Grozījums Nr. 101

Direktīvas priekšlikums
24. pants – 3. punkts

Komisijas ierosinātais teksts	*Grozījums*
3. Ja 1. punktā minētajai vienībai nav darījumdarbības vietas Savienībā, bet tā piedāvā pakalpojumus Savienībā, tā izraugās pārstāvi Savienībā. Minētajam pārstāvim darījumdarbības vieta ir vienā no dalībvalstīm, kurās tiek piedāvāti pakalpojumi. Uzskata, ka šāda vienība ir tās dalībvalsts jurisdikcijā, kurā ir pārstāvja darījumdarbības vieta. Ja nav izraudzīta pārstāvja Savienībā atbilstoši šim pantam, jebkura dalībvalsts, kurā vienība sniedz pakalpojumus, var veikt tiesiskas darbības pret vienību sakarā ar neatbilstību šajā direktīvā noteiktajiem pienākumiem.	3. Ja 1. punktā minētajai vienībai nav darījumdarbības vietas Savienībā, bet tā piedāvā pakalpojumus Savienībā, tā izraugās pārstāvi Savienībā. Minētajam pārstāvim darījumdarbības vieta ir vienā no dalībvalstīm, kurās tiek piedāvāti pakalpojumi. ***Neskarot Regulā (ES) 2016/679 minēto uzraudzības iestāžu kompetences,*** uzskata, ka šāda vienība ir tās dalībvalsts jurisdikcijā, kurā ir pārstāvja darījumdarbības vieta. Ja nav izraudzīta pārstāvja Savienībā atbilstoši šim pantam, jebkura dalībvalsts, kurā vienība sniedz pakalpojumus, var veikt tiesiskas darbības pret vienību sakarā ar neatbilstību šajā direktīvā noteiktajiem pienākumiem.

Grozījums Nr. 102

Direktīvas priekšlikums
25. pants – 1. punkts – ievaddaļa

Komisijas ierosinātais teksts	*Grozījums*
1. ENISA izveido un uztur 24. panta 1. punktā minēto būtisko un svarīgo vienību reģistru. Vienības līdz [12 mēneši pēc šīs direktīvas stāšanās spēkā] iesniedz ENISA šādu informāciju:	1. ENISA izveido un uztur 24. panta 1. punktā minēto būtisko un svarīgo vienību ***drošu*** reģistru. Vienības līdz [12 mēneši pēc šīs direktīvas stāšanās spēkā] iesniedz ENISA šādu informāciju:

Grozījums Nr. 103

Direktīvas priekšlikums
26. pants – 1. punkts – ievaddaļa

Komisijas ierosinātais teksts	*Grozījums*
1. Neskarot Regulu (ES) 2016/679, dalībvalstis nodrošina, ka būtiskās un	1. Neskarot Regulu (ES) 2016/679 ***vai Direktīvu 2002/58/EK***, dalībvalstis

svarīgās vienības var savstarpēji apmainīties ar būtisku kiberdrošības informāciju, ieskaitot informāciju, kas attiecas uz kiberdraudiem, neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem, ja šāda informācijas apmaiņa:	nodrošina, ka būtiskās un svarīgās vienības var savstarpēji apmainīties ar būtisku kiberdrošības informāciju, ieskaitot informāciju, kas attiecas uz kiberdraudiem, neaizsargātību, apdraudējuma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem***, kā arī uzbrucēja atrašanās vietu vai identitāti***, ja šāda informācijas apmaiņa:

Grozījums Nr. 104

Direktīvas priekšlikums
28. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. Pievēršoties incidentiem, kuru rezultātā notiek persondatu aizsardzības pārkāpumi, kompetentās iestādes strādā ciešā sadarbībā ar ***datu aizsardzības*** iestādēm.	2. Pievēršoties incidentiem, kuru rezultātā notiek persondatu aizsardzības pārkāpumi, kompetentās iestādes strādā ciešā sadarbībā ar ***uzraudzības iestādēm, neskarot šīm*** iestādēm ***Regulā (ES) 2016/679 paredzētās kompetences, uzdevumus un pilnvaras. Šajā nolūkā kompetentās iestādes un uzraudzības iestādes apmainās ar informāciju, kas attiecas uz to attiecīgo kompetences jomu. Turklāt kompetentās iestādes pēc kompetento uzraudzības iestāžu pieprasījuma sniedz tām visu informāciju, kas iegūta saistībā ar jebkādām revīzijām un izmeklēšanām, kuras attiecas uz personas datu apstrādi.***

Grozījums Nr. 105

Direktīvas priekšlikums
29. pants – 4. punkts – h apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(h) uzdot minētajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos vērojama neatbilstība šajā direktīvā noteiktajiem pienākumiem;	***svītrots***

Grozījums Nr. 106

Direktīvas priekšlikums
29. pants – 5. punkts – b apakšpunkts

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

Grozījums Nr. 107

Direktīvas priekšlikums
29. pants – 5. punkts – 1. daļa

Komisijas ierosinātais teksts	*Grozījums*
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.	***Šo sankciju*** piemēro tikai līdz brīdim, kad vienība veic nepieciešamo darbību, lai izlabotu trūkumus vai izpildītu kompetentās iestādes prasības, attiecībā uz kurām šādas sankcijas piemērotas.

Grozījums Nr. 108

Direktīvas priekšlikums
29. pants – 7. punkts – c apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(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	(c) ***faktisko radīto materiālo*** vai ***nemateriālo*** kaitējumu vai ***radītos*** zaudējumus, 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

citiem pakalpojumiem, skarto vai iespējami skarto lietotāju skaitu;	skarto lietotāju skaitu;

Grozījums Nr. 109

Direktīvas priekšlikums
29. pants – 7. punkts – ca apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(ca) jebkādus attiecīgus skartās vienības iepriekšējus pārkāpumus;

Grozījums Nr. 110

Direktīvas priekšlikums
29. pants – 7. punkts – cb apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(cb) veidu, kādā par pārkāpumu ir uzzinājusi kompetentā iestāde, jo īpaši to, vai vienība ir ziņojusi par pārkāpumu, un, ja ir, – kādā apjomā;

Grozījums Nr. 111

Direktīvas priekšlikums
29. pants – 7. punkts – g apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(g) ***to, cik lielā mērā pie atbildības sauktā(-ās) fiziskā(-ās) vai juridiskā(-ās) persona(-as) sadarbojas ar kompetentajām iestādēm.***	(g) ***sadarbības pakāpi ar kompetentajām iestādēm, lai novērstu pārkāpumu un mazinātu pārkāpumu iespējamās nelabvēlīgās sekas;***

Grozījums Nr. 112

Direktīvas priekšlikums
29. pants – 7. punkts – ga apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(ga) jebkādu citu pastiprinošu vai mīkstinošu apstākli, kas attiecas uz lietas faktiskajiem apstākļiem, piemēram, no pārkāpuma tieši vai netieši gūto finansiālo labumu vai novērstos zaudējumus.

Grozījums Nr. 113

Direktīvas priekšlikums
29. pants – 9. punkts

Komisijas ierosinātais teksts	*Grozījums*
9. Dalībvalstis nodrošina, ka to kompetentās iestādes, kad tās īsteno savas uzraudzības un izpildes pilnvaras, kuru mērķis ir nodrošināt, lai būtiska vienība, kas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva] identificēta kā kritiska, vai vienība, kas ir līdzvērtīga kritiskai vienībai, ievērotu šajā direktīvā noteiktos pienākumus, informē attiecīgās kompetentās iestādes ***citā dalībvalstī***, kuras izraudzītas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva]. Ja to pieprasa kompetentās iestādes atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], kompetentās iestādes var īstenot savas uzraudzības un izpildes pilnvaras attiecībā uz būtisku vienību, kas identificēta kā kritiska vai kritiskai līdzvērtīga vienība.	9. Dalībvalstis nodrošina, ka to kompetentās iestādes, kad tās īsteno savas uzraudzības un izpildes pilnvaras, kuru mērķis ir nodrošināt, lai būtiska vienība, kas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva] identificēta kā kritiska, vai vienība, kas ir līdzvērtīga kritiskai vienībai, ievērotu šajā direktīvā noteiktos pienākumus, ***reāllaikā*** informē attiecīgās kompetentās iestādes ***visās dalībvalstīs***, kuras izraudzītas atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva]. Ja to pieprasa kompetentās iestādes atbilstoši Direktīvai (ES) XXXX/XXXX [Kritisko vienību noturības direktīva], kompetentās iestādes var īstenot savas uzraudzības un izpildes pilnvaras attiecībā uz būtisku vienību, kas identificēta kā kritiska vai kritiskai līdzvērtīga vienība.

Grozījums Nr. 114

Direktīvas priekšlikums
30. pants – 4. punkts – g apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(g) uzdot minētajām vienībām noteiktā veidā publiskot informāciju par to, kādos aspektos vērojama neatbilstība šajā direktīvā noteiktajiem to pienākumiem;	***svītrots***

Grozījums Nr. 115

Direktīvas priekšlikums
30. pants – 4. punkts – h apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
(h) sniegt publisku paziņojumu, kurā norāda ***fizisko(-ās) un*** juridisko(-ās) personu(-as), kas atbild par šajā direktīvā noteikta pienākuma pārkāpumu, un par attiecīgā pārkāpuma raksturu;	h) sniegt publisku paziņojumu, kurā norāda juridisko(-ās) personu(-as), kas atbild par šajā direktīvā noteikta pienākuma pārkāpumu, un par attiecīgā pārkāpuma raksturu;

Grozījums Nr. 116

Direktīvas priekšlikums
31. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
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.	2. Administratīvos naudas sodus 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***, atkarībā no katra individuālā gadījuma apstākļiem***.

Grozījums Nr. 117

Direktīvas priekšlikums
31. pants – 3. punkts

Komisijas ierosinātais teksts	*Grozījums*
3. Izlemjot, vai piemērot administratīvu naudas sodu, un lemjot par tā summu, katrā individuālā gadījumā	3. Izlemjot, vai piemērot administratīvu naudas sodu, ***jāņem vērā katra individuāla gadījuma faktiskie***

pienācīgi ņem vērā vismaz 29. panta 7. punktā paredzētos elementus.	***apstākļi,*** un lemjot par tā summu, katrā individuālā gadījumā pienācīgi ņem vērā vismaz 29. panta 7. punktā paredzētos elementus.

Grozījums Nr. 118

Direktīvas priekšlikums
32. punkts – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Ja kompetentajām iestādēm ir sniegtas norādes, ka būtiskas vai svarīgas vienības izdarīts 18. un 20. pantā noteikto pienākumu pārkāpums ietver persondatu aizsardzības pārkāpumu, kas definēts Regulas (ES) 2016/679 4. panta 12. punktā un ko paziņo atbilstoši minētās regulas 33. pantam, tās ***saprātīgā termiņā*** informē uzraudzības iestādes, kas ir kompetentas atbilstoši minētās regulas 55. un 56. pantam.	1. Ja kompetentajām iestādēm ir sniegtas norādes, ka būtiskas vai svarīgas vienības izdarīts 18. un 20. pantā noteikto pienākumu pārkāpums ietver persondatu aizsardzības pārkāpumu, kas definēts Regulas (ES) 2016/679 4. panta 12. punktā un ko paziņo atbilstoši minētās regulas 33. pantam, tās ***bez liekas kavēšanās, bet jebkurā gadījumā 24 stundu laikā,*** informē uzraudzības iestādes, kas ir kompetentas atbilstoši minētās regulas 55. un 56. pantam.

Grozījums Nr. 119

Direktīvas priekšlikums
32. pants – 3. punkts

Komisijas ierosinātais teksts	*Grozījums*
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.	3. Ja uzraudzības iestāde, kas ir kompetenta atbilstoši Regulai (ES) 2016/679, veic darbību citā dalībvalstī, kas nav kompetentās iestādes dalībvalsts, kompetentā iestāde ***informē*** uzraudzības iestādi, kas veic darbību minētajā dalībvalstī.

Grozījums Nr. 120

Direktīvas priekšlikums
34.a pants (jauns)

Komisijas ierosinātais teksts	*Grozījums*

	34.a pants
	Atbildība par noteikumu neievērošanu
	Neskarot nekādu pieejamo administratīvo vai ārpustiesas tiesisko aizsardzību, būtisko un svarīgo vienību sniegto pakalpojumu saņēmējiem, kuriem ir radušies zaudējumi tādēļ, ka pakalpojumu sniedzēji nav ievērojuši šo direktīvu, ir tiesības uz efektīvu tiesisko aizsardzību tiesā.

Grozījums Nr. 121

Direktīvas priekšlikums
35. punkts – 1. daļa

Komisijas ierosinātais teksts	*Grozījums*
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. Šim nolūkam un lai turpinātu attīstīt stratēģisko un operatīvo sadarbību, Komisija ņem vērā sadarbības grupas un CSIRT tīkla ziņojumus par stratēģiskā un operatīvā līmenī gūto pieredzi. Pirmo ziņojumu iesniedz līdz (..) ***54*** mēneši pēc šīs direktīvas spēkā stāšanās dienas.	Komisija periodiski pārskata šīs direktīvas darbību un ***reizi trīs gados*** iesniedz ziņojumu Eiropas Parlamentam un Padomei. Ziņojumā ***jo īpaši izvērtē, cik lielā mērā direktīva ir palīdzējusi nodrošināt vienādi augsta līmeņa tīklu*** un ***informācijas sistēmu drošību un integritāti***, ***vienlaikus nodrošinot optimālu privātās dzīves*** un ***personas datu aizsardzību,*** un ***to, cik liela nozīme*** ekonomikas un ***sabiedrības darbībai*** saistībā ar kiberdrošību ***ir I un II pielikumā minēto struktūru nozaru un apakšnozaru lielumam un veidam***. Šim nolūkam un lai turpinātu attīstīt stratēģisko un operatīvo sadarbību, Komisija ņem vērā sadarbības grupas un CSIRT tīkla ziņojumus par stratēģiskā un operatīvā līmenī gūto pieredzi. Pirmo ziņojumu iesniedz līdz (..) ***36*** mēneši pēc šīs direktīvas spēkā stāšanās dienas.

Grozījums Nr. 122

Direktīvas priekšlikums
I pielikums – 5. punkts (Veselība) – 6. ievilkums (jauns)

Komisijas ierosinātais teksts

Nozare	Apakšnozare	Vienības veids
5. Veselība		– Veselības aprūpes sniedzēji, kas minēti Direktīvas 2011/24/ES 3. panta g) punktā – ES references laboratorijas, kas minētas Regulas XXXX/XXXX par nopietniem pārrobežu veselības apdraudējumiem[91] 15. pantā – Vienības, kas veic izpētes un izstrādes darbības attiecībā uz zālēm, kas minētas Direktīvas 2001/83/EK[92] 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 ierīces, kuras uzskata par kritiskām sabiedrības veselības ārkārtas situācijā (“kritisko ierīču saraksts sabiedrības veselības ārkārtas situācijām”) un kuras minētas Regulas XXXX[93] 20. pantā

[91] [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]

[92] 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.).

[93] [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]

Grozījums

Nozare	Apakšnozare	Vienības veids
5. Veselība		– Veselības aprūpes sniedzēji, kas minēti Direktīvas 2011/24/ES 3. panta g) punktā ([90]) – ES references laboratorijas, kas minētas Regulas XXXX/XXXX par nopietniem pārrobežu veselības apdraudējumiem 15. pantā[91] – Vienības, kas veic izpētes un izstrādes darbības attiecībā uz zālēm, kas minētas Direktīvas 2001/83/EK 1. panta 2. punktā ([92]) – Vienības, kas ražo farmaceitiskās pamatvielas un farmaceitiskos preparātus, kuri minēti NACE 2. red. 21. nodaļas C sadaļā – Vienības, kas ražo medicīniskās ierīces, kuras uzskata par kritiskām sabiedrības veselības ārkārtas situācijā (“kritisko ierīču saraksts sabiedrības

veselības ārkārtas situācijām") un kuras minētas Regulas XXXX[93] 20. pantā

– Vienības, kurām ir Direktīvas 2001/83/EK 79. pantā minētā izplatīšanas atļauja

[91] [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)0727 final].

[92] 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.).

[93] [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)0725 final].

ATZINUMU SNIEDZOŠĀS KOMITEJAS PROCEDŪRA

Virsraksts	Pasākumi nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienībā un Direktīvas (ES) 2016/1148 atcelšana
Atsauces	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Atbildīgā komiteja Datums, kad paziņoja plenārsēdē	ITRE 21.1.2021
Atzinumu sniedza Datums, kad paziņoja plenārsēdē	LIBE 21.1.2021
Iesaistītās komitejas - datums, kad paziņoja plenārsēdē	20.5.2021
Atzinuma sagatavotājs(-a) Iecelšanas datums	Lukas Mandl 12.4.2021
Izskatīšana komitejā	16.6.2021 3.9.2021 11.10.2021
Pieņemšanas datums	12.10.2021
Galīgais balsojums	+: 44 –: 14 0: 4
Komitejas locekļi, kas bija klāt galīgajā balsošanā	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Aizstājēji, kas bija klāt galīgajā balsošanā	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

ATZINUMU SNIEDZOŠĀS KOMITEJAS
GALĪGAIS BALSOJUMS PĒC SARAKSTA

44	**+**
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	**-**
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	**0**
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Izmantoto apzīmējumu skaidrojums:
+ : par
- : pret
0 : atturas