Eiropas Savienības
Padome

Briselē, 2018. gada 29. maijā
(OR. en)

9350/18

Starpiestāžu lieta:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

PIEZĪME

Sūtītājs:	prezidentvalsts
Saņēmējs:	Padome
Iepr. dok. Nr.:	8834/18
K-jas dok. Nr.:	12183/17
Temats:	Priekšlikums – EIROPAS PARLAMENTA UN PADOMES REGULA par *ENISA* – ES Kiberdrošības aģentūru – un Regulas (ES) 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju ("Kiberdrošības akts") – vispārēja pieeja

I. IEVADS

1. 2017. gada 13. septembrī saistībā ar savu digitālā vienotā tirgus stratēģiju Komisija pieņēma un nosūtīja Padomei un Eiropas Parlamentam iepriekš minēto priekšlikumu [1], kura juridiskais pamats ir LESD 114. pants. Priekšlikums ietilpst tā dēvētajā kiberdrošības paketē, un tā mērķis ir nodrošināt augsta līmeņa kiberdrošību, kibernoturību un uzticēšanos Savienībā nolūkā panākt iekšējā tirgus pienācīgu darbību.

2. Ierosinātajā regulā ir izklāstīti ES Kiberdrošības aģentūras jeb *ENISA* mērķi, uzdevumi un organizatoriskie aspekti un tiek radīts satvars Eiropas kiberdrošības sertifikācijas shēmu iedibināšanai nolūkā nodrošināt pienācīgu kiberdrošības līmeni IKT produktiem un pakalpojumiem Savienībā. Komisijas priekšlikumam ir pievienots ietekmes novērtējums, kurā iztirzāts konkrēts astoņu iespējamo politikas variantu kopums un iekļauts *ENISA* un IKT kiberdrošības sertifikācijas pārskats.

3. Ierosinātajā regulā ir divi galvenie virzieni:

   - pastāvīgs pilnvarojums Aģentūrai ar konkrētu darbības jomu, ņemot vērā vajadzības jaunu politisko prioritāšu un instrumentu apstākļos, un atjaunināts uzdevumu un funkciju kopums Aģentūrai, lai tā varētu efektīvi un ražīgi sniegt atbalstu dalībvalstīm ES iestādēm un citām ieinteresētajām personām nolūkā nodrošināt drošu kibertelpu;

   - Eiropas kiberdrošības sertifikācijas satvars IKT produktiem un pakalpojumiem un noteikumi, ar ko regulē Eiropas kiberdrošības sertifikācijas shēmas un rada iespēju, ka šādu shēmu ietvaros izdotie sertifikāti ir derīgi un atzīti visās dalībvalstīs, kā arī noteikumi, ar ko tiek novērsta pašreizējā tirgus sadrumstalotība.

[1] Dok. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. 2017. gada oktobrī Eiropadome [2] aicināja, lai Komisijas priekšlikumi kiberdrošības jomā tiktu izstrādāti holistiski, iesniegti laicīgi un izskatīti bez vilcināšanās, pamatojoties uz Padomes sagatavotu rīcības plānu.

5. 2017. gada 12. decembrī Vispārējo lietu padome pieņēma Rīcības plānu [3], lai īstenotu Padomes secinājumus [4] par kopīgo paziņojumu [5] Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību". Rīcības plānā tika minēts Padomes mērķis panākt vispārēju pieeju par priekšlikumu līdz 2018. gada jūnijam.

6. Eiropas Parlamentā par referenti ir izraudzīta *Angelika NIEBLER* (*ITRE*, *PPE*). Balsojums *ITRE* komitejā ir plānots 2018. gada 19. jūnijā.

7. Eiropas Ekonomikas un sociālo lietu komiteja savu atzinumu pieņēma 2018. gada 14. februārī.

II. DARBS PADOMĒ

8. Komisija šo priekšlikumu un tā ietekmes novērtējumu iesniedza Kiberjautājumu horizontālajai darba grupai (turpmāk "darba grupa") 2017. gada 26. septembrī, kam sekoja ietekmes novērtējuma izskatīšana darba grupā 2017. gada 20. oktobrī. Turpmākās diskusijas koncentrējās uz Aģentūras operatīvajām spējām un to, cik plaša būtu mijiedarbība ar valstu kompetentajām iestādēm, kā arī uz to, kā sertifikācijas satvars ietekmēs tirgu un uzņēmumu konkurētspēju. Kopumā par ietekmes novērtējumu un priekšlikumu tika saņemtas labas atsauksmes no delegācijām.

---

[2] EUCO 14/17, 11. punkts
[3] Dok. 15748/17.
[4] Dok. 14435/17.
[5] Dok. 12211/17.

9. Diskusija par pašu priekšlikumu darba grupā sākās 2017. gada novembrī Igaunijas prezidentūras laikā un turpinājās Bulgārijas prezidentūras laikā. Par priekšlikumu tika sarīkotas 12 sanāksmes, kā rezultātā viena pēc otras tika izstrādātas astoņas pārskatītas priekšlikuma versijas, lai par vispārēju pieeju varētu vienoties gaidāmajā TTE (Telekomunikācijas) padomē, kura plānota 2018. gada 8. jūnijā.

10. Iznākums darba grupas diskusijām 2018. gada 14. un 15. maija sanāksmē, kā arī pārskatītais prezidentvalsts kompromisa teksts ir pievienoti šīs piezīmes pielikumā. Apsvērumi tika pielāgoti, lai atspoguļotu izmaiņas normatīvajā daļā. Visas izmaiņas salīdzinājumā ar Komisijas priekšlikumu ir norādītas **treknrakstā** vai ar [...]. Izmaiņas salīdzinājumā ar jaunāko darba grupas dokumentu 8834/18 ir norādītas **pasvītrotā treknrakstā**, un svītrojumi – ar **[...]**.

III. NOBEIGUMS

11. Pielikumā izklāstītais prezidentvalsts kompromisa teksts atspoguļo prezidentvalsts un dalībvalstu centienus tekstā panākt pienācīgu līdzsvaru.

12. 2018. gada 25. maijā Pastāvīgo pārstāvju komiteja panāca vienošanos par prezidentvalsts kompromisa tekstu, ar nosacījumu, ka tiks grozīts 19. panta 5. punkts un 48. panta 5. punkts, kā izklāstīts pielikumā.

13. Tāpēc Padome tiek aicināta 2018. gada 8. jūnija sanāksmē pieņemt vispārēju pieeju un pilnvarot prezidentvalsti sākt sarunas par šo dosjē ar Eiropas Parlamenta un Eiropas Komisijas pārstāvjiem.

PIELIKUMS

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par *ENISA – [...] Eiropas Savienības Kiberdrošības aģentūru* – un Regulas (ES) 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju ("Kiberdrošības akts")

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu [6],

ņemot vērā Reģionu komitejas atzinumu [7],

saskaņā ar parasto likumdošanas procedūru,

[6] OV C , , . lpp.
[7] OV C , , . lpp.

tā kā:

(1) Tīklu un informācijas sistēmām un telesakaru tīkliem un pakalpojumiem ir būtiska nozīme sabiedrības dzīvē, un tie ir kļuvuši par ekonomikas izaugsmes pamatu. Informācijas un komunikācijas tehnoloģijas tiek izmantotas tādu kompleksu sistēmu pamatā, kuras ļauj mums īstenot sabiedrisko darbību; tās uztur saimniecisko darbību tādās nozīmīgās nozarēs kā veselības aprūpe, enerģētika, finanses un transports un jo īpaši atbalsta iekšējā tirgus darbību.

(2) Iedzīvotāji, uzņēmumi un valdības plaši izmanto tīklu un informācijas sistēmas visā ES teritorijā. Digitalizācija un savienojamība kļūst par galvenajiem elementiem aizvien plašākajā produktu un pakalpojumu klāstā, un, attīstoties lietu internetam (*IoT*), paredzams, ka tuvākajos desmit gados visā ES izmantos miljoniem vai pat miljardiem satīkloto digitālo ierīču. Lai gan internetam pieslēgto ierīču kļūst aizvien vairāk, drošība un noturība nav pietiekami integrēta un līdz ar to arī kiberdrošības līmenis nav pietiekami augsts. Šādos apstākļos, ja sertifikācijas izmantošana ir ierobežota, ne organizācijas, ne individuālie lietotāji nav pietiekami informēti par IKT produktu un pakalpojumu kiberdrošības aspektiem, un tas savukārt mazina uzticēšanos digitālajiem risinājumiem.

(3) Aizvien plašākā digitalizācija un satīklojamība rada arī lielākus kiberdrošības riskus, tādējādi sabiedrību kopumā padarot mazāk aizsargātu pret kiberdraudiem un palielinot briesmas, ar ko saskaras iedzīvotāji, tostarp tādas neaizsargātas personas kā bērni. Lai mazinātu šo risku, kam pakļauta sabiedrība, ir jāveic visi vajadzīgie pasākumi, kuru mērķis ir uzlabot kiberdrošību Eiropas Savienībā, lai tādējādi tīklu un informācijas sistēmas, telesakaru tīklus, digitālos produktus, pakalpojumus un ierīces, ko izmanto iedzīvotāji, valdības un uzņēmumi (no MVU līdz pat kritiskās infrastruktūras apsaimniekotājiem), labāk aizsargātu pret kiberdraudiem.

(4) Kiberuzbrukumi kļūst aizvien biežāki, tāpēc satīklotai ekonomikai un sabiedrībai, kas ir mazāk aizsargāta pret kiberdraudiem un uzbrukumiem, ir vajadzīga spēcīgāka aizsardzība. Tomēr, lai gan kiberuzbrukumi bieži notiek pāri robežām, kiberdrošības iestādes politikas risinājumus un tiesībaizsardzības iestādes pilnvaras pārsvarā var īstenot tikai konkrētā valstī. Plašapmēra kiberincidenti var pārtraukt būtisku pakalpojumu sniegšanu visā ES. Tas rada vajadzību pēc efektīvas tādas ES līmeņa atbildes un krīzes pārvarēšanas, kuras pamatā izmantota specifiska politika un plašāka mēroga instrumenti Eiropas solidaritātes un savstarpējā atbalsta nodrošināšanai. Turklāt politikas veidotājiem, nozarei un lietotājiem ir svarīgi, lai kiberdrošības un noturības stāvoklis Savienībā tiktu regulāri izvērtēts, pamatojoties uz ticamiem Savienības līmeņa datiem, kā arī sistemātiski tiktu prognozēta turpmākā attīstība, problēmas un draudi gan Savienības, gan globālā līmenī.

(5) Ņemot vērā pieaugošās kiberdrošības problēmas, ar ko saskaras Savienība, ir jāizveido visaptverošs pasākumu kopums, kas papildinātu agrāko Savienības rīcību un palīdzētu sasniegt savstarpēji pastiprinošus mērķus. Tie cita starpā paredz vairāk uzlabot dalībvalstu un uzņēmumu spējas un sagatavotību, kā arī sekmēt sadarbību un koordināciju starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām. Turklāt, ņemot vērā kiberdraudu pārrobežu raksturu, ir jāpalielina spējas Savienības līmenī, kas varētu papildināt dalībvalstu rīcību, sevišķi plašapmēra pārrobežu kiberdrošības incidentu un krīžu gadījumā. Vajadzīgi arī papildu centieni, kas uzlabotu iedzīvotāju un uzņēmumu izpratni kiberdrošības jautājumos. Turklāt, sniedzot pārredzamu informāciju par IKT produktu un pakalpojumu drošības līmeni, jāpanāk lielāka uzticēšanās digitālajam vienotajam tirgum. To var veicināt ES mēroga sertifikācija, kuras ietvaros visos valstu tirgos un nozarēs tiktu izvirzītas vienotas kiberdrošības prasības un izvērtēšanas kritēriji.

(6) Eiropas Parlaments un Padome 2004. gadā pieņēma Regulu (EK) Nr. 460/2004 [8], ar ko izveido *ENISA*, lai tā sniegtu ieguldījumu ceļā uz augsta līmeņa tīklu un informācijas drošību Savienībā un palīdzētu attīstīt tīklu un informācijas drošības kultūru iedzīvotāju, patērētāju, uzņēmumu un valsts pārvaldes iestāžu interesēs. Vēlāk, 2008. gadā, Eiropas Parlaments un Padome pieņēma Regulu (EK) Nr. 1007/2008 [9], pagarinot Aģentūras pilnvaru termiņu līdz 2012. gada martam. Savukārt ar Regulu (EK) Nr. 580/2011 [10] Aģentūras pilnvaru termiņu pagarināja līdz 2013. gada 13. septembrim. 2013. gadā Eiropas Parlaments un Padome pieņēma Regulu (ES) Nr. 526/2013 [11] par *ENISA* un ar ko atceļ Regulu (EK) Nr. 460/2004; ar to Aģentūras pilnvaru termiņš tika pagarināts līdz 2020. gada jūnijam.

---

[8] Eiropas Parlamenta un Padomes Regula (EK) Nr. 460/2004 (2004. gada 10. marts), ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru (OV L 77, 13.3.2004., 1. lpp.).

[9] Eiropas Parlamenta un Padomes Regula (EK) Nr. 1007/2008 (2008. gada 24. septembris), ar kuru Regulu (EK) Nr. 460/2004, ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru, groza attiecībā uz aģentūras darbības termiņu (OV L 293, 31.10.2008., 1. lpp.).

[10] Eiropas Parlamenta un Padomes Regula (ES) Nr. 580/2011 (2011. gada 8. jūnijs), ar kuru Regulā (EK) Nr. 460/2004, ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru, izdara grozījumus attiecībā uz aģentūras darbības termiņu (OV L 165, 24.6.2011., 3. lpp.).

[11] Eiropas Parlamenta un Padomes Regula (ES) Nr. 526/2013 (2013. gada 21. maijs) par Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*) un ar ko atceļ Regulu (EK) Nr. 460/2004 (OV L 165, 18.6.2013., 41. lpp.).

(7) Savienība jau ir veikusi būtiskus pasākumus, lai nodrošinātu kiberdrošību un palielinātu uzticēšanos digitālajām tehnoloģijām. 2013. gadā tika pieņemta ES kiberdrošības stratēģija, lai veidotu uz kiberdraudiem un kiberriskiem vērstu Savienības politisko reakciju. Cenšoties uzlabot eiropiešu aizsardzību tiešsaistē, 2016. gadā Savienība pieņēma pirmo tiesību aktu kiberdrošības jomā, proti, Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā ("TID direktīva"). TID direktīvā ir ieviestas prasības attiecībā uz valstu spējām kiberdrošības jomā, izveidoti pirmie mehānismi dalībvalstu stratēģiskās un operatīvās sadarbības stiprināšanai un noteikti pienākumi attiecībā uz drošības pasākumiem un incidentu paziņošanu visās ekonomiski un sabiedriski nozīmīgās nozarēs, piemēram, enerģētikā, transporta, ūdensapgādes, banku, finanšu tirgus infrastruktūru, veselības aprūpes un digitālās infrastruktūras nozarē, kā arī pienākumi galvenajiem digitālo pakalpojumu sniedzējiem (meklētājprogrammas, mākoņdatošanas pakalpojumi un tiešsaistes tirdzniecības vietas). Lai atbalstītu šīs direktīvas īstenošanu, *ENISA* tika piešķirta būtiska nozīme. Turklāt rezultatīva cīņa pret kibernoziegumiem ir noteikta par svarīgu prioritāti Eiropas Drošības programmā, tādējādi palīdzot sasniegt vispārējo mērķi attiecībā uz augstu kiberdrošības līmeni.

(8) Ir atzīts, ka kopš ES kiberdrošības stratēģijas pieņemšanas 2013. gadā un Aģentūras pilnvaru pēdējās pārskatīšanas vispārējais politikas konteksts ir ievērojami mainījies, arī sakarā ar aizvien neskaidrāko un nedrošāko situāciju pasaules mērogā. Šajā sakarībā un saistībā ar jaunās Savienības kiberdrošības politikas izveidi ir jāpārskata *ENISA* pilnvaras, lai noteiktu tās uzdevumus mainītajā kiberdrošības ekosistēmā un nodrošinātu, ka tā sekmīgi palīdz rast Savienības risinājumus kiberdrošības problēmām, kas izriet no šīs radikāli pārveidotās apdraudējuma ainas, attiecībā uz kuru, kā atzīts Aģentūras izvērtējumā, tagadējais pilnvaru tvērums nav pietiekami plašs.

(9) Ar šo regulu izveidotajai Aģentūrai būtu jāpārņem ar Regulu (EK) Nr. 526/2013 izveidotās *ENISA* darbs. Aģentūrai būtu jāpilda pienākumi, kas tai uzticēti ar šo regulu un Savienības tiesību aktiem kiberdrošības jomā, un, to darot, cita starpā jādalās lietpratībā un jādod padomi, kā arī jādarbojas kā Savienības informācijas un zināšanu centram. Tai būtu jāveicina paraugprakses apmaiņa dalībvalstu un privāto ieinteresēto personu starpā, Eiropas Komisijai un dalībvalstīm izvirzot ierosinājumus politikas nostādnēm, darbojoties kā uzziņas punktam attiecībā uz Savienības nozaru politikas iniciatīvām kiberdrošības jautājumos un sekmējot operatīvo sadarbību gan starp dažādām dalībvalstīm, gan starp dalībvalstīm un Eiropas iestādēm, aģentūrām un struktūrām.

(10) Saskaņā ar Lēmumu 2004/97/EK, *Euratom*, kas tika pieņemts Eiropadomes 2003. gada 13. decembra sanāksmē, dalībvalstu pārstāvji nolēma, ka *ENISA* atrašanās vieta būs kādā no Grieķijas pilsētām, kuru izvēlēsies Grieķijas valdība. Aģentūras mītnes dalībvalstij būtu jānodrošina pēc iespējas labāki apstākļi Aģentūras netraucētai un efektīvai darbībai. Lai tā varētu pienācīgi un efektīvi veikt savus uzdevumus, pieņemt darbā darbiniekus un noturēt tos un lai uzlabotu tīklošanas darbību efektivitāti, Aģentūrai noteikti būtu jāatrodas piemērotā vietā, kurā cita starpā būtu nodrošināta pienācīga satiksme un darbinieku laulāto un bērnu vajadzību apmierināšana. Nepieciešamie pasākumi būtu jāparedz Aģentūras un mītnes dalībvalsts nolīgumā, ko noslēgtu pēc Aģentūras Administratīvās padomes apstiprinājuma saņemšanas.

(11) Ņemot vērā pieaugošās kiberdrošības problēmas, ar ko saskaras Savienība, būtu jāpalielina Aģentūrai piešķirtie finansiālie līdzekļi un cilvēkresursi, lai tie atbilstu tās paplašinātajai lomai un uzdevumiem, kā arī īpaši svarīgajai nozīmei Eiropas digitālās ekosistēmas aizsardzības organizāciju vidē.

(12) Aģentūrai būtu jāattīsta un jāsaglabā augsts lietpratības līmenis un jākļūst par uzziņas punktu, kas ar savu neatkarību, kvalitatīvu padomu un izplatīto informāciju, darba procedūru un darbības metožu pārredzamību un neatlaidību savu uzdevumu izpildē rada uzticēšanos vienotajam tirgum. Aģentūrai būtu **jāatbalsta** [...] valstu un **aktīvi jāveicina** Savienības centieni, pildot savus uzdevumus pilnīgā sadarbībā ar Savienības iestādēm, [...] aģentūrām **un struktūrām** un dalībvalstīm. Turklāt Aģentūrai būtu jāizmanto privātā sektora, kā arī citu attiecīgo ieinteresēto personu piedāvātais atbalsts un sadarbības iespējas. Aģentūras uzdevumu kopumam būtu jānosaka tās mērķu sasniegšanas veidi, vienlaikus ļaujot tai darboties elastīgi.

(13) Aģentūrai būtu jāpalīdz Komisijai ar padomiem, atzinumiem un analīzi visos Savienības jautājumos saistībā ar politikas un tiesību aktu izstrādi, atjaunināšanu un pārskatīšanu kiberdrošības **un tās ar konkrētām nozarēm saistītajos aspektos nolūkā palielināt ES politikas un tiesību aktu ar kiberdrošības dimensiju nozīmīgumu un ļautu panākt to īstenošanas konsekvenci valstu līmenī** [...]. Saistībā ar konkrētu nozaru Savienības politikas un tiesību aktu iniciatīvām, kurās ietverti ar kiberdrošību saistīti jautājumi, Aģentūrai vajadzētu darboties kā uzziņas punktam, kurā iespējams saņemt padomu un lietpratēju atzinumus.

(14) Aģentūras pamatuzdevums ir veicināt attiecīgā tiesiskā regulējuma konsekventu īstenošanu, jo īpaši TID direktīvas rezultatīvu īstenošanu, kas ir būtiski svarīga kibernoturības līmeņa paaugstināšanai. Ņemot vērā strauji mainīgo kiberdrošības apdraudējuma ainu, ir skaidrs, ka dalībvalstis ir jāatbalsta, palīdzot tām izstrādāt visaptverošu daudznozaru pieeju kibernoturības veidošanā.

(15) Aģentūrai būtu jāatbalsta dalībvalstu un Savienības iestāžu, [...] aģentūru **un struktūru** centieni veidot un uzlabot spējas un gatavību novērst un atklāt kiberdrošības [...] **draudus** un incidentus, un reaģēt uz tiem, kā arī saistībā ar tīklu un informācijas sistēmu drošību. Aģentūrai jo īpaši būtu jāatbalsta valstu *CSIRT* izveide un uzlabošana ar mērķi Savienībā tajās panākt vienādi augsta līmeņa gatavību. **Darbībām, ko *ENISA* veic saistībā ar dalībvalstu operatīvajām spējām, būtu vienīgi jāpapildina pašu dalībvalstu rīcība nolūkā pildīt to saistības, kas izriet no TID direktīvas, un tādējādi nevajadzētu tās pārsniegt** [...].

(15.a) Aģentūrai arī būtu jāpalīdz izstrādāt un atjaunināt Savienības un – pēc pieprasījuma – dalībvalstu tīklu un informācijas sistēmu drošības, jo īpaši kiberdrošības, stratēģijas, jāveicina to izplatīšana un jāseko to īstenošanai. Aģentūrai būtu arī jāpiedāvā publiskajām struktūrām apmācība un mācību materiāli un attiecīgā gadījumā "jāapmāca mācībspēki", tādējādi palīdzot dalībvalstīm attīstīt pašām savas apmācības spējas.

(16) Aģentūrai būtu jāpalīdz ar TID direktīvu izveidotajai Sadarbības grupai pildīt tās uzdevumus, jo īpaši daloties lietpratībā, sniedzot padomus un veicinot paraugprakses apmaiņu, jo īpaši attiecībā uz pamatpakalpojumu sniedzēju identifikāciju, ko veic dalībvalstis, un tostarp pievēršoties pārrobežu atkarībai saistībā ar riskiem un incidentiem.

(17) Lai sekmētu sadarbību starp publisko un privāto sektoru un starp privātā sektora dalībniekiem, [...] **Aģentūrai būtu jāatbalsta informācijas apmaiņa nozarēs un starp tām, jo īpaši nozarēs, kas uzskaitītas Direktīvas (ES) 2016/1148 II pielikumā, nodrošinot paraugpraksi un norādes par pieejamajiem rīkiem, procedūrām, kā arī sniedzot norādes, kā pievērsties regulatīviem problēmjautājumiem saistībā ar informācijas apmaiņu, piemēram, veicinot** [...] nozaru informācijas apmaiņas un analīzes centru (*ISAC*) izveidi [...].

(18) Aģentūrai, **lai palīdzētu dalībvalstīm** attiecībā uz informācijas apmaiņu ieviest kopīgas [...] **procedūras**, valodas lietojumu un terminoloģiju, būtu jāapkopo un jāanalizē valstu *CSIRT* un *CERT-EU* ziņojumi**, kas sniegti brīvprātīgā apmaiņā**. Aģentūrai būtu arī jāiesaista privātais sektors saistībā ar TID direktīvu, kurā izklāstīti iemesli brīvprātīgai tehniskās informācijas apmaiņai operatīvā līmenī [...] *CSIRT* tīkla **iekšienē**.

(19) Aģentūrai būtu jāpalīdz nodrošināt Savienības līmeņa reaģēšanu uz plašapmēra pārrobežu kiberdrošības incidentiem un krīzēm. Šī funkcija būtu **jāveic saskaņā ar tās pilnvarām, ievērojot šo Regulu, un ar pieeju, par kurām dalībvalstīm jāvienojas saistībā ar Komisijas Ieteikumu par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm**. **Pildot šo pienākumu,** Aģentūrai cita starpā būtu jāvāc attiecīgā informācija un jādarbojas kā starpniecei starp *CSIRT* tīklu un tehniskajiem speciālistiem, kā arī par krīžu pārvarēšanu atbildīgajiem lēmumu pieņēmējiem. Turklāt incidentu risināšanā Aģentūra varētu sniegt arī tehniska veida atbalstu, sekmējot attiecīgo tehnisko risinājumu apmaiņu starp dalībvalstīm un sniedzot ieguldījumu publisko sakaru jomā. Aģentūrai būtu jāatbalsta šis process, šādas sadarbības mehānismu pārbaudot [...] **regulārās** kiberdrošības mācībās.

(20) [...] **Sniedzot atbalstu** operatīvajai **sadarbībai** [...], Aģentūrai būtu jāizmanto pieejamā *CERT-EU* **tehniskā un operatīvā** lietpratība, izmantojot strukturētu sadarbību [...]. [...] Attiecīgā gadījumā starp abām organizācijām būtu jāpanāk īpaša vienošanās par šādas sadarbības praktiskas īstenošanas kārtību **un jāizvairās no darbību dublēšanās**.

(21) Atbilstīgi uzdevumiem [...] **atbalstīt operatīvo sadarbību *CSIRT* tīkla iekšienē** Aģentūrai būtu jāspēj sniegt atbalstu dalībvalstīm **pēc to pieprasījuma**, piemēram, sniedzot padomus **par to, kā uzlabot spējas novērst un atklāt incidentus un reaģēt uz tiem, atvieglojot** [...] tehniski **risināt incidentus, kam ir būtiska vai nozīmīga ietekme** [...] vai nodrošinot draudu un incidentu analīzi. **Tādu incidentu tehniskas risināšanas, kam ir būtiska vai nozīmīga ietekme, veicināšanā būtu jāiekļauj jo īpaši tas, ka *ENISA* atbalsta brīvprātīgu apmaiņu ar tehniskiem risinājumiem starp dalībvalstīm vai izstrādā apvienotu tehnisko informāciju, piemēram, tehniskus risinājumus, ko dalībvalstis sniedz brīvprātīgā apmaiņā.** Komisijas Ieteikumā par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm ieteikts dalībvalstīm godprātīgi sadarboties un bez liekas kavēšanās savā starpā un ar *ENISA* dalīties ar informāciju par plašapmēra kiberdrošības incidentiem un krīzēm. Šādai informācijai būtu vēl vairāk jāpalīdz *ENISA* [...] **operatīvās sadarbības atbalstīšanā**.

(22) Lai regulāras tehniskās sadarbības ietvaros veicinātu situācijas apzināšanos Savienībā, Aģentūrai regulāri **un ciešā sadarbībā ar dalībvalstīm** būtu jāsagatavo ES kiberdrošības tehniskās situācijas ziņojums par incidentiem un apdraudējumiem, kurš balstīts uz publiski pieejamu informāciju, Aģentūras veikto analīzi un ziņojumiem, ko tai [...] snieguši dalībvalstu *CSIRT* vai ar TID direktīvu izveidotie vienotie kontaktpunkti **(abos gadījumos – brīvprātīgi)**, Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), *CERT-EU* un – attiecīgā gadījumā – Eiropas Ārējās darbības dienesta (EĀDD) ES Izlūkdatu analīzes centrs (*INTCEN*). Ziņojums būtu jādara pieejams attiecīgajām Padomes un Komisijas struktūrām, Savienības Augstajam pārstāvim ārlietās un drošības politikas jautājumos un *CSIRT* tīklam.

(23) **Aģentūras atbalstā** *e[...]x-post* tehniskajai **izmeklēšanai** [...] par incidentiem, kam ir būtiska ietekme [...], kad to pieprasījusi [...] **attiecīgā** dalībvalsts, būtu jāorientējas uz turpmāku incidentu novēršanu [...]. **Attiecīgajām dalībvalstīm būtu jāsniedz nepieciešamā informācija, lai dotu Aģentūrai iespēju efektīvi atbalstīt tehnisko izmeklēšanu.**

(24) [...]

(25) Dalībvalstis var aicināt uzņēmumus, kurus skāris incidents, sadarboties un sniegt Aģentūrai nepieciešamo informāciju un palīdzību, neskarot to tiesības uz sensitīvas komercinformācijas aizsardzību.

(26) Lai labāk izprastu izaicinājumus kiberdrošības jomā un sniegtu stratēģiskus ilgtermiņa padomus dalībvalstīm un Savienības iestādēm, Aģentūrai ir jāanalizē pašreizējie un turpmākie riski. Šajā nolūkā Aģentūrai sadarbībā ar dalībvalstīm un vajadzības gadījumā ar statistikas un citām iestādēm būtu jāvāc attiecīga **publiski pieejama vai brīvprātīgi sniegta** informācija un jāanalizē jaunās tehnoloģijas, un jāveic novērtējumi par konkrētām tēmām saistībā ar tehnoloģiju inovāciju paredzamo sociālo, juridisko, ekonomisko un regulatīvo ietekmi tīklu un informācijas sistēmu drošības, jo īpaši kiberdrošības, jomā. Turklāt Aģentūrai, analizējot apdraudējumus un incidentus, būtu jāpalīdz dalībvalstīm un Savienības iestādēm, aģentūrām un struktūrām noteikt jaunās tendences un novērst [...] kiberdrošības **incidentus**.

(27) Lai palielinātu Savienības noturību, Aģentūrai, sniedzot padomus, norādījumus un paraugpraksi, būtu jāattīsta izcilība jautājumos par tādu **infrastruktūru kiber**drošību, **ar kurām jo īpaši atbalsta TID direktīvas II pielikumā uzskaitītās nozares un kuras izmanto digitālo pakalpojumu sniedzēji, kas ir uzskaitīti minētās direktīvas III pielikumā** [...]. Lai nodrošinātu vienkāršāku piekļuvi labāk strukturētai informācijai par kiberdrošības riskiem un iespējamiem risinājumiem, Aģentūrai būtu jāizveido un jāuztur Savienības "informācijas mezgls", kas darbotos kā vienots kontaktpunkts – portāls, kurā plašāka sabiedrība varētu iepazīties ar ES un dalībvalstu iestāžu, aģentūru un struktūru sniegto informāciju par kiberdrošību.

(28) Aģentūrai būtu jāpalīdz uzlabot sabiedrības izpratni par riskiem, kas saistīti ar kiberdrošību, un jāsniedz iedzīvotājiem un organizācijām adresēti norādījumi par labu praksi individuāliem lietotājiem. Aģentūrai arī būtu jāpalīdz veicināt paraugpraksi un risinājumus iedzīvotāju un organizāciju līmenī, apkopojot un analizējot publiski pieejamu informāciju par būtiskiem incidentiem, kā arī sagatavojot ziņojumus, kuros sniegti norādījumi uzņēmumiem un iedzīvotājiem, un uzlabojot vispārējo sagatavotības līmeni un noturību. Turklāt Aģentūrai sadarbībā ar dalībvalstīm un Savienības iestādēm, [...] aģentūrām **un struktūrām** būtu jāorganizē uz galalietotājiem vērstas regulāras informatīvās un sabiedrības izglītošanas kampaņas, kuru mērķis ir veicināt indivīdu tiešsaistes uzvedības drošākus paradumus un palielināt izpratni par potenciālajiem draudiem kibertelpā, tostarp par tādiem kibernoziegumiem kā personas datu izkrāpšanas jeb pikšķerēšanas uzbrukumi, botu tīkli, krāpšana finanšu un banku darījumos, kā arī sniegt pamatieteikumus attiecībā uz autentifikāciju un datu aizsardzību. Aģentūrai, straujāk uzlabojot galalietotāju izpratni par drošību ierīcēs, būtu jāuzņemas galvenā loma.

(29) Lai atbalstītu kiberdrošības nozares uzņēmumus, kā arī lietotājus, kas izmanto kiberdrošības risinājumus, Aģentūrai, regulāri analizējot kiberdrošības tirgus tendences gan no pieprasījuma, gan piedāvājuma viedokļa un izplatot šo informāciju, būtu jāizveido un jāuztur "tirgus novērošanas centrs".

(30) Lai nodrošinātu savu mērķu pilnīgu sasniegšanu, Aģentūrai būtu jāsadarbojas ar attiecīgām iestādēm, aģentūrām un struktūrām, tostarp *CERT-EU*, Eiropola Eiropas Kibernoziedzības apkarošanas centru (*EC3*) un Eiropas Aizsardzības aģentūras (EAA), Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai (*eu-LISA*), Eiropas Aviācijas drošības aģentūru (*EASA*), **Eiropas *GNSS* aģentūru** un citām ES aģentūrām, kas iesaistītas kiberdrošības jautājumu risināšanā. Tai būtu jāsadarbojas arī ar iestādēm, kuru pārziņā ir datu aizsardzība, šādā veidā apmainoties ar zinātību un paraugpraksi un sniedzot padomus par kiberdrošības aspektiem, kas varētu ietekmēt to darbu. Valstu un Savienības tiesībaizsardzības un datu aizsardzības iestāžu pārstāvjiem vajadzētu būt tiesīgiem piedalīties Aģentūras Pastāvīgajā ieinteresēto personu grupā. Sadarbojoties ar tiesībaizsardzības struktūrām attiecībā uz tīklu un informācijas drošības aspektiem, kas varētu ietekmēt viņu darbu, Aģentūrai būtu jāņem vērā pastāvošie informācijas kanāli un izveidotie tīkli.

(31) Aģentūrai **kā** [...] *CSIRT* tīkla sekretariātam būtu jāatbalsta dalībvalstu *CSIRT* un *CERT-EU* operatīvajā sadarbībā, un tas jādara papildus visiem attiecīgajiem *CSIRT* tīkla uzdevumiem, kas noteikti TID direktīvā. Turklāt Aģentūrai, vienlaikus pienācīgi ņemot vērā *CSIRT* tīkla darbības standartprocedūras, būtu jāveicina un jāatbalsta sadarbība starp attiecīgām *CSIRT* to pārvaldīto vai aizsargāto tīklu vai infrastruktūras incidentu, uzbrukumu vai traucējumu gadījumā, ja tas attiecas vai varētu attiekties vismaz uz divām *CERT*.

(32) Lai uzlabotu Savienības gatavību saistībā ar reaģēšanu uz kiberdrošības incidentiem, Aģentūrai būtu jāorganizē [...] **regulāras** kiberdrošības mācības Savienības līmenī un pēc pieprasījuma jāsniedz atbalsts mācību organizēšanā dalībvalstīm un ES iestādēm, aģentūrām un struktūrām.

(33) Aģentūrai būtu vēl vairāk jāattīsta un jāsaglabā sava lietpratība kiberdrošības sertifikācijas jautājumos, lai tā spētu atbalstīt Savienības politiku šajā jomā. Aģentūrai būtu jāveicina sertifikācijas ieviešana Savienībā, cita starpā palīdzot izveidot un uzturēt kiberdrošības sertifikācijas satvaru Savienības mērogā, lai uzlabotu IKT produktu un pakalpojumu kiberdrošības apliecinājuma pārredzamību un tādējādi stiprinātu uzticēšanos digitālajam iekšējam tirgum.

(34) Efektīvas kiberdrošības politikas pamatā gan publiskajā, gan privātajā sektorā vajadzētu būt labi izstrādātām riska izvērtēšanas metodēm. Riska izvērtēšanas metodes izmanto dažādos līmeņos, un nav vienotas efektīvas piemērošanas prakses. Ar riska izvērtēšanu un sadarbspējīgu riska pārvaldības risinājumu meklēšanu saistītas paraugprakses veicināšana un attīstīšana publiskā un privātā sektora organizācijās paaugstinās kiberdrošības līmeni Savienībā. Tādēļ Aģentūrai būtu jāatbalsta ieinteresēto personu sadarbība Savienības līmenī, palīdzot tām izveidot un pārņemt Eiropas un starptautiskos standartus, ko izmanto attiecībā uz elektronisko produktu, sistēmu, tīklu un pakalpojumu, kas kopā ar programmatūru veido tīkla un informācijas sistēmas, riska pārvaldību un drošības novērtēšanu.

(35) Aģentūrai būtu jāmudina dalībvalstis un pakalpojumu sniedzēji paaugstināt savus vispārīgos drošības standartus tā, lai visi interneta lietotāji varētu veikt nepieciešamos pasākumus paši savas kiberdrošības panākšanai. Konkrētāk, pakalpojumu sniedzējiem un produktu ražotājiem vajadzētu atsaukt vai pārstrādāt kiberdrošības standartiem neatbilstošus produktus un pakalpojumus. Sadarbībā ar kompetentajām iestādēm *ENISA* var izplatīt informāciju par iekšējā tirgū piedāvāto produktu un pakalpojumu kiberdrošības līmeni un izdot pakalpojumu sniedzējiem un ražotājiem brīdinājumus, kuros tos informē par prasību uzlabot savu produktu drošību, tostarp kiberdrošību.

(36) Aģentūrai būtu pilnībā jāņem vērā aktuālie pētniecības, izstrādes un tehnoloģiju izvērtēšanas pasākumi, jo īpašie tie, kas notiek saskaņā ar dažādām Savienības pētniecības iniciatīvām, lai Savienības iestādēm, [...] aģentūrām **un struktūrām**, kā arī attiecīgos gadījumos pēc pieprasījuma dalībvalstīm sniegtu padomus par vajadzību veikt pētījumus [...] kiberdrošības, jomā. **Nolūkā apzināt pētniecības vajadzības un prioritātes Aģentūrai būtu jāapspriežas arī ar attiecīgajām lietotāju grupām.**

(37) Kiberdrošības [...] **draudi** ir pasaules mēroga problēma. Lai uzlabotu **kiber**drošības standartus, tostarp definētu kopīgas uzvedības normas, un informācijas apmaiņu un veicinātu ātrāku starptautisko sadarbību atbildes pasākumu jomā, kā arī vienotu globālu pieeju tīklu un informācijas drošības jautājumiem, ir nepieciešams ciešāk sadarboties starptautiskā līmenī. Tādēļ Aģentūrai būtu jāatbalsta plašāka Savienības iesaistīšanās un sadarbība ar trešām valstīm un starptautiskām organizācijām, vajadzības gadījumā attiecīgām Savienības iestādēm, [...] aģentūrām **un struktūrām** sniedzot nepieciešamos lietpratības atzinumus un veicot analīzi.

(38) Aģentūrai būtu jāspēj reaģēt uz dalībvalstu un ES iestāžu, aģentūru un struktūru *ad hoc* pieprasījumiem pēc padomiem un palīdzības, kas atbilst Aģentūras mērķiem.

(39) Aģentūras pārvaldībā ir nepieciešams ieviest noteiktus principus saskaņā ar kopīgo paziņojumu un kopīgo pieeju, par ko 2012. gada jūlijā vienojās starpiestāžu darba grupa ES decentralizēto aģentūru jautājumos, kuras paziņojuma un pieejas mērķis ir pilnveidot aģentūru darbību un uzlabot to sniegumu. Kopīgais paziņojums un kopīgā pieeja attiecīgos gadījumos būtu jāatspoguļo arī Aģentūras darba programmās, izvērtējumos, kā arī pārskatu sniegšanas un administratīvajā praksē.

(40) Aģentūras Administratīvajai padomei, ko veidotu dalībvalstis un Komisija, būtu jānosaka Aģentūras darbības vispārīgais virziens un jāgādā, lai tā pildītu savus pienākumus saskaņā ar šo regulu. Aģentūras Administratīvā padome būtu jāpilnvaro izstrādāt budžetu, pārbaudīt tā izpildi, pieņemt atbilstošus finansiālos noteikumus, noteikt pārredzamas darba procedūras Aģentūras lēmumu pieņemšanai, apstiprināt Aģentūras vienoto programmdokumentu, pieņemt savu reglamentu, iecelt izpilddirektoru un lemt par izpilddirektora pilnvaru termiņa pagarināšanu un izbeigšanu.

(41) Lai Aģentūra darbotos pienācīgi un rezultatīvi, Komisijai un dalībvalstīm būtu jānodrošina, ka personām, kuras tiek ieceltas Administratīvajā padomē, ir atbilstoša profesionālā lietpratība un pieredze funkcionālajās jomās. Lai nodrošinātu Administratīvās padomes darba nepārtrauktību, Komisijai un dalībvalstīm būtu arī jācenšas ierobežot savu attiecīgo pārstāvju mainību Administratīvajā padomē.

(42) Lai Aģentūras darbība būtu sekmīga, tās izpilddirektors jāieceļ, ņemot vērā nopelnus un ar dokumentiem apliecinātas administratīvā un pārvaldības darba iemaņas, kā arī kompetenci un pieredzi kiberdrošības jomā, turklāt izpilddirektora pienākumi jāpilda pilnīgi neatkarīgi. Izpilddirektoram būtu jāsagatavo priekšlikums Aģentūras darba programmai, iepriekš apspriežoties ar Komisiju, un jāveic visi vajadzīgie pasākumi, lai nodrošinātu Aģentūras darba programmas pienācīgu izpildi. Izpilddirektoram būtu jāsagatavo un jāiesniedz Administratīvajai padomei gada darbības pārskata projekts, **tostarp par Aģentūras gada darba programmas īstenošanu**, jāizstrādā Aģentūras ieņēmumu un izdevumu tāmes projekts un jāizpilda budžets. Izpilddirektoram vajadzētu būt iespējai veidot *ad hoc* darba grupas, lai risinātu konkrētus jautājumus, jo īpaši zinātniskus, tehniskus, juridiskus vai sociālekonomiskus jautājumus. Izpilddirektoram būtu jāgādā, lai *ad hoc* darba grupu locekļi tiktu izraudzīti saskaņā ar augstākajiem lietpratības standartiem, nodrošinot dalībvalstu administrāciju, Savienības iestāžu un privātā sektora, tostarp nozares, lietotāju un tīklu un informācijas drošības jomas akadēmisko ekspertu pienācīgu pārstāvniecības līdzsvaru atbilstoši konkrēti risināmajiem jautājumiem.

(43) Valdei būtu jāpalīdz nodrošināt rezultatīvu Administratīvās padomes darbību. Veicot savu sagatavošanās darbu saistībā ar Administratīvās padomes lēmumiem, tai būtu detalizēti jāizvērtē attiecīgā informācija, jāapzina pieejamās iespējas un jāsniedz padomi un risinājumi attiecīgo Administratīvās padomes lēmumu sagatavošanai.

(44) Aģentūrā vajadzētu būt izveidotai Pastāvīgai ieinteresēto personu grupai, kas darbotos kā padomdevēja struktūra, kas uzturētu regulāru dialogu ar privāto sektoru, patērētāju organizācijām un citām attiecīgajām ieinteresētajām personām. Pastāvīgajai ieinteresēto personu grupai, ko pēc izpilddirektora priekšlikuma izveidotu Administratīvā padome, galvenokārt būtu jārisina ieinteresētajām personām svarīgi jautājumi un par tiem jāinformē Aģentūra. Pastāvīgā ieinteresēto personu grupa, ar kuru jāapspriežas, jo īpaši attiecībā uz [...] darba [...] programmas projektu, jāveido tā, lai tās sastāvs un tai uzdotie uzdevumi nodrošinātu pietiekami lielu ieinteresēto personu pārstāvību Aģentūras darbā.

(45) Aģentūrā vajadzētu būt ieviestiem noteikumiem par to, kā novērst un risināt interešu konfliktus. Aģentūrai būtu arī jāievēro atbilstīgi Savienības noteikumi par publisku piekļuvi dokumentiem, kā noteikts Eiropas Parlamenta un Padomes Regulā (EK) Nr. 1049/2001 [12]. Personas datu apstrādei Aģentūrā būtu jānotiek saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti [13]. Aģentūrai būtu jāievēro Savienības iestādēm piemērojamie noteikumi un valstu tiesību akti, kas attiecas uz rīkošanos ar datiem, jo īpaši sensitīvu, bet neklasificētu informāciju un ES klasificētu informāciju.

---

[12] Eiropas Parlamenta un Padomes Regula (EK) Nr. 1049/2001 (2001. gada 30. maijs) par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem (OV L 145, 31.5.2001., 43. lpp.).

[13] OV L 8, 12.1.2001., 1. lpp.

(46) Lai garantētu Aģentūras pilnīgu autonomiju un neatkarību un ļautu tai veikt papildu un jaunus uzdevumus, tostarp neparedzētus ārkārtas uzdevumus, būtu jāpiešķir Aģentūrai pietiekams un atsevišķs budžets, kura ieņēmumus veidotu galvenokārt Savienības un Aģentūras darbā iesaistīto trešo valstu iemaksas. Lielākajai daļai Aģentūras darbinieku vajadzētu būt tieši iesaistītai Aģentūras pilnvaru īstenošanā saistībā ar darbību. Mītnes dalībvalstij vai jebkurai citai dalībvalstij vajadzētu būt iespējai veikt brīvprātīgas iemaksas Aģentūras budžetā. Savienības budžeta procedūru būtu jāturpina piemērot attiecībā uz visām subsīdijām, ko piešķir no Savienības vispārējā budžeta. Turklāt Revīzijas palātai būtu jāveic Aģentūras finanšu pārskatu revīzija, lai nodrošinātu pārredzamību un pārskatatbildību.

(47) [...]

(48) Kiberdrošības sertifikācija ir būtiska, lai vairotu uzticēšanos IKT produktiem un pakalpojumiem un to drošību. Digitālais vienotais tirgus, jo īpaši datu ekonomika un lietu internets, var attīstīties vienīgi tad, ja plašai sabiedrībai ir pārliecība par to, ka šiem produktiem un pakalpojumiem ir nodrošināta noteikta līmeņa kiberdrošība. Satīklotās un automatizētās automašīnas, elektroniskās medicīniskās ierīces, ražošanas automatizācijas vadības sistēmas vai viedtīkli – tie ir tikai daži to nozaru piemēri, kurās jau tagad plaši izmanto sertifikāciju vai kurās to varētu izmantot tuvākajā nākotnē. Arī TID direktīvas reglamentētajās nozarēs kiberdrošības sertifikācijai ir izšķiroša nozīme.

(49) 2016. gada paziņojumā "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari" Komisija uzsvēra nepieciešamību pēc augstas kvalitātes, cenas ziņā pieejamiem un sadarbspējīgiem kiberdrošības produktiem un risinājumiem. IKT produktu un pakalpojumu piedāvājums vienotajā tirgū joprojām ir ļoti sadrumstalots ģeogrāfiskajā ziņā. Tas noticis tādēļ, ka kiberdrošības nozare Eiropā lielā mērā ir veidojusies atbilstīgi valsts pieprasījumam. Turklāt kiberdrošības jomā vienotajā tirgū ir arī citas nepilnības, piemēram, trūkst sadarbspējīgu risinājumu (tehniskie standarti), nav pietiekamas sertifikācijas prakse un ES mēroga sertifikācijas mehānismu. No vienas puses, tas Eiropas uzņēmumiem apgrūtina iespēju kļūt konkurētspējīgiem valsts, Eiropas un pasaules mērogā. No otras puses, tiek samazināts privātpersonām un uzņēmumiem pieejamo derīgo un izmantojamo kiberdrošības tehnoloģiju klāsts. Līdzīgi, digitālā vienotā tirgus stratēģijas īstenošanas vidusposma pārskatā Komisija ir uzsvērusi vajadzību pēc drošiem satīklotiem produktiem un sistēmām, un norādījusi, ka tāda Eiropas IKT drošības satvara izveide, kas paredz noteikumus par IKT drošības sertifikācijas organizēšanu Savienībā, varētu gan saglabāt uzticēšanos internetam, gan atrisināt pašreizējo kiberdrošības tirgus sadrumstalotības problēmu.

(50) Pašlaik IKT **procesu**, produktu un pakalpojumu kiberdrošības sertifikācija tiek izmantota visai ierobežoti. Ja arī tā ir ieviesta, galvenokārt tā tiek izmantota dalībvalstu līmenī vai konkrētu nozaru shēmās. Šādos apstākļos sertifikātu, ko izdevusi vienas valsts kiberdrošības iestāde, citas dalībvalstis principā neatzīst. Tādējādi šādiem uzņēmumiem var nākties sertificēt savus produktus un pakalpojumus vairākās dalībvalstīs, kurās tie darbojas, piemēram, ja tie vēlas piedalīties valsts iepirkuma procedūrās. Turklāt, lai gan tiek veidotas jaunas shēmas, šķiet, attiecībā uz horizontāliem kiberdrošības jautājumiem, piemēram, lietu interneta jomā, nav saskaņotas un visaptverošas pieejas. Esošajām shēmām ir ievērojami trūkumi un atšķirības tādos aspektos kā produktu klāsts, apliecinājuma līmeņi, būtiskie kritēriji un faktiskais izmantojums.

(51) Iepriekš ir bijuši zināmi centieni Eiropā panākt sertifikātu savstarpēju atzīšanu. Tomēr tie bijuši tikai daļēji sekmīgi. Visspilgtākais piemērs šajā sakarā ir Augstāko amatpersonu grupa informācijas sistēmu drošības (*SOG-IS*) Savstarpējās atzīšanas nolīguma (SAN) jautājumos. *SOG-IS* ir visnozīmīgākais sadarbības un savstarpējās atzīšanas modelis drošības sertifikācijas jomā, tomēr [...] tajā ir iekļauta tikai daļa Savienības dalībvalstu. Ņemot vērā iekšējā tirgus aspektu, tas ir ierobežojis *SOG-IS* SAN rezultativitāti.

(52) Tādējādi, ņemot vērā iepriekšminēto, ir jāizveido Eiropas kiberdrošības sertifikācijas satvars, kas nosaka galvenās horizontālās prasības izstrādājamajām Eiropas kiberdrošības sertifikācijas shēmām un pieļauj IKT produktu un pakalpojumu sertifikātu **un ES atbilstības apliecinājumu** atzīšanu un izmantošanu visās dalībvalstīs. Eiropas satvars būtu jāveido atbilstīgi divējādam mērķim – pirmkārt, tam būtu jāsekmē lielāka uzticēšanās atbilstīgi šādām shēmām sertificētiem IKT produktiem un pakalpojumiem un, otrkārt, tam būtu jāpalīdz izvairīties no valsts kiberdrošības sertifikācijas shēmu aizvien izplatītākā pretrunīguma vai pārklāšanās un tādējādi samazināt to uzņēmumu izmaksas, kuri darbojas digitālajā vienotajā tirgū. Shēmām vajadzētu būt nediskriminējošām un balstītām uz starptautiskiem un/vai [...] **Eiropas** standartiem, taču tas neattiektos uz standartiem, kas ir nerezultatīvi vai nepietiekami atbilstoši, lai izpildītu ES leģitīmos mērķus šajā jomā.

(53) Komisijai vajadzētu būt pilnvarotai pieņemt Eiropas kiberdrošības sertifikācijas shēmas attiecībā uz konkrētām IKT **procesu,** produktu un pakalpojumu grupām. Šīs shēmas būtu jāīsteno un jāpārrauga valstu **kiberdrošības** sertifikācijas [...] iestādēm, un šajās shēmās izsniegtajiem sertifikātiem vajadzētu būt derīgiem un atzītiem visā Savienībā. Nozarē vai citās privātās organizācijās izmantotajām sertifikācijas shēmām nebūtu jāietilpst šīs regulas darbības jomā. Tomēr struktūras, kas izmanto šāda veida shēmu, var ierosināt Komisijai apsvērt iespēju to izmantot par pamatu un pēc tam to apstiprināt kā Eiropas shēmu.

(54) Šīs regulas noteikumiem nebūtu jāskar Savienības tiesību akti, kuros izklāstīti īpaši noteikumi par IKT produktu un pakalpojumu sertifikāciju. Konkrēti, Vispārīgajā datu aizsardzības regulā (VDAR) ir izklāstīti noteikumi par sertifikācijas mehānismu ieviešanu un datu aizsardzības zīmogiem un marķējumu, kam uzskatāmi jāparāda datu pārziņu un apstrādātāju veikto apstrādes darbību atbilstība minētajai regulai. Ar šādiem sertifikācijas mehānismiem un datu aizsardzības zīmogiem un marķējumiem vajadzētu būt nodrošinātai iespējai datu subjektam ātri novērtēt konkrētu produktu un pakalpojumu datu aizsardzības līmeni. Šī regula neskar datu apstrādes darbību sertifikāciju, arī tad, kad tādas darbības saskaņā ar VDAR ir iestrādātas produktos un pakalpojumos.

(55) Eiropas kiberdrošības sertifikācijas shēmas būtu jāveido ar mērķi nodrošināt, ka saskaņā ar šādu shēmu sertificēti IKT **procesi,** produkti un pakalpojumi atbilst noteiktajām prasībām [...] nolūkā [...] **aizsargāt** tādu glabāto, pārsūtīto vai apstrādāto datu vai saistīto funkciju, vai pakalpojumu pieejamību, autentiskumu, integritāti un konfidencialitāti, ko **visā to dzīves ciklā** piedāvā izmantot minētie produkti, procesi, pakalpojumi un sistēmas, vai kam, tos izmantojot, var piekļūt tā, kā paredzēts šajā regulā. Šajā regulā nav iespējams detalizēti izklāstīt visiem IKT **procesiem,** produktiem un pakalpojumiem piemērojamās kiberdrošības prasības. IKT **procesi,** produkti un pakalpojumi un ar tiem saistītās kiberdrošības vajadzības ir tik daudzveidīgas, ka ir ļoti grūti izstrādāt vispārīgas, visās jomās piemērojamas kiberdrošības prasības. Tādēļ sertifikācijas vajadzībām ir nepieciešams pieņemt plašu un vispārēju kiberdrošības jēdzienu, ko papildina konkrētu kiberdrošības mērķu kopums, kas jāņem vērā Eiropas kiberdrošības sertifikācijas shēmu izstrādē. Pēc tam saistībā ar katru Komisijas pieņemto sertifikācijas shēmu, piemēram, atsaucoties uz standartiem vai, **ja piemēroti standarti nav pieejami, –** tehniskajām specifikācijām, būtu jāprecizē kārtība, kādā minētie mērķi tiks sasniegti attiecībā uz konkrētiem IKT **procesiem,** produktiem un pakalpojumiem.

(55.a) Tehniskās specifikācijas, kas jāizmanto Eiropas kiberdrošības sertifikācijas shēmā, būtu nosakāmas, ievērojot Regulas (ES) 1025/2012 II pielikumā izklāstītos principus. Tomēr dažas novirzes no minētajiem principiem varētu uzskatīt par nepieciešamām pienācīgi pamatotos gadījumos, ja minētās tehniskās specifikācijas paredzēts izmantot Eiropas kiberdrošības sertifikācijas shēmā, kurā ir norāde uz augstu apliecinājuma līmeni. Iemesli šādām novirzēm ir jādara publiski pieejami.

(55.b) Sertificētais atbilstības novērtējums ir process, kurā tiek izvērtēts, vai noteiktās prasības attiecībā uz IKT procesu, produktu vai pakalpojumu ir izpildītas. Šo procesu veic neatkarīga trešā persona, kas nav produkta ražotājs vai pakalpojuma sniedzējs. Veiksmīgam IKT procesa, produkta vai pakalpojuma izvērtējuma procesam seko sertifikāta izdošanas process. Tas būtu uzskatāms par apstiprinājumu, ka attiecīgais izvērtējums ir veikts pienācīgi. Atkarībā no apliecinājuma līmeņa Eiropas kiberdrošības shēmai būtu jāparedz, vai sertifikātu izdod privāta vai publiska struktūra. Atbilstības novērtējums vai sertifikācija paši par sevi nevar garantēt, ka sertificēti IKT produkti un pakalpojumi ir kiberdroši. Tā drīzāk ir tāda procedūra un tehniskā metodika, kas apliecina, ka IKT produkti un pakalpojumi ir testēti un ka tie atbilst noteiktām kiberdrošības prasībām, kuras izklāstītas citur, piemēram, tehniskajos standartos.

(55.c) Sertifikātu lietotāju izvēlei attiecībā uz piemērotu sertifikācijas līmeni un ar to saistītajām drošības prasībām būtu jāpamatojas uz riska analīzi par attiecīgā IKT procesa, produkta vai pakalpojuma lietojumu. Apliecinājuma līmenim tātad vajadzētu būt samērojamam ar riska līmeni, kas saistīts ar IKT procesa, produkta vai pakalpojuma paredzamo lietojumu.

(55.d) Eiropas kiberdrošības sertifikācijas shēmā varētu paredzēt veikt atbilstības novērtējumu, par ko ir atbildīgs tikai pats IKT produktu ražotājs vai pakalpojumu sniedzējs (atbildības pašnovērtējums). Šādos gadījumos ir pietiekami, ja ražotājs vai pakalpojumu sniedzējs pats veic visas pārbaudes, lai nodrošinātu IKT procesa, produktu vai pakalpojumu atbilstību sertifikācijas shēmai. Šāds atbilstības novērtējums būtu uzskatāms par piemērotu IKT produktiem un pakalpojumiem ar zemu sarežģītības pakāpi (piemēram, vienkārša konstrukcija un ražošanas mehānisms), kas rada zemu risku sabiedrības interesēm. Turklāt atbilstības pašnovērtējumu varētu veikt tikai tādiem IKT produktiem un pakalpojumiem, kas atbilst pamata apliecinājuma līmenim.

(55.e) Eiropas kiberdrošības sertifikācijas shēmā varētu paredzēt gan IKT produktu un pakalpojumu sertifikāciju, gan to atbilstības pašnovērtējumu. Šādā gadījumā shēmā būtu jāparedz skaidri un saprotami līdzekļi, ar kuriem patērētāji vai citi lietotāji varētu atšķirt produktus un pakalpojumus, par kuru novērtējumu atbild ražotājs vai pakalpojumu sniedzējs, no produktiem un pakalpojumiem, kurus sertificē trešā persona.

(55.f) Atbilstības novērtēšanas procedūras ietvaros IKT produktu ražotājam vai pakalpojumu sniedzējam, kas veic atbilstības pašnovērtējumu, būtu jāsagatavo un jāparaksta ES atbilstības apliecinājums. ES atbilstības apliecinājums ir dokuments, kurā apliecināts, ka konkrēts IKT produkts vai pakalpojums atbilst shēmas prasībām. Sagatavojot un parakstot ES atbilstības apliecinājumu, ražotājs vai pakalpojumu sniedzējs uzņemas atbildību par IKT produkta vai pakalpojuma atbilstību shēmas juridiskajām prasībām. ES atbilstības apliecinājuma kopija būtu jāiesniedz valsts kiberdrošības sertifikācijas iestādei un *ENISA*.

(55.g) IKT produktu ražotājam vai pakalpojumu sniedzējam ES atbilstības apliecinājums un tehniskā dokumentācija par visu attiecīgo informāciju, kas saistīta ar IKT produktu vai pakalpojumu atbilstību shēmai, būtu jāglabā tā, lai tā būtu minētās valsts kiberdrošības sertifikācijas iestādes rīcībā uz laiku, kas noteikts konkrētajā Eiropas kiberdrošības sertifikācijas shēmā. Tehniskajā dokumentācijā būtu jānorāda piemērojamās prasības, un, ciktāl tas ir nepieciešams novērtēšanai, jāaptver IKT produkta vai pakalpojuma projektēšana, ražošana un ekspluatācija. Tehniskā dokumentācija būtu jāapkopo tā, lai būtu iespējams novērtēt IKT produkta vai pakalpojuma atbilstību attiecīgajām prasībām.

(55.h) Dalībvalstīm un ieinteresētajām organizācijām vajadzētu būt tiesīgām ierosināt Eiropas Kiberdrošības sertifikācijas grupai sagatavot kandidātshēmu. Ieinteresētās organizācijas ir nozares vai patērētāju pārstāvju organizācijas, tostarp tādu MVU organizāciju pārstāvji, kam ir pamatota interese konkrētas Eiropas kiberdrošības sertifikācijas shēmas izstrādē. Šādi ierosinājumi būtu jāizskata, ņemot vērā Eiropas Kiberdrošības sertifikācijas grupas izstrādātos kritērijus, izmantojot pamatnostādnes, kas balstītas uz pārredzamības, atvērtības, objektivitātes, konsensa, efektivitātes, nozīmīguma un saskaņotības principiem.

(56) Komisijai **un Grupai** vajadzētu būt pilnvarotai pieprasīt, lai *ENISA* **bez nepamatotas kavēšanās** sagatavo kandidātshēmas konkrētiem IKT **procesiem,** produktiem vai pakalpojumiem. Pēc tam, pamatojoties uz *ENISA* ierosināto kandidātshēmu, Komisijai vajadzētu būt pilnvarotai ar īstenošanas aktiem pieņemt Eiropas kiberdrošības sertifikācijas shēmu. Ņemot vērā šajā regulā noteikto vispārējo mērķi un drošības mērķus, Komisijas pieņemtās Eiropas kiberdrošības sertifikācijas shēmās būtu jānosaka minimālais elementu kopums, kas izmantojams attiecībā uz katras shēmu priekšmetu, tvērumu un darbību. Cita starpā šiem elementiem būtu jāietver kiberdrošības sertifikācijas tvērums un priekšmets, tostarp IKT **procesu,** produktu un pakalpojumu kategorijas, detalizēti noteiktas kiberdrošības prasības (piemēram, atsaucoties uz standartiem vai tehniskajām specifikācijām), specifiskie izvērtēšanas kritēriji un metodes, kā arī plānotais apliecinājuma līmenis (pamata, būtisks un/vai augsts) **un attiecīgā gadījumā – izvērtējuma līmeņi**.

(56.a) Eiropas sertifikācijas shēmas apliecinājums ir pamats pārliecībai, ka IKT process, produkts vai pakalpojums atbilst konkrētas Eiropas kiberdrošības sertifikācijas shēmas drošības prasībām. Lai nodrošinātu sertificētu IKT procesu, produktu un pakalpojumu satvara konsekvenci, Eiropas kiberdrošības sertifikācijas shēmā varētu noteikt apliecinājuma līmeņus Eiropas kiberdrošības sertifikātiem un ES atbilstības apliecinājumiem, ko izdod saskaņā ar minēto shēmu. Katrā sertifikātā varētu būt norādīts viens no apliecinājuma līmeņiem, proti, pamata, būtisks vai augsts, savukārt ES atbilstības apliecinājumā varētu norādīt tikai pamata apliecinājuma līmeni. Apliecinājuma līmeņi paredz atbilstošu izvērtēšanā ieguldāmā darba pakāpi [...] un tos raksturo, norādot ar to saistītām tehniskajām specifikācijām, standartiem un procedūrām, tostarp tehniskām kontrolēm, kuru mērķis ir mazināt vai novērst kiberdrošības incidentus. Katram apliecinājuma līmenim vajadzētu būt konsekventam dažādās nozaru jomās, kur sertifikācija tiek piemērotu.

(56.b) Eiropas kiberdrošības sertifikācijas shēmā var noteikt vairākus izvērtējuma līmeņus atkarībā no izmantotās izvērtēšanas metodikas stingrības un dziļuma, un tam būtu jāatbilst vienam no apliecinājuma līmeņiem un vajadzētu būt saistītam ar apliecinājuma komponentu piemērotu kombināciju. Visos apliecinājuma līmeņos IKT produktam vai pakalpojumam būtu jāietver virkne drošu funkciju, kā definēts shēmā, un tās cita starpā var būt: droša iepriekš iestatīta konfigurācija, parakstīts kods, drošas atjaunināšanas un ļaunprātīga ekspluatējuma mazināšanas iespējas un pilnvērtīga steka/kaudzes atmiņas aizsardzība. Minētām funkcijām vajadzētu būt izstrādātām un tās būtu jāuztur, izmantojot uz drošību orientētas izstrādes pieejas un ar tām saistītus rīkus, lai nodrošinātu, ka uzticami ir iestrādāti efektīvi mehānismi (gan programmatūras, gan aparatūras līmenī). Attiecībā uz pamata apliecinājuma līmeni izvērtējumā būtu jāvadās pēc vismaz šādiem apliecinājuma komponentiem: izvērtējumā būtu jāietver vismaz IKT produkta vai pakalpojuma tehniskās dokumentācijas pārskats, ko veic atbilstības novērtēšanas struktūra. Ja sertifikācija aptver IKT procesus, tehniskajā pārskatīšanā būtu jāizvērtē arī process, kas izmantots IKT produkta vai pakalpojuma projektēšanā, izstrādē un uzturēšanā. Gadījumos, kad Eiropas kiberdrošības sertifikācijas shēmā paredzēts atbilstības pašnovērtējums, vajadzētu pietikt ar to, ka ražotājs vai pakalpojuma sniedzējs ir veicis pašnovērtējumu par IKT procesa, produktu vai pakalpojumu atbilstību sertifikācijas shēmai. Attiecībā uz būtisku apliecinājuma līmeni izvērtējumā papildus pamata apliecinājuma līmenim būtu jāorientējas uz to, lai tiktu pārbaudīta vismaz IKT produkta vai pakalpojuma drošības funkciju atbilstību tā tehniskajai dokumentācijai. Attiecībā uz augstu apliecinājuma līmeni izvērtējumā papildus būtiskam apliecinājuma līmenim būtu jāorientējas uz to, lai tiktu veikta vismaz efektivitātes testēšana, kurā novērtē IKT produkta vai pakalpojuma drošības funkciju noturību pret sarežģītu kiberuzbrukumu veicējiem ar nozīmīgām prasmēm un resursiem.

(56.c) Gatavojot kandidātshēmu, *ENISA* būtu jāapspriežas ar visām attiecīgajām ieinteresētajām personām, piemēram, Eiropas standartizācijas organizācijām, attiecīgajām valstu iestādēm, organizācijām, kas balstās uz savstarpējās atzīšanas nolīgumiem, tādām kā *SOG-IS* SAN, MVU, patērētāju organizācijām, kā arī ieinteresētajām personām vides un sociālajā jomā.

(56.d) *ENISA* būtu jāuztur tīmekļa vietne, kurā sniedz informāciju par Eiropas kiberdrošības sertifikācijas shēmām un nodrošina tām publicitāti, un tajā cita starpā būtu jāiekļauj pieprasījumi par Eiropas kiberdrošības sertifikācijas kandidātshēmu, kā arī atsauksmes, kas saņemtas *ENISA* veiktajā apspriešanās procesā sagatavošanās posmā. Šādā tīmekļa vietnē būtu jāsniedz arī informācija par sertifikātiem un ES atbilstības apliecinājumiem, kas izdoti saskaņā ar šo regulu.

(57) Eiropas kiberdrošības sertifikācijas un **ES atbilstības apliecinājuma** izmantošanai būtu jāpaliek fakultatīvai, ja vien Savienības vai dalībvalstu tiesību aktos**, kas pieņemti saskaņā ar Savienības tiesību aktiem,** nav noteikts citādi. **Ja saskaņotu tiesību aktu nav, dalībvalstis var pieņemt valsts tehniskos noteikumus atbilstīgi Direktīvai (ES) 2015/1535, kurā paredzēta obligāta sertifikācija saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu. Dalībvalstis varētu izmantot arī Eiropas kiberdrošības sertifikāciju saistībā ar publisko iepirkumu un Direktīvu 2014/214/ES.** [...]

(57.a) Lai sasniegtu šīs regulas mērķus un izvairītos no iekšējā tirgus sadrumstalotības, valsts kiberdrošības sertifikācijas shēmām vai procedūrām, kas piemērojamas kādā Eiropas kiberdrošības sertifikācijas shēmā ietvertajiem IKT produktiem un pakalpojumiem, no Komisijas īstenošanas aktā noteiktas dienas vairs nevajadzētu būt spēkā. Arī dalībvalstīm vairs nebūtu jāievieš jaunas valsts sertifikācijas shēmas, kas paredz kiberdrošības sertifikācijas shēmas IKT produktiem un pakalpojumiem, uz kuriem jau attiecas spēkā esoša Eiropas kiberdrošības sertifikācijas shēma. Tomēr dalībvalstīm nevajadzētu liegt pieņemt vai saglabāt valsts sertifikācijas shēmas nacionālās drošības vajadzībām.

(58) Pēc Eiropas kiberdrošības sertifikācijas shēmas pieņemšanas IKT produktu izgatavotājiem un IKT pakalpojumu sniedzējiem būtu jābūt iespējai savu produktu vai pakalpojumu sertifikācijas pieteikumu iesniegt pašu izvēlētai atbilstības novērtēšanas struktūrai. Atbilstības novērtēšanas struktūras būtu jāakreditē akreditācijas struktūrai, ja tās atbilst dažām konkrētām šajā regulā izklāstītām prasībām. Akreditācija būtu jāpiešķir uz laikposmu, kas nav ilgāks par pieciem gadiem, un to varētu atjaunot ar tādiem pašiem nosacījumiem, ja atbilstības novērtēšanas struktūra ievēro prasības. Akreditācijas struktūrām atbilstības novērtēšanas struktūras akreditācija būtu **jāierobežo, jāaptur vai** jāatsauc, ja akreditācijas nosacījumi nav vai vairs netiek izpildīti vai ja atbilstības novērtēšanas struktūras veiktie pasākumi pārkāpj šo regulu.

(59) [...] Dalībvalstīm **[...] būtu jā**izraugās viena **vai vairākas** kiberdrošības sertifikācijas [...] **iestādes**, lai uzraudzītu atbilstību **no šīs regulas izrietošajiem pienākumiem**. **Ja kāda dalībvalsts uzskata par piemērotu, uzdevumus var noteikt jau esošām iestādēm. Dalībvalstīm arī vajadzētu būt iespējai, savstarpēji vienojoties ar citu dalībvalsti, izlemt par vienas vai vairāku uzraudzības iestāžu izraudzīšanos minētās citas dalībvalsts teritorijā. Iestādei jo īpaši būtu jāpārrauga IKT produktu ražotāju vai pakalpojumu sniedzēju, kas veic uzņēmējdarbību iestādes attiecīgajā teritorijā, pienākumus, kas saistīti ar ES atbilstības apliecinājumu, un jānodrošina šo pienākumu izpilde, jāpalīdz valsts akreditācijas struktūrām atbilstības novērtēšanas struktūru darbību pārraudzīšanā un uzraudzīšanā, nodrošinot tām lietpratību un attiecīgu informāciju, jāpilnvaro atbilstības novērtēšanas struktūras veikt to uzdevumus, ja tās ir izpildījušas shēmā izklāstītās papildu prasības, un jānovēro nozīmīgas norises kiberdrošības sertifikācijas jomā**[...]. Valstu **kiberdrošības** sertifikācijas [...] iestādēm būtu jāizskata sūdzības, ko fiziskas vai juridiskas personas iesniegušas saistībā ar **to izdotiem sertifikātiem vai atbilstības novērtēšanas struktūru izsniegtajiem sertifikātiem, kur norādīts augsts apliecinājuma līmenis** [...], pienācīgā mērā jāizmeklē sūdzības priekšmeti un samērīgā termiņā jāinformē sūdzības iesniedzējs par lietas virzību un izskatīšanas rezultātiem. Turklāt tām arī būtu jāsadarbojas ar citām valsts **kiberdrošības** sertifikācijas [...] iestādēm vai citām publiskām iestādēm, tostarp, daloties informācijā par IKT produktu un pakalpojumu iespējamu neatbilstību šās regulas prasībām vai konkrētām kiberdrošības shēmām.

(60) Lai nodrošinātu Eiropas kiberdrošības sertifikācijas satvara konsekventu piemērošanu, būtu jāizveido Eiropas Kiberdrošības sertifikācijas grupa ("Grupa"), kas sastāv no valstu **kiberdrošības** sertifikācijas [...] iestāžu **vai citu attiecīgu valstu iestāžu pārstāvjiem**. Grupas galvenais uzdevums būtu dot padomus un palīdzēt Komisijai tās darbā, lai nodrošinātu Eiropas kiberdrošības sertifikācijas satvara konsekventu īstenošanu un piemērošanu; palīdzēt Aģentūrai un ar to cieši sadarboties kiberdrošības sertifikācijas kandidātshēmu izveidē; ieteikt Komisijai, lai tā pieprasītu Aģentūrai izveidot Eiropas kiberdrošības sertifikācijas kandidātshēmu; un pieņemt **Aģentūrai** adresētus atzinumus **par kandidātshēmām un** Komisijai adresētus atzinumus, kas attiecas uz esošo Eiropas kiberdrošības sertifikācijas shēmu uzturēšanu un pārskatīšanu.

(60.a) Grupai būtu jāveicina labas prakses un lietpratības apmaiņa starp valstu kiberdrošības sertifikācijas iestādēm, kas atbild par atļauju izsniegšanu atbilstības novērtēšanas struktūrām un par sertifikātu izdošanu. Saistībā ar kandidātshēmas sagatavošanu un tās īstenošanu Grupai būtu jāatbild par salīdzinošās novērtēšanas mehānisma izstrādi struktūrām, kas izsniedz Eiropas kiberdrošības sertifikātus par augstu apliecinājuma līmeni. Šādos salīdzinošās novērtēšanas mehānismos jo īpaši būtu jāizvērtē, vai attiecīgajām struktūrām ir pienācīga lietpratība un vai tās veic uzdevumus saskaņoti. Salīdzinošās novērtēšanas rezultāti būtu jādara publiski pieejami. Šīs struktūras var pieņemt piemērotus pasākumus, lai pielāgotu savu praksi un lietpratību.

(61) Lai uzlabotu izpratni par topošajām ES kiberdrošības shēmām un sekmētu to atzīšanu, Eiropas Komisija var izdot tādas vispārīgas vai konkrētai nozarei paredzētas kiberdrošības vadlīnijas, piemēram, par labu kiberdrošības praksi vai atbildīgu rīcību kiberdrošības jomā, kuras akcentētu sertificētu IKT produktu un pakalpojumu izmantošanas labvēlīgo ietekmi.

(61.a) Lai vēl vairāk veicinātu tirdzniecību un, atzīstot, ka IKT piegādes ķēdes ir globālas, Savienība saskaņā ar LESD 218. pantu var slēgt savstarpējās atzīšanas nolīgumus par sertifikātiem, ko izdevušas shēmas, kuras izveidotas saskaņā ar Eiropas kiberdrošības sertifikācijas satvaru. Komisija, ņemot vērā *ENISA* un Eiropas Kiberdrošības sertifikācijas grupas padomus, var ieteikt attiecīgu sarunu sākšanu. Katrā shēmā būtu jāparedz konkrēti nosacījumi attiecībā uz savstarpējo atzīšanu ar trešām valstīm.

(62) [...]

(63) [...]

(64) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir Komisijai īstenošanas pilnvaras gadījumiem, kas paredzēti šajā regulā. Minētās pilnvaras būtu jāīsteno saskaņā ar Regulu (ES) Nr. 182/2011.

(65) Pārbaudes procedūra būtu jāizmanto, lai pieņemtu īstenošanas aktus par Eiropas kiberdrošības sertifikācijas shēmām, kas izmantojamas attiecībā uz IKT produktiem un pakalpojumiem; par kārtību, kādā Aģentūrai veicama [...] **izmeklēšana**; kā arī par tādu atbilstības novērtēšanas struktūru paziņojumu sniegšanas apstākļiem, veidu un kārtību, kurus Komisijai sniedz valsts **kiberdrošības** sertifikācijas [...] iestādes.

(66) Aģentūras darbība būtu jāizvērtē neatkarīgi. Izvērtējumā būtu jāņem vērā Aģentūras mērķu sasniegšana, tās darba prakse un uzdevumu būtiskums. Izvērtējumā būtu arī jānosaka Eiropas kiberdrošības sertifikācijas satvara ietekme, lietderība un efektivitāte.

(67) Regula (ES) Nr. 526/2013 būtu jāatceļ.

(68) Ņemot vērā to, ka šīs regulas mērķus nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet minētos mērķus var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai,

IR PIEŅĒMUŠI ŠO REGULU.

I SADAĻA
VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets un darbības joma

1. Lai nodrošinātu iekšējā tirgus pienācīgu darbību, vienlaikus cenšoties panākt augstu kiberdrošības, kibernoturības un uzticēšanās līmeni, šajā regulā ir:

a) noteikti *ENISA* – [...] **Eiropas Savienības Kiberdrošības** aģentūras (turpmāk "Aģentūra") – mērķi, uzdevumi un organizatoriskie aspekti, un

b) izklāstīts satvars, kurā jāizveido Eiropas kiberdrošības sertifikācijas shēmas, lai Savienībā IKT **procesu,** produktu un pakalpojumu jomā nodrošinātu pietiekami augstu kiberdrošības līmeni. Šādu satvaru piemēro, neskarot citu Savienības tiesību aktu īpašos noteikumus par fakultatīvu vai obligātu sertifikāciju.

2. **Šī regula neskar dalībvalstu kompetenci kiberdrošības jomā, un tā nekādā ziņā neskar darbības, kas attiecas uz sabiedrisko drošību, aizsardzību, valsts drošību, un valsts pasākumus krimināltiesību jomā.**

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "kiberdrošība" ietver visas darbības, kas jāveic, lai tīklu un informācijas sistēmas, to lietotājus un iesaistītās personas aizsargātu pret kiberdraudiem;

2) "tīklu un informācijas sistēma" ir sistēma Direktīvas (ES) 2016/1148 4. panta 1. punkta nozīmē;

3) "valsts tīklu un informācijas sistēmu drošības stratēģija" ir sistēma Direktīvas (ES) 2016/1148 4. panta 3. punkta nozīmē;

4) "pamatpakalpojumu sniedzējs" ir publiska vai privāta vienība, kas definēta Direktīvas (ES) 2016/1148 4. panta 4. punktā;

5) "digitālā pakalpojuma sniedzējs" ir Direktīvas (ES) 2016/1148 4. panta 6. punktā definēta juridiska persona, kas sniedz digitālo pakalpojumu;

6) "incidents" ir katrs notikums, kas definēts Direktīvas (ES) 2016/1148 4. panta 7. punktā;

7) "incidenta risināšana" ir procedūra, kas definēta Direktīvas (ES) 2016/1148 4. panta 8. punktā;

8) "kiberdraudi" ir jebkādi iespējami apstākļi vai notikums, kas var **radīt bojājumus vai traucējumus vai citādi** negatīvi ietekmēt tīklu un informācijas sistēmas, to lietotājus un iesaistītās personas;

9) "Eiropas kiberdrošības sertifikācijas shēma" ir Savienības līmenī noteikts visaptverošs noteikumu, tehnisko prasību, standartu un procedūru kopums, kas attiecas uz to informācijas un komunikācijas tehnoloģiju (IKT) **procesu,** produktu un pakalpojumu sertifikāciju **vai atbilstības novērtēšanu**, kuri ietilpst minētās konkrētās shēmas tvērumā;

9.a) "valsts kiberdrošības sertifikācijas shēma" ir visaptverošs noteikumu, tehnisko prasību, standartu un procedūru kopums, ko izstrādājusi un pieņēmusi valsts publiskā iestāde un kas attiecas uz to IKT procesu, produktu un pakalpojumu sertifikāciju vai atbilstības novērtēšanu, kuri ietilpst minētās konkrētās shēmas tvērumā;

10) "Eiropas kiberdrošības sertifikāts" ir dokuments, [...] kas apliecina, **ka ir izvērtēta attiecīgā** IKT **procesa**, produkta vai pakalpojuma [...] **atbilstība** konkrētajām Eiropas kiberdrošības sertifikācijas shēmā noteiktajām **drošības** prasībām;

11) "IKT produkts [...]" ir jebkurš tīklu un informācijas sistēmu elements vai elementu grupa;

11.a) "IKT pakalpojums" ir jebkurš pakalpojums, kas pilnībā vai galvenokārt sastāv no informācijas pārsūtīšanas, uzglabāšanas, izgūšanas vai apstrādes ar tīklu un informācijas sistēmu palīdzību;

11.b) "IKT process" ir jebkādu tādu darbību kopums, kuru mērķis ir izstrādāt, attīstīt, nodrošināt un uzturēt IKT produktu vai pakalpojumu;

12) "akreditācija" ir akreditācija, kas definēta Regulas (EK) Nr. 765/2008 2. panta 10. punktā;

13) "valsts akreditācijas struktūra" ir valsts akreditācijas struktūra, kas definēta Regulas (EK) Nr. 765/2008 2. panta 11. punktā;

14) "atbilstības novērtēšana" ir atbilstības novērtēšana, kas definēta Regulas (EK) Nr. 765/2008 2. panta 12. punktā;

15) "atbilstības novērtēšanas struktūra" ir atbilstības novērtēšanas struktūra, kas definēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā;

16) "standarts" ir standarts, kas definēts Regulas (ES) Nr. 1025/2012 2. panta 1. punktā;

16.a) "tehniskā specifikācija" ir dokuments, kurā noteiktas tehniskās prasības, kurām IKT procesam, produktam vai pakalpojumam ir jāatbilst;

16.b) "apliecinājuma līmenis" ir pamats paļauties, ka IKT process, produkts vai pakalpojums atbilst konkrētās Eiropas kiberdrošības sertifikācijas shēmas prasībām, un sniedz informāciju par to, kādā līmenī tas ir izvērtēts; apliecinājuma līmenis neliecina par paša IKT procesa, produkta vai pakalpojuma drošību.

II SADAĻA

ENISA – "[...] Eiropas Savienības Kiberdrošības aģentūra"

I NODAĻA

PILNVARAS UN MĒRĶI */.../*

3. pants

Pilnvaras

1. Aģentūra veic ar šo regulu tai uzticētos uzdevumus, lai [...] **visā** Savienībā veicinātu augstu kiberdrošības līmeni**, jo īpaši palīdzot dalībvalstīm un Savienības iestādēm, aģentūrām un struktūrām uzlabot kiberdrošību**. **Aģentūra ir uzziņas punkts, kurā Savienības iestādes, aģentūras un struktūras saņem padomu un lietpratēja atzinumu par kiberdrošību.**

2. Aģentūra pilda uzdevumus, kas tai noteikti Savienības tiesību aktos, kuros paredzēti pasākumi dalībvalstu kiberdrošības jomā izstrādāto normatīvo un administratīvo aktu tuvināšanai.

2.a Pildot savus uzdevumus, Aģentūra rīkojas neatkarīgi un maksimāli ņem vērā dalībvalstu attiecīgo iestāžu lietpratību, vienlaikus izvairoties no darbību dublēšanās.

3. [...]

4. pants

Mērķi

1. Aģentūra kiberdrošības jomā darbojas kā lietpratības centrs, kas ir neatkarīgs, nodrošina savu doto padomu, sniegtās palīdzības un izplatītās informācijas zinātnisko un tehnisko kvalitāti, darba procedūru un darbības metožu pārredzamību un apliecina neatlaidību savu uzdevumu izpildē.

2. Aģentūra palīdz Savienības iestādēm, aģentūrām un struktūrām, kā arī dalībvalstīm izstrādāt un īstenot ar kiberdrošību saistītu **Savienības** politiku, **tostarp nozaru politiku jautājumos, kas attiecas uz kiberdrošību**.

3. Aģentūra Savienībā atbalsta spēju veidošanu un uzlabo gatavību, palīdzot Savienības **iestādēm, aģentūrām un struktūrām, kā arī** dalībvalstīm un publiskajām un privātajām ieinteresētajām personām palielināt savu tīklu un informācijas sistēmu aizsardzību, attīstīt **un uzlabot kibernoturību un reaģēšanas spējas un attīstīt** prasmes un kompetenci kiberdrošības jomā [...].

4. Aģentūra ar kiberdrošību saistītos jautājumos veicina Savienības līmeņa sadarbību un koordināciju starp dalībvalstīm, Savienības iestādēm, aģentūrām un struktūrām un attiecīgām **privātām un publiskām** ieinteresētajām personām [...].

5. Aģentūra **sekmē** kiberdrošības spēju **uzlabošanu** [...] Savienības līmenī, lai dalībvalstīm [...] **palīdzētu** novērst kiberdraudus un reaģēt uz tiem, it īpaši pārrobežu incidentu gadījumā.

6. Aģentūra veicina sertifikācijas izmantošanu **nolūkā izvairīties no sertifikācijas shēmu sadrumstalotības ES. Aģentūra jo īpaši palīdz** [...] izveidot un uzturēt kiberdrošības sertifikācijas satvaru Savienības līmenī saskaņā ar šīs regulas III sadaļu, lai uzlabotu IKT produktu un pakalpojumu kiberdrošības apliecinājuma pārredzamību un tādējādi stiprinātu uzticēšanos digitālajam iekšējam tirgum.

7. Aģentūra sekmē iedzīvotāju un uzņēmumu dziļu izpratni ar kiberdrošību saistītos jautājumos.

IA NODAĻA
UZDEVUMI

5. pants

[...] ***Savienības politikas un tiesību aktu izstrāde un īstenošana***

Savienības politikas un tiesību aktu izstrādi un īstenošanu Aģentūra sekmē šādi:

1. galvenokārt ar saviem neatkarīgiem atzinumiem un priekšdarbiem palīdz un sniedz padomus par to, kā izstrādāt un pārskatīt Savienības politiku un tiesību aktus kiberdrošības jomā, kā arī ar konkrētām nozarēm saistītas politikas un tiesību aktu iniciatīvas, kas ietver ar kiberdrošību saistītus aspektus;

2. palīdz dalībvalstīm konsekventi īstenot Savienības politiku un tiesību aktus kiberdrošības jomā, īpaši saistībā ar Direktīvu (ES) 2016/1148, cita starpā sniedzot atzinumus, vadlīnijas, padomus un apmainoties ar paraugpraksi tādās jomās kā riska pārvaldība, ziņošana par incidentiem un informācijas apmaiņa, kā arī veicinot paraugprakses apmaiņu šajā jomā kompetento iestāžu starpā;

3. daloties lietpratībā un dodot padomus, sekmē Direktīvas (ES) 2016/1148 11. pantā minētās Sadarbības grupas darbu;

4. atbalsta:

   1) Savienības politikas izstrādi un īstenošanu elektroniskās identifikācijas un uzticamības pakalpojumu jomā, īpaši ar padomu un tehniskām vadlīnijām, kā arī sekmējot paraugprakses apmaiņu kompetento iestāžu starpā;

   2) elektronisko sakaru drošības līmeņa paaugstināšanu, cita starpā daloties lietpratībā un dodot padomus, kā arī veicinot paraugprakses apmaiņu kompetento iestāžu starpā;

5. atbalsta Savienības politikas pasākumu regulāru pārskatīšanu, sagatavojot gada pārskatu par attiecīgā tiesiskā regulējuma īstenošanu un vēršot uzmanību uz:

   a) dalībvalstu paziņojumiem par incidentiem, ko Sadarbības grupai sniedz vienotais kontaktpunkts saskaņā ar Direktīvas (ES) 2016/1148 10. panta 3. punktu;

   b) paziņojumiem par drošības pārkāpumiem vai integritātes zaudēšanu, par ko ziņots uzticamības pakalpojumu sniedzējiem; šos paziņojumus Aģentūrai iesniedz pārraudzības iestādes saskaņā ar Regulas (ES) Nr. 910/2014 19. panta 3. punktu;

   c) paziņojumiem par drošības **incidentiem** [...], ko nosūtījuši uzņēmumi, kuri nodrošina publiskos sakaru tīklus vai sniedz publiski pieejamus elektronisko sakaru pakalpojumus; tos Aģentūrai iesniedz kompetentās iestādes saskaņā ar [Direktīvas par Eiropas Elektronisko sakaru kodeksa izveidi] 40. pantu.

6. pants

[...] ***Spēju veidošana***

1. Aģentūra palīdz:

a) dalībvalstīm to centienos uzlabot **kiberdraudu** [...] un incidentu novēršanas, atklāšanas, analīzes un risināšanas spējas, sniedzot tām nepieciešamās zināšanas un daloties lietpratībā;

b) Savienības iestādēm, [...] aģentūrām **un struktūrām** to centienos uzlabot [...] **kiberdraudu** [...] un incidentu novēršanas, atklāšanas, analīzes un risināšanas spējas, **jo īpaši** sniedzot pienācīgu atbalstu Savienības iestāžu un aģentūru datorapdraudējumu reaģēšanas vienībai (*CERT-EU*);

c) dalībvalstīm pēc to pieprasījuma izveidot valstu datordrošības incidentu reaģēšanas vienības (*CSIRT*) atbilstoši Direktīvas (ES) 2016/1148 9. panta 5. punktam;

d) dalībvalstīm, pēc pieprasījuma, izstrādāt valstu tīklu un informācijas sistēmu drošības stratēģijas atbilstoši Direktīvas (ES) 2016/1148 7. panta 2. punktam; Aģentūra arī veicina minēto stratēģiju izplatīšanu un [...] **seko** to īstenošanas gaitai Savienībā, tādējādi sekmējot paraugprakses izveidi;

e) Savienības iestādēm izstrādāt un pārskatīt Savienības kiberdrošības stratēģijas, veicināt to izplatīšanu un uzraudzīt to īstenošanas gaitu;

f) paaugstināt valstu un Savienības *CSIRT* spēju līmeni, tostarp veicinot dialogu un informācijas apmaiņu, lai nodrošinātu, ka attiecībā uz nozares jaunākajiem sasniegumiem katra *CSIRT* atbilst kopīgam spēju minimumam un darbojas saskaņā ar paraugpraksi;

g) dalībvalstīm, organizējot [...] **regulāras** kiberdrošības mācības Savienības līmenī, kā minēts 7. panta 6. punktā, un sniedzot politikas ieteikumus, kuri sagatavoti, balstoties uz šo mācību izvērtējumu un tajās gūto pieredzi;

h) attiecīgajām publiskajām struktūrām, piedāvājot mācības par kiberdrošības jautājumiem, vajadzības gadījumā sadarbībā ar ieinteresētajām personām;

i) Sadarbības grupai, [...] **izmantojot** [...] paraugprakses apmaiņu, īpaši saistībā ar dalībvalstu veikto pamatpakalpojumu sniedzēju identifikāciju, arī attiecībā uz pārrobežu atkarību saistībā ar riskiem un incidentiem, kā tas paredzēts Direktīvas (ES) 2016/1148 11. panta 3. punkta l) apakšpunktā.

2. Aģentūra **atbalsta informācijas apmaiņu gan pašās nozarēs, gan nozaru starpā** [...], jo īpaši Direktīvas (ES) 2016/1148 II pielikumā uzskaitītajās nozarēs, nodrošinot paraugpraksi un norādījumus par pieejamiem rīkiem un procedūrām, kā arī par to regulatīvo jautājumu risināšanu, kuri saistīti ar informācijas apmaiņu.

7. pants

[...] ***Savienības līmeņa operatīvā sadarbība***

1. Aģentūra atbalsta operatīvo sadarbību starp **dalībvalstīm, Savienības iestādēm, aģentūrām un** [...] struktūrām un starp ieinteresētajām personām.

2. Aģentūra sadarbojas operatīvā līmenī un veido sinerģiju ar Savienības iestādēm, [...] aģentūrām **un struktūrām**, tostarp *CERT-EU*, dienestiem, kas darbojas kibernoziedzības apkarošanas jomā, un pārraudzības iestādēm, kuru pārziņā ir privātuma un personas datu aizsardzība, un šīs sadarbības mērķis ir risināt kopīgas problēmas, cita starpā šādi:

a) apmainoties ar zinātību un paraugpraksi;

b) sniedzot padomus un vadlīnijas par attiecīgiem ar kiberdrošību saistītajiem jautājumiem;

c) pēc apspriešanās ar Komisiju izveidojot praktiski izmantojamus mehānismus īpašu uzdevumu izpildei.

3. Aģentūra nodrošina *CSIRT* tīkla sekretariātu atbilstīgi Direktīvas (ES) 2016/1148 12. panta 2. punktam un**, pildot šo pienākumu,** [...] veicina informācijas apmaiņu un sadarbību starp tā locekļiem.

4. Aģentūra **atbalsta** [...] operatīvo sadarbību *CSIRT* tīkla ietvaros, dalībvalstīm **pēc to pieprasījuma** sniedzot atbalstu šādi:

a) dodot padomus par to, kā uzlabot to spējas novērst un atklāt incidentus un reaģēt uz tiem;

b) [...] **veicinot** tādu [...] incidentu, kam ir būtiska vai nozīmīga ietekme, tehnisko aspektu **risināšanu, tostarp jo īpaši atbalstot to, ka dalībvalstis brīvprātīgi apmainās ar tehniskiem risinājumiem**;

c) analizējot vājās vietas [...] un incidentus**;**

ca) palīdzot tādu incidentu, kam ir būtiska vai nozīmīga ietekme, *ex-post* tehniskajā izmeklēšanā, ievērojot Direktīvu (ES) 2016/1148,

Veicot šos uzdevumus, Aģentūra un *CERT-EU* īsteno strukturētu sadarbību, lai tādējādi gūtu labumu no sinerģijas **un izvairītos no darbību dublēšanās** [...].

5. [...]

[...]

6. Aģentūra organizē [...] **regulāras** kiberdrošības mācības Savienības līmenī un atbalsta dalībvalstis un ES iestādes, aģentūras un struktūras, pēc to pieprasījuma(-iem) organizējot mācības. **Šādas mācības Savienības līmenī var ietvert tehniskus, operatīvus vai stratēģiskus elementus** [...]. **Reizi divos gados organizē plašapmēra mācības, kurās ietver visus minētos elementus.** Aģentūra arī veicina nozaru kiberdrošības mācības un vajadzības gadījumā palīdz tās organizēt kopā ar attiecīgajām [...] **organizācijām, kuras var** piedalīties arī Savienības mēroga kiberdrošības mācībās.

7. **Ciešā sadarbībā ar dalībvalstīm** Aģentūra regulāri sagatavo ES kiberdrošības tehniskās situācijas ziņojumu par incidentiem un apdraudējumiem, kurš balstīts uz publiski pieejamo informāciju, Aģentūras veikto analīzi un ziņojumiem, ko tai cita starpā sniegušas: dalībvalstu *CSIRT* [...] vai ar TID direktīvu izveidotie vienotie kontaktpunkti (**abi uz brīvprātības pamata** [...]); Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), *CERT-EU*.

8. Aģentūra palīdz sagatavoties uz sadarbību balstītai reaģēšanai gan Savienības, gan dalībvalstu līmenī ar kiberdrošību saistītu plašapmēra pārrobežu incidentu vai krīžu gadījumos, galvenokārt:

   a) apkopojot no valstu avotiem saņemtus ziņojumus**, ar kuriem dalās brīvprātīgi,** lai tādējādi palīdzētu nonākt pie kopīgas situācijas apzināšanās;

   b) nodrošinot efektīvu informācijas plūsmu un aktivizācijas mehānismus, kas izmantojami starp *CSIRT* tīklu un tehnisko un politisko lēmumu pieņēmējiem Savienības līmenī;

c) [...] **pēc dalībvalstu pieprasījuma veicinot** incidenta vai krīzes tehnisko aspektu risināšanu, tostarp **jo īpaši** [...] **atbalstot** tehnisko risinājumu **brīvprātīgu** apmaiņu dalībvalstu starpā;

d) palīdzot **ES iestādēm, aģentūrām un struktūrām un – pēc pieprasījuma – dalībvalstīm** publiskot ar incidentu vai krīzi saistīto informāciju;

e) **pēc dalībvalstu pieprasījuma palīdzot tām** [...] testēt sadarbības plānus, kurus paredzēts izmantot reaģēšanā uz šādiem incidentiem vai krīzēm.

8. pants

*[...] **Tirgus, kiberdrošības sertifikācija un standartizācija***

Aģentūra:

a) atbalsta un veicina Savienības politikas izstrādi un īstenošanu saistībā ar IKT **procesu,** produktu un pakalpojumu kiberdrošības sertifikāciju, kā noteikts šīs regulas III sadaļā:

1) **sadarbībā ar nozares pārstāvjiem un** saskaņā ar šīs regulas 44. pantu sagatavojot Eiropas kiberdrošības sertifikācijas kandidātshēmas IKT **procesiem,** produktiem un pakalpojumiem;

2) palīdzot Komisijai nodrošināt Eiropas Kiberdrošības sertifikācijas grupas sekretariātu saskaņā ar šīs regulas 53. pantu;

3) sadarbībā ar valstu **kiberdrošības** sertifikācijas [...] iestādēm un nozares pārstāvjiem apkopojot un publicējot vadlīnijas un izstrādājot labu praksi saistībā ar IKT produktu un pakalpojumu kiberdrošības prasībām;

3.a) iesakot tehniskās specifikācijas, kas būtu piemērotas Eiropas Kiberdrošības sertifikācijas shēmu izstrādei, kā minēts 47. panta 1. punkta b) apakšpunktā, gadījumos, kad standarti nav pieejami;

3.b) apkopojot un publicējot vadlīnijas, kā arī pēc pieprasījuma sniedzot atbalstu dalībvalstīm, veicināt to, lai tiktu veidotas pietiekamas ar izvērtēšanas un sertifikācijas procesiem saistītās spējas;

b) palīdz izveidot un ieviest Eiropas un starptautiskos riska pārvaldības un IKT **procesu,** produktu un pakalpojumu drošības standartus [...]**;**

ba) sadarbībā ar dalībvalstīm sagatavo padomus un vadlīnijas par tehniskajām jomām, kas saistītas ar drošības prasībām pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, kā arī par jau spēkā esošajiem standartiem, tostarp dalībvalstu standartiem, kā tas noteikts Direktīvas (ES) 2016/1148 19. panta 2. punktā;

c) regulāri veicot aktuālāko kiberdrošības tirgus – gan pieprasījuma, gan piedāvājuma – tendenču analīzi un izplatot tās rezultātus, lai tādējādi sekmētu kiberdrošības tirgu Savienībā.

9. pants

[...] ***Zināšanas*** **un** ***informācija*** *[...]*

Aģentūra:

a) analizē jaunās tehnoloģijas un sagatavo novērtējumus par konkrētām tēmām saistībā ar tehnoloģiju inovāciju paredzamo sociālo, juridisko, ekonomisko un regulatīvo ietekmi kiberdrošības jomā;

b) veic kiberdrošības apdraudējumu un incidentu ilgtermiņa stratēģisko analīzi, lai apzinātu jaunās tendences un palīdzētu novērst kiberdrošības [...] **incidentus**;

c) sadarbībā ar ekspertiem no dalībvalstu iestādēm sniedz padomus un norādījumus un dalās ar paraugpraksi attiecībā uz tīklu un informācijas sistēmu drošību, jo īpaši [...] tādas infrastruktūras drošību, kas ir Direktīvas (ES) 2016/1148 II pielikumā minēto nozaru pamatā, **un tādas, ko izmanto minētās direktīvas III pielikumā uzskaitīto digitālo pakalpojumu sniedzēji**;

d) apkopo, kārto un īpaši izveidotā portālā dara publiski pieejamu informāciju par kiberdrošību, ko sniedz Savienības iestādes, aģentūras un struktūras, **un – uz brīvprātības pamata – dalībvalstis un privātas un publiskas ieinteresētās personas**;

e) [...]

f) vāc un analizē publiski pieejamu informāciju par būtiskiem incidentiem un sagatavo ziņojumus, kuros sniegti norādījumi uzņēmumiem un iedzīvotājiem visā Savienībā.

g) [...].

9.a pants

Izpratnes veicināšana un izglītošana

Aģentūra:

a) uzlabo sabiedrības izpratni par kiberdrošības riskiem un sniedz iedzīvotājiem un organizācijām adresētus norādījumus par labu praksi individuāliem lietotājiem;

b) ciešā sadarbībā ar dalībvalstīm, Savienības iestādēm, struktūrām, aģentūrām un nozares pārstāvjiem organizē regulāras informatīvas kampaņas, lai palielinātu kiberdrošību un uzlabotu tās pamanāmību Savienībā;

c) palīdz dalībvalstīm palielināt izpratni par kiberdrošību un veicināt izglītotību par kiberdrošības jautājumiem;

d) atbalsta ciešāku koordināciju un paraugprakses apmaiņu starp dalībvalstīm tādos jautājumos kā izglītotība par kiberdrošību un kiberdrošības izpratne, veicinot valsts izglītības kontaktpunktu tīkla izveidi un uzturēšanu.

10. pants

[...] ***Pētniecība un inovācija***

Saistībā ar pētniecību un inovāciju Aģentūra:

a) dod padomus Savienībai un dalībvalstīm par vajadzību veikt pētījumus kiberdrošības jomā un šādu pētījumu prioritātēm, lai tās varētu efektīvi reaģēt uz pašreizējiem un jauniem riskiem un apdraudējumiem, tostarp attiecībā uz jaunām un topošām informācijas un komunikācijas tehnoloģijām, un iedarbīgi izmantot riska novēršanas tehnoloģijas;

b) piedalās pētniecības un inovācijas finansēšanas programmu īstenošanas posmā vai iesaistās kā saņēmēja, ja Komisija ir deleģējusi attiecīgas pilnvaras.

11. pants

[...] ***Starptautiskā sadarbība***

Aģentūra atbalsta Savienības centienus sadarboties ar trešām valstīm un starptautiskām organizācijām, lai veicinātu starptautisko sadarbību ar kiberdrošību saistītos jautājumos, un šajā sakarībā tā:

a) vajadzības gadījumā piedalās starptautisku mācību organizēšanas novērošanā, analizējot šādu mācību rezultātus un ziņojot par tiem Administratīvajai padomei;

b) [...] veicina paraugprakses apmaiņu **attiecīgajos starptautiskās sadarbības satvaros** [...];

c) pēc pieprasījuma sniedz Komisijai lietpratēju atzinumus**;**

ca) sadarbībā ar Eiropas Kiberdrošības sertifikācijas grupu, kas izveidota saskaņā ar 53. pantu, sniedz padomus un atbalstu Komisijai par jautājumiem, kas saistīti ar nolīgumiem, ko par kiberdrošības sertifikātu savstarpēju atzīšanu slēdz ar trešām valstīm.

II NODAĻA
AĢENTŪRAS ORGANIZĀCIJA

12. pants

Struktūra

Aģentūras administratīvo un pārvaldības struktūru veido:

a) Administratīvā padome, kas pilda 14. pantā izklāstītās funkcijas;

b) Valde, kas pilda 18. pantā aprakstītās funkcijas;

c) izpilddirektors, kas pilda 19. pantā izklāstītos pienākumus; [...]

d) Pastāvīgā ieinteresēto personu grupa, kas pilda 20. pantā izklāstītās funkcijas**;**

da) valsts sadarbības koordinatoru tīkls, kas pilda 20.a pantā izklāstītās funkcijas.

1. IEDAĻA
ADMINISTRATĪVĀ PADOME

13. pants

Administratīvās padomes sastāvs

1. Administratīvajā padomē ir pa vienam pārstāvim no katras dalībvalsts un divi pārstāvji, kurus ieceļ Komisija. Balsstiesības ir visiem pārstāvjiem.

2. Katram Administratīvās padomes loceklim ir aizstājējs, kas viņu pārstāv prombūtnes gadījumā.

3. Administratīvās padomes locekļus un viņu aizstājējus ieceļ, pamatojoties uz viņu zināšanām kiberdrošības jomā un ņemot vērā arī attiecīgās pārvaldības, administratīvās un budžeta veidošanas prasmes. Komisija un dalībvalstis cenšas ierobežot savu pārstāvju mainību Administratīvajā padomē, lai nodrošinātu Administratīvās padomes darba nepārtrauktību. Komisija un dalībvalstis tiecas panākt, lai Administratīvajā padomē būtu līdzsvarota vīriešu un sieviešu pārstāvība.

4. Administratīvās padomes locekļu un viņu aizstājēju pilnvaru termiņš ir četri gadi. Minēto pilnvaru termiņu var pagarināt.

14. pants

Administratīvās padomes funkcijas

1. Administratīvā padome:

a) nosaka Aģentūras darbības vispārīgo virzienu un gādā arī par to, lai tā darbotos saskaņā ar šajā regulā paredzētajiem noteikumiem un principiem. Tā arī nodrošina Aģentūras darbības saskaņotību ar dalībvalstu un Savienības līmeņa pasākumiem;

b) pieņem 21. pantā minētā Aģentūras vienotā programmdokumenta projektu un pēc tam iesniedz to Komisijai, lai saņemtu tās atzinumu;

c) ņemot vērā Komisijas atzinumu, ar locekļu divu trešdaļu balsu vairākumu un saskaņā ar 17. pantu pieņem Aģentūras vienoto programmdokumentu;

ca) pārrauga to, kā tiek īstenoti vienotajā programmdokumentā ietvertie daudzgadu plāni un gada plāni;

d) ar locekļu divu trešdaļu balsu vairākumu pieņem Aģentūras gada budžetu un saskaņā ar III nodaļu pilda citas funkcijas attiecībā uz budžetu;

e) novērtē un pieņem konsolidēto gada pārskatu par Aģentūras darbību un ne vēlāk kā līdz nākamā gada 1. jūlijam gan ziņojumu, gan tā novērtējumu nosūta Eiropas Parlamentam, Padomei, Komisijai un Revīzijas palātai. Gada pārskatā iekļauj grāmatvedības pārskatus un apraksta, kā Aģentūra ir izpildījusi savus darbības rādītājus. Gada pārskats ir publiski pieejams;

f) saskaņā ar 29. pantu pieņem Aģentūrai piemērojamos finansiālos noteikumus;

g) pieņem krāpšanas apkarošanas stratēģiju, kas ir proporcionāla krāpšanas riskiem, ņemot vērā veicamo pasākumu izmaksas un ieguvumus;

h) attiecībā uz saviem locekļiem pieņem noteikumus interešu konfliktu novēršanai un pārvaldībai;

i) nodrošina pienācīgu reaģēšanu uz konstatējumiem un ieteikumiem, kas izriet no Eiropas Biroja krāpšanas apkarošanai (*OLAF*) izmeklēšanas un dažādiem iekšējās vai ārējās revīzijas ziņojumiem un izvērtējumiem;

j) pieņem savu reglamentu;

k) saskaņā ar 2. punktu attiecībā uz Aģentūras personālu īsteno pilnvaras, kas Civildienesta noteikumos piešķirtas iecēlējinstitūcijai un "Savienības pārējo darbinieku nodarbināšanas kārtībā" – iestādei, kura pilnvarota slēgt darba līgumu ("iecēlējinstitūcijas pilnvaras");

l) pieņem Civildienesta noteikumu un "Savienības pārējo darbinieku nodarbināšanas kārtības" īstenošanas noteikumus saskaņā ar kārtību, kas paredzēta Civildienesta noteikumu 110. pantā;

m) ieceļ izpilddirektoru un attiecīgā gadījumā pagarina viņa pilnvaru laiku vai viņu atceļ no amata saskaņā ar šīs regulas 33. pantu;

n) ieceļ grāmatvedi, kurš var būt Komisijas grāmatvedis un kurš savu pienākumu izpildē ir pilnīgi neatkarīgs;

o) ņemot vērā vajadzības attiecībā uz Aģentūras darbību un ievērojot pareizu budžeta pārvaldību, pieņem visus lēmumus par Aģentūras iekšējo struktūru izveidi un vajadzības gadījumā to pārveidi;

p) atļauj vienoties par sadarbības mehānismu saskaņā ar 7. un 39. pantu.

2. Saskaņā ar Civildienesta noteikumu 110. pantu, pamatojoties uz Civildienesta noteikumu 2. panta 1. punktu un "Savienības pārējo darbinieku nodarbināšanas kārtības" 6. pantu, Administratīvā padome pieņem lēmumu, ar kuru izpilddirektoram deleģē attiecīgās iecēlējinstitūcijas pilnvaras un nosaka nosacījumus, ar kādiem šo pilnvaru deleģējumu var apturēt. Izpilddirektoram atļauts minētās pilnvaras deleģēt tālāk.

3. Īpašu izņēmuma apstākļu dēļ Administratīvā padome var lemt uz laiku apturēt iecēlējinstitūcijas pilnvaru deleģējumu izpilddirektoram, kā arī pilnvaras, ko izpilddirektors deleģējis tālāk, un tās īstenot pati vai deleģēt kādam no saviem locekļiem vai personāla loceklim, kurš nav izpilddirektors.

15. pants

Administratīvās padomes priekšsēdētājs

Administratīvā padome ar locekļu divu trešdaļu balsu vairākumu ievēlē priekšsēdētāju un viņa vietnieku no savu locekļu vidus uz četru gadu laikposmu, ko var pagarināt vienu reizi. Tomēr, ja Administratīvās padomes priekšsēdētāja vai priekšsēdētāja vietnieka dalība Administratīvajā padomē beidzas viņu amata pilnvaru laikā, arī viņu amata pilnvaru laiks automātiski beidzas tajā pašā dienā. Priekšsēdētāja vietnieks *ex officio* aizstāj priekšsēdētāju, ja priekšsēdētājs nespēj pildīt savus pienākumus.

16. pants

Administratīvās padomes sanāksmes

1. Administratīvās padomes sanāksmes sasauc tās priekšsēdētājs.

2. Administratīvā padome regulārajās sanāksmēs pulcējas vismaz divreiz gadā. Tā rīko arī ārkārtas sanāksmes pēc priekšsēdētāja, Komisijas vai vismaz vienas trešdaļas locekļu pieprasījuma.

3. Izpilddirektors Administratīvās padomes sanāksmēs piedalās bez balsstiesībām.

4. Pastāvīgās ieinteresēto personu grupas locekļi Administratīvās padomes sanāksmēs var piedalīties pēc priekšsēdētāja uzaicinājuma, taču viņiem nav balsstiesību.

5. Atbilstīgi Administratīvās padomes reglamentam tās locekļiem un viņu aizstājējiem sanāksmēs var palīdzēt padomdevēji vai eksperti.

6. Aģentūra nodrošina Administratīvajai padomei sekretariātu.

17. pants

Administratīvās padomes balsošanas noteikumi

1. Administratīvā padome pieņem lēmumus ar locekļu balsu vairākumu.

2. Vienotā programmdokumenta un gada budžeta pieņemšanai, izpilddirektora iecelšanai amatā, viņa pilnvaru termiņa pagarināšanai un atbrīvošanai no amata ir vajadzīgs divu trešdaļu Administratīvās padomes locekļu balsu vairākums.

3. Katram loceklim ir viena balss. Ja kāds Administratīvās padomes loceklis sanāksmē nepiedalās, viņa balsstiesības ir tiesīgs izmantot šā locekļa aizstājējs.

4. Priekšsēdētājs piedalās balsošanā.

5. Izpilddirektors nepiedalās balsošanā.

6. Administratīvās padomes reglamentā balsošanas kārtību detalizē, jo īpaši, norādot, ar kādiem nosacījumiem loceklis var darboties cita locekļa vārdā. 2.

2. IEDAĻA
VALDE

18. pants

Valde

1. Administratīvajai padomei palīdz Valde.

2. Valde:

   a) sagatavo lēmumus, kas jāpieņem Administratīvajai padomei;

   b) kopā ar Administratīvo padomi nodrošina atbilstīgu turpmāku rīcību saistībā ar konstatējumiem un ieteikumiem, kas izriet no *OLAF* izmeklēšanas un dažādiem iekšēju un ārēju revīziju ziņojumiem un izvērtējumiem;

   c) neskarot 19. pantā noteiktos izpilddirektora pienākumus, palīdz un sniedz padomus izpilddirektoram Administratīvās padomes lēmumu īstenošanā par administratīviem un budžeta jautājumiem atbilstīgi 19. pantam.

3. Valde sastāv no pieciem locekļiem, ko ieceļ no Administratīvās padomes locekļiem, starp kuriem ir Administratīvās padomes priekšsēdētājs, kas var būt arī Valdes priekšsēdētājs, un viens no Komisijas pārstāvjiem. Izpilddirektors piedalās Valdes sanāksmēs, bet viņam nav balsstiesību.

4. Valdes locekļu amata pilnvaru ilgums ir četri gadi. Minēto pilnvaru termiņu var pagarināt.

5. Valdes sanāksmes notiek vismaz reizi trijos mēnešos. Valdes priekšsēdētājs sasauc papildu sanāksmes pēc tās locekļu pieprasījuma.

6. Valdes reglamentu nosaka Administratīvā padome.

7. [...]

3. IEDAĻA
IZPILDDIREKTORS

19. pants

Izpilddirektora pienākumi

1. Aģentūru vada izpilddirektors, kas, pildot savus pienākumus, ir neatkarīgs. Izpilddirektors sniedz pārskatu Administratīvajai padomei.

2. Izpilddirektors pēc Eiropas Parlamenta uzaicinājuma tam ziņo par savu pienākumu izpildi. Padome var aicināt izpilddirektoru ziņot par savu pienākumu izpildi.

3. Izpilddirektors atbild par to, lai tiktu:

a) ikdienā vadīts Aģentūras darbs;

b) īstenoti Administratīvās padomes pieņemtie lēmumi;

c) sagatavots un Administratīvajā padomē apstiprināšanai iesniegts vienotā programmdokumenta projekts, lai pēc tam to iesniegtu Komisijā;

d) īstenots vienotais programmdokuments un par tā īstenošanu sniegts pārskats Administratīvajai padomei;

e) sagatavots un Administratīvajai padomei novērtēšanai un pieņemšanai iesniegts konsolidētais gada pārskats par Aģentūras darbību, **tostarp par gada darba programmas īstenošanu**;

f) sagatavots rīcības plāns, kurā tiek noteikti turpmākie pasākumi attiecībā uz retrospektīvo izvērtējumu secinājumiem, un reizi divos gados par īstenošanas gaitu ziņots Komisijai;

g) sagatavots rīcības plāns, kurā tiek noteikti turpmākie pasākumi attiecībā uz secinājumiem, kas izriet no iekšējās vai ārējās revīzijas ziņojumiem, kā arī no izmeklēšanas, kuru veicis Eiropas Birojs krāpšanas apkarošanai (*OLAF*), un divreiz gadā par plāna īstenošanas gaitu ziņots Komisijai un regulāri – Administratīvajai padomei;

h) sagatavots Aģentūrai piemērojamo finansiālo noteikumu projekts;

i) sagatavoti Aģentūras ieņēmumu un izdevumu tāmju projekti un izpildīts tās budžets;

j) aizsargātas Savienības finansiālās intereses, piemērojot profilaktiskus pasākumus pret krāpšanu, korupciju un citām nelikumīgām darbībām, veicot efektīvas pārbaudes un, ja ir atklāti pārkāpumi, atgūstot nepamatoti izmaksātas summas, un attiecīgos gadījumos piemērojot iedarbīgas, samērīgas un atturošas administratīvas un finansiālas sankcijas;

k) sagatavotas un Administratīvajai padomei apstiprināšanai iesniegtas Aģentūras stratēģijas krāpšanas apkarošanai;

l) nodibināti un uzturēti sakari ar uzņēmēju aprindām un patērētāju organizācijām, lai nodrošinātu regulāru dialogu ar attiecīgajām ieinteresētajām personām;

la) uzturēta regulāra saziņa ar Savienības iestādēm, aģentūrām un struktūrām par to darbībām kiberdrošības jomā, lai nodrošinātu saskaņotību ES politikas veidošanā un īstenošanā;

m) izpildīti citi ar šo regulu izpilddirektoram uzticēti uzdevumi.

4. Vajadzības gadījumā, Aģentūras pilnvaru ietvaros un saskaņā ar Aģentūras mērķiem un uzdevumiem izpilddirektors var veidot ekspertu *ad hoc* darba grupas, tostarp no dalībvalstu kompetentajām iestādēm. Par to iepriekš informē Administratīvo padomi. Procedūras, jo īpaši attiecībā uz darba grupu sastāvu, kārtību, kādā izpilddirektors izraugās darba grupas ekspertus, un darba grupu darbību, nosaka Aģentūras darbības iekšējos noteikumos.

5. **Vajadzības gadījumā, lai Aģentūras uzdevumi tiktu pildīti rezultatīvi un efektīvi, un uz pienācīgas izmaksu un ieguvumu analīzes pamata** izpilddirektors **var** nolemt [...] **izveidot vienu vai vairākus vietējus birojus vienā vai vairākās dalībvalstīs**. Pirms izlemj izveidot vietējo biroju, izpilddirektors **lūdz attiecīgās(-o) dalībvalsts(-u) viedokli, tostarp tās dalībvalsts, kurā atrodas Aģentūras mītne, un** saņem iepriekšēju piekrišanu no Komisijas **un** Administratīvās padomes [...]. **Ja izpilddirektors un attiecīgā dalībvalsts apspriešanās gaitā nevar vienoties, jautājumu izvirza apspriešanai Padomē.** Lēmumā norāda vietējā birojā veicamo darbību tvērumu, izvairoties no liekām izmaksām un Aģentūras administratīvo funkciju dublēšanas.[...] **Darbinieku skaits visos vietējos birojos ir minimāls un kopā nav lielāks par [...] 40 % no to darbinieku skaita, kuri atrodas dalībvalstī, kurā atrodas Aģentūras mītne. Darbinieku skaits katrā vietējā birojā nav lielāks par 10 % no to [...] darbinieku skaita, [...] kuri atrodas dalībvalstī, kurā atrodas Aģentūras mītne.**

4. IEDAĻA
PASTĀVĪGĀ IEINTERESĒTO PERSONU GRUPA

20. pants

Pastāvīgā ieinteresēto personu grupa

1. Pēc izpilddirektora priekšlikuma Administratīvā padome izveido Pastāvīgo ieinteresēto personu grupu, kurā darbojas atzīti eksperti, kas pārstāv attiecīgas ieinteresētās personas, piemēram, IKT nozares pārstāvjus, sabiedrībai pieejamu elektronisko sakaru tīklu vai pakalpojumu nodrošinātājus, **pamatpakalpojumu sniedzējus**, patērētāju grupas, ekspertus no akadēmiskajām aprindām kiberdrošības jomā un pārstāvjus no kompetentajām iestādēm, par kurām paziņots atbilstīgi [Direktīvai par Eiropas elektronisko sakaru kodeksa izveidi], kā arī tiesībaizsardzības un datu aizsardzības pārraudzības iestādēm.

2. Pastāvīgajā ieinteresēto personu grupā izmantojamās procedūras, jo īpaši attiecībā uz grupas sastāvu, locekļu skaitu un kārtību, kādā Administratīvā padome tos ieceļ, izpilddirektora priekšlikumu un grupas darbību, nosaka Aģentūras darbības iekšējos noteikumos un publicē.

3. Pastāvīgo ieinteresēto personu grupu vada izpilddirektors vai jebkura persona, kuru izpilddirektors ieceļ attiecīgajam gadījumam.

4. Pastāvīgās ieinteresēto personu grupas locekļu pilnvaru ilgums ir divarpus gadi. Pastāvīgās ieinteresēto personu grupas locekļi nedrīkst būt Administratīvās padomes locekļi. Komisijas un dalībvalstu ekspertiem ir tiesības būt klāt Pastāvīgās ieinteresēto personu grupas sanāksmēs un piedalīties tās darbā. Pārstāvji no citām izpilddirektora ieskatā saistītām struktūrām, kaut arī viņi nav Pastāvīgās ieinteresēto personu grupas locekļi, var tikt uzaicināti piedalīties Pastāvīgās ieinteresēto personu grupas sanāksmēs un darbā.

5. Pastāvīgā ieinteresēto personu grupa dod padomus Aģentūrai attiecībā uz tās darba izpildi. Īpaši tā dod padomus izpilddirektoram par Aģentūras darba programmas priekšlikuma izstrādi un saziņas nodrošināšanu ar attiecīgajām ieinteresētajām personām par visiem jautājumiem, kas attiecas uz darba programmu.

5.a Pastāvīgā ieinteresēto personu grupa par savu darbību regulāri informē Administratīvo padomi.

4.A IEDAĻA
VALSTS SADARBĪBAS KOORDINATORU TĪKLS

20.a pants

Valsts sadarbības koordinatoru tīkls

1. Pēc izpilddirektora priekšlikuma Administratīvā padome izveido Valsts sadarbības koordinatoru tīklu, kurā darbojas dalībvalstu pārstāvji.

2. Valsts sadarbības koordinatoru tīklā darbojas visu dalībvalstu pārstāvji. Katra dalībvalsts ieceļ vienu pārstāvi. Tīkla sanāksmes var notikt dažādu ekspertu sastāvā.

3. Valsts sadarbības koordinatoru tīkls jo īpaši veicina informācijas apmaiņu starp *ENISA* un dalībvalstīm. Tas jo īpaši sniedz atbalstu *ENISA* saistībā ar tās darbību, konstatējumu un ieteikumu izplatīšanu visā ES attiecīgajām ieinteresētajām personām.

4. Valsts sadarbības koordinatori ir centrālais kontaktpunkts valsts līmenī, un tā mērķis ir atvieglot *ENISA* un valstu ekspertu sadarbību *ENISA* darba programmas īstenošanas kontekstā.

5. Lai gan valsts sadarbības koordinatoriem būtu cieši jāsadarbojas ar savu attiecīgo valstu pārstāvjiem Administratīvajā padomē, paša tīkla darbs nedublē ne Administratīvās padomes, ne citu ES forumu darbu.

6. Valsts sadarbības koordinatoru tīkla funkcijas un procedūras nosaka Aģentūras darbības iekšējos noteikumos un publisko.

5. IEDAĻA
DARBĪBA

21. pants

Vienotais programmdokuments

1. Aģentūra darbojas saskaņā ar vienoto programmdokumentu, kurā ietverti daudzgadu plāni un gada plāni un izklāstīti visi tās plānotie pasākumi.

2. Izpilddirektors katru gadu atbilstīgi Komisijas Deleģētās regulas (ES) Nr. 1271/2013 [14] 32. pantam un Komisijas vadlīnijām izstrādā vienoto programmdokumentu ar daudzgadu plāniem un gada plāniem, kuros ietverts atbilstošo cilvēkresursu un finansiālo līdzekļu plānojums.

3. Ik gadu ne vēlāk kā 30. novembrī Administratīvā padome pieņem 1. punktā minēto vienoto programmdokumentu, un to, kā arī visas nākamās dokumenta redakcijas, ne vēlāk kā nākamā gada 31. janvārī nosūta Eiropas Parlamentam, Padomei un Komisijai.

4. Vienotais programmdokuments kļūst galīgs pēc Eiropas Savienības vispārējā budžeta galīgās pieņemšanas, un vajadzības gadījumā to attiecīgi koriģē.

5. Gada darba programmā ietver detalizētus mērķus un gaidāmos rezultātus, arī gaidāmos snieguma rādītājus. Ievērojot tādus principus kā budžeta līdzekļu sadale pēc darbības jomām un budžeta pārvaldība pa darbības jomām, programmā ietver arī finansējamo darbību aprakstu un norādi par katrai darbībai piešķirtajiem finansiālajiem līdzekļiem un cilvēkresursiem. Gada darba programma saskan ar 7. punktā minēto daudzgadu darba programmu. Tajā skaidri norāda, kādi uzdevumi ir pievienoti, mainīti vai svītroti salīdzinājumā ar iepriekšējo finanšu gadu.

---

[14] Komisijas Deleģētā regula (ES) Nr. 1271/2013 (2013. gada 30. septembris) par finanšu pamatregulu struktūrām, kas minētas Eiropas Parlamenta un Padomes Regulas (ES, *Euratom*) Nr. 966/2012 208. pantā (OV L 328, 7.12.2013., 42. lpp.).

6. Ja Aģentūrai tiek uzticēts jauns uzdevums, Administratīvā padome pieņemto gada darba programmu groza. Būtiskus gada darba programmas grozījumus pieņem tādā pašā procedūrā, kādā pieņem sākotnējo gada darba programmu. Pilnvaras izdarīt nebūtiskus grozījumus gada darba programmā Administratīvā padome var deleģēt izpilddirektoram.

7. Daudzgadu darba programmā izklāsta vispārējo stratēģisko plānu, ietverot mērķus, gaidāmos rezultātus un snieguma rādītājus. Tajā apraksta arī resursu plānu, ietverot daudzgadu budžetu un personāla plānojumu.

8. Resursu plānu atjaunina reizi gadā. Stratēģisko plānu vajadzības gadījumā atjaunina, jo īpaši, lai ņemtu vērā 56. pantā minētās izvērtēšanas iznākumu.

22. pants

Interešu deklarācija

1. Administratīvās padomes locekļi, izpilddirektors un dalībvalstu uz laiku norīkotās amatpersonas katra iesniedz saistību deklarāciju un deklarāciju, kurā norāda, ka tām nav tiešu vai netiešu interešu, kuras varētu uzskatīt par tādām, kas ietekmē viņu neatkarību, vai ka tādas ir. Deklarācijas ir precīzas un pilnīgas, tās ik gadu iesniedz rakstiski un atjaunina, kad vien nepieciešams.

2. Administratīvās padomes locekļi, izpilddirektors un ārējie eksperti, kas piedalās *ad hoc* darba grupās, ne vēlāk kā katras sanāksmes sākumā katrs precīzi un pilnīgi deklarē visas intereses, kuras var uzskatīt par tādām, kas ietekmē viņu neatkarību attiecībā uz darba kārtībā iekļautajiem jautājumiem, un nepiedalās šādu jautājumu apspriešanā un balsošanā par tiem.

3. Aģentūra darbības iekšējos noteikumos paredz praktiskos pasākumus 1. un 2. punktā minēto interešu deklarāciju noteikumiem.

23. pants

Pārredzamība

1. Aģentūra savā darbībā nodrošina augsta līmeņa pārredzamību saskaņā ar 25. pantu.

2. Aģentūra gādā, lai sabiedrība un visas ieinteresētās personas saņemtu atbilstošu, objektīvu, ticamu un viegli pieejamu informāciju, jo īpaši par Aģentūras darba rezultātiem. Tā arī publicē interešu deklarācijas, kas iesniegtas saskaņā ar 22. pantu.

3. Administratīvā padome pēc izpilddirektora priekšlikuma drīkst atļaut ieinteresētajām personām novērot dažu Aģentūras pasākumu norisi.

4. Aģentūra darbības iekšējos noteikumos paredz praktiskos pasākumus 1. un 2. punktā minēto pārredzamības noteikumu īstenošanai.

24. pants

Konfidencialitāte

1. Neskarot 25. pantu, Aģentūra neizpauž trešām personām informāciju, ko tā apstrādā vai saņem, ja par to visu vai daļu no tās ir izteikts pamatots pieprasījums to uzskatīt par konfidenciālu.

2. Uz Administratīvās padomes locekļiem, izpilddirektoru, Pastāvīgās ieinteresēto personu grupas locekļiem, ārējiem ekspertiem, kas piedalās *ad hoc* darba grupās, un Aģentūras personāla locekļiem, tostarp dalībvalstu uz laiku norīkotajām amatpersonām, konfidencialitātes prasības saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 339. pantu attiecas arī pēc tam, kad šīs personas ir beigušas pildīt savus pienākumus.

3. Aģentūra darbības iekšējos noteikumos paredz praktiskos pasākumus 1. un 2. punktā minēto konfidencialitātes noteikumu īstenošanai.

4. Ja tas nepieciešams Aģentūras uzdevumu veikšanai, Administratīvā padome atļauj Aģentūrai apstrādāt klasificētu informāciju. Tādā gadījumā Administratīvā padome, vienojoties ar Komisijas dienestiem, pieņem darbības iekšējos noteikumos, piemērojot drošības principus, kas noteikti Komisijas Lēmumā (ES, *Euratom*) 2015/443 [15] un Lēmumā (ES, *Euratom*) 2015/444 [16]. Minētie noteikumi reglamentē klasificētas informācijas apmaiņu, apstrādi un glabāšanu.

---

15 Komisijas Lēmums (ES, *Euratom*) 2015/443 (2015. gada 13. marts) par drošību Komisijā (OV L 72, 17.3.2015., 41. lpp.).

16 Komisijas Lēmums (ES, *Euratom*) 2015/444 (2015. gada 13. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.).

25. pants

Piekļuve dokumentiem

1. Uz Aģentūras rīcībā esošajiem dokumentiem attiecas Regula (EK) Nr. 1049/2001.

2. Sešu mēnešu laikā kopš Aģentūras izveides Administratīvā padome pieņem Regulas (EK) Nr. 1049/2001 izpildei vajadzīgos pasākumus.

3. Par lēmumiem, ko Aģentūra pieņem atbilstīgi Regulas (EK) Nr. 1049/2001 8. pantam, var iesniegt sūdzību Ombudam saskaņā ar LESD 228. pantu vai prasību Eiropas Savienības Tiesā saskaņā ar LESD 263. pantu.

III NODAĻA
BUDŽETA IZVEIDE UN UZBŪVE

26. pants

Budžeta izveide

1. Katru gadu izpilddirektors izstrādā Aģentūras ieņēmumu un izdevumu tāmes projektu nākamajam finanšu gadam un kopā ar štatu saraksta projektu nosūta Administratīvajai padomei. Ieņēmumi un izdevumi ir līdzsvarā.

2. Pamatojoties uz 1. punktā minēto ieņēmumu un izdevumu tāmes projektu, katru gadu Administratīvā padome sagatavo Aģentūras ieņēmumu un izdevumu tāmi nākamajam finanšu gadam.

3. Panta 2. punktā minēto tāmes projektu, kas ir iekļauts vienotā programmdokumenta projektā, Administratīvā padome līdz katra gada 31. janvārim nosūta Komisijai un trešām valstīm, ar kurām Savienība ir noslēgusi nolīgumus saskaņā ar 39. pantu.

4. Pamatojoties uz minēto tāmi, Komisija Savienības budžeta projektā iekļauj aplēses, ko uzskata par vajadzīgām attiecībā uz štatu sarakstu un tās iemaksas apjomu, kas attiecināma uz vispārējo budžetu, un iesniedz tās Eiropas Parlamentam un Padomei saskaņā ar Līguma 313. un 314. pantu.

5. Eiropas Parlaments un Padome apstiprina iemaksu apropriācijas Aģentūrai.

6. Eiropas Parlaments un Padome apstiprina Aģentūras štatu sarakstu.

7. Administratīvā padome kopā ar vienoto programmdokumentu pieņem Aģentūras budžetu. Tas kļūst par galīgo variantu pēc Savienības vispārējā budžeta pieņemšanas galīgā variantā. Vajadzības gadījumā Administratīvā padome Aģentūras budžetu un vienoto programmdokumentu koriģē saskaņā ar Savienības vispārējo budžetu.

27. pants

Budžeta struktūra

1. Neskarot citus resursus, Aģentūras ieņēmumos ietilpst:

   a) iemaksas no Savienības budžeta;

   b) ieņēmumi, kas konkrētiem izdevumu posteņiem piešķirti saskaņā ar Aģentūras finansiālajiem noteikumiem, kas izklāstīti 29. pantā;

   c) Savienības finansējums deleģēšanas nolīgumu vai *ad hoc* dotāciju veidā saskaņā ar tās finansiālajiem noteikumiem, kas izklāstīti 29. pantā, un noteikumiem attiecīgajos tiesību aktos, ar kuriem atbalsta Savienības politikas jomas;

d) iemaksas no trešām valstīm, kuras piedalās Aģentūras darbā saskaņā ar 39. pantu;

e) jebkādas dalībvalstu brīvprātīgas iemaksas naudā vai natūrā. Dalībvalstis, kuras veic brīvprātīgās iemaksas, nevar šā iemesla dēļ pieprasīt īpašas tiesības vai pakalpojumus.

2. Aģentūras izdevumus veido personāla, administratīvā un tehniskā atbalsta pasākumu, infrastruktūras un darbības izmaksas un izmaksas, ko rada ar trešām personām noslēgti līgumi.

28. pants

Budžeta izpilde

1. Par Aģentūras budžeta izpildi atbild izpilddirektors.

2. Komisijas iekšējam revidentam Aģentūrā ir tādas pašas pilnvaras kā Komisijas dienestos.

3. Līdz nākamā finanšu gada 1. martam ((N+1). gada 1. marts) Aģentūras grāmatvedis Komisijas grāmatvedim un Revīzijas palātai nosūta provizoriskos pārskatus.

4. Kad ir saņemti Revīzijas palātas apsvērumi par Aģentūras provizoriskajiem pārskatiem, Aģentūras grāmatvedis uz savu atbildību sagatavo Aģentūras galīgos pārskatus.

5. Izpilddirektors galīgos pārskatus iesniedz Administratīvajai padomei, lai saņemtu tās atzinumu.

6. Līdz (N+1). gada 31. martam izpilddirektors ziņojumu par budžeta un finanšu pārvaldību nosūta Eiropas Parlamentam, Padomei, Komisijai un Revīzijas palātai.

7. Līdz (N+1). gada 1. jūlijam grāmatvedis galīgos pārskatus kopā ar Administratīvās padomes atzinumu pārsūta Eiropas Parlamentam, Padomei, Komisijas grāmatvedim un Revīzijas palātai.

8. Tajā pašā dienā, kad nosūtīti galīgie pārskati, grāmatvedis Revīzijas palātai nosūta arī apliecinājuma vēstuli par minētajiem galīgajiem pārskatiem, kopiju nosūtot Komisijas grāmatvedim.

9. Izpilddirektors publicē galīgos pārskatus līdz nākamā gada 15. novembrim.

10. Līdz (N+1). gada 30. septembrim izpilddirektors Revīzijas palātai nosūta atbildi par tās apsvērumiem, bet Administratīvajai padomei un Komisijai – atbildes kopiju.

11. Saskaņā ar Finanšu regulas 165. panta 3. punktu pēc Eiropas Parlamenta pieprasījuma izpilddirektors tam iesniedz visu informāciju, kas vajadzīga netraucētai attiecīgā finanšu gada budžeta izpildes apstiprinājuma procedūras piemērošanai.

12. Pēc Padomes ieteikuma Eiropas Parlaments izpilddirektoram līdz (N+2). gada 15. maijam sniedz apstiprinājumu par (N). gada budžeta izpildi.

29. pants

Finanšu noteikumi

Aģentūrai piemērojamos finanšu noteikumus pieņem Administratīvā padome pēc apspriešanās ar Komisiju. Tie neatkāpjas no Regulas (ES) Nr. 1271/2013, ja vien atkāpšanās nav īpaši nepieciešama Aģentūras darbībai un Komisija iepriekš nav devusi piekrišanu.

30. pants

Krāpšanas apkarošana

1. Lai palīdzētu apkarot krāpšanu, korupciju un citas nelikumīgas darbības, kā paredzēts Eiropas Parlamenta un Padomes Regulā (EK) 883/2013 [17], Aģentūra sešu mēnešu laikā pēc darbības sākšanas pievienojas 1999. gada 25. maija Iestāžu nolīgumam par iekšējām izmeklēšanām, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*), un, izmantojot minētā nolīguma pielikumā doto paraugu, pieņem attiecīgus noteikumus, kas piemērojami visiem Aģentūras darbiniekiem.

2. Revīzijas palātai ir tiesības, pārbaudot dokumentus un veicot pārbaudes uz vietas, revidēt visus dotāciju saņēmējus, līgumslēdzējus un apakšuzņēmējus, kuri no Aģentūras ir saņēmuši Savienības līdzekļus.

---

[17] Eiropas Parlamenta un Padomes Regula (ES, *Euratom*) Nr. 883/2013 (2013. gada 11. septembris) par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*), un ar ko atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1073/1999 un Padomes Regulu (*Euratom*) Nr. 1074/1999 (OV L 248, 18.9.2013., 1. lpp.).

3. *OLAF* var veikt izmeklēšanu, tostarp pārbaudes un inspekcijas uz vietas, saskaņā ar noteikumiem un procedūrām, kas noteiktas Eiropas Parlamenta un Padomes Regulā 883/2013 un Padomes Regulā (*Euratom*, EK) Nr. 2185/96 (1996. gada 11. novembris) par pārbaudēm un apskatēm uz vietas, ko Komisija veic, lai aizsargātu Savienības finanšu intereses pret krāpšanu un citām nelikumībām [18], lai noteiktu, vai nav notikusi krāpšana, korupcija vai kādas citas nelikumīgas darbības, kas ietekmē Savienības finansiālās intereses, kuras saistītas ar Aģentūras finansētu dotāciju vai līgumu.

4. Neskarot 1., 2. un 3. punktu, Aģentūras sadarbības nolīgumos ar trešām valstīm un starptautiskām organizācijām, līgumos, dotāciju nolīgumos un dotāciju lēmumos ietver noteikumus, kas Revīzijas palātu un *OLAF* skaidri pilnvaro savas attiecīgās kompetences ietvaros veikt šādas revīzijas un izmeklēšanas.

IV NODAĻA
AĢENTŪRAS DARBINIEKI

31. pants

Vispārīgi noteikumi

Uz Aģentūras personālu attiecas Civildienesta noteikumi un Savienības pārējo darbinieku nodarbināšanas kārtība un noteikumi, kas pieņemti, vienojoties Savienības iestādēm, lai īstenotu minētos Civildienesta noteikumus.

[18] Padomes Regula (*Euratom*, EK) Nr. 2185/96 (1996. gada 11. novembris) par pārbaudēm un apskatēm uz vietas, ko Komisija veic, lai aizsargātu Eiropas Kopienu finanšu intereses pret krāpšanu un citām nelikumībām (OV L 292, 15.11.1996., 2. lpp.).

32. pants

Privilēģijas un imunitāte

Uz Aģentūru un tās personālu attiecas Protokols (Nr. 7) par privilēģijām un imunitāti Eiropas Savienībā, kas pievienots Līgumam par Eiropas Savienību un LESD.

33. pants

Izpilddirektors

1. Izpilddirektoru pieņem darbā kā Aģentūras pagaidu darbinieku saskaņā ar "Savienības pārējo darbinieku nodarbināšanas kārtības" 2. panta a) punktu.

2. Izpilddirektoru atklātā un pārredzamā atlases procedūrā no Komisijas ierosināta kandidātu saraksta ieceļ Administratīvā padome.

3. Lai noslēgtu līgumu ar izpilddirektoru, Aģentūru pārstāv Administratīvās padomes priekšsēdētājs.

4. Pirms iecelšanas amatā Eiropas Parlamenta attiecīgā komiteja uzaicina Administratīvās padomes izraudzīto kandidātu sniegt paziņojumu un atbildēt uz deputātu jautājumiem.

5. Izpilddirektora amata pilnvaru ilgums ir **četri** [...] gadi. Līdz minētā laikposma beigām Komisija veic novērtējumu, kurā ņem vērā izpilddirektora snieguma izvērtējumu un Aģentūras turpmākos uzdevumus un risināmos jautājumus.

6. Administratīvās padomes lēmumus par izpilddirektora iecelšanu amatā, viņa pilnvaru laika pagarināšanu vai atbrīvošanu no amata pieņem ar balsstiesīgo locekļu divu trešdaļu balsu vairākumu.

7. Administratīvā padome, rīkojoties pēc Komisijas priekšlikuma, kurā ņemts vērā 5. punktā minētais novērtējums, izpilddirektora amata pilnvaru laiku var vienu reizi pagarināt par laiku, kas nepārsniedz **četrus** [...] gadus.

8. Administratīvā padome informē Eiropas Parlamentu par nodomu pagarināt izpilddirektora pilnvaru termiņu. Trīs mēnešu laikā pirms šādas pagarināšanas izpilddirektors, ja viņu uzaicina, sniedz paziņojumu Eiropas Parlamenta attiecīgajā komitejā un atbild uz deputātu jautājumiem.

9. Izpilddirektors, kura pilnvaru termiņš ir ticis pagarināts, nevar piedalīties citā atlases procedūrā uz to pašu amata vietu.

10. Izpilddirektoru no amata var atcelt tikai ar Administratīvās padomes lēmumu [...].

34. pants

Norīkotie valsts eksperti un pārējie darbinieki

1. Aģentūra var izmantot norīkotos valsts ekspertus vai pārējos darbiniekus, kas nav nodarbināti Aģentūrā. Uz šādiem darbiniekiem neattiecas Civildienesta noteikumi un Savienības pārējo darbinieku nodarbināšanas kārtība.

2. Administratīvā padome pieņem lēmumu, ar ko paredz noteikumus attiecībā uz valstu ekspertu norīkošanu uz Aģentūru.

V NODAĻA
VISPĀRĪGI NOTEIKUMI

35. pants

Aģentūras juridiskais statuss

1. Aģentūra ir Savienības struktūra, un tā ir juridiska persona.

2. Visās dalībvalstīs Aģentūrai ir visplašākā tiesībspēja un rīcībspēja, ko attiecīgās valsts tiesību akti piešķir juridiskām personām. Tā jo īpaši var iegādāties vai atsavināt kustamu un nekustamu īpašumu un būt par pusi tiesas procesā [...].

3. Aģentūru pārstāv izpilddirektors.

36. pants

Aģentūras atbildība

1. Aģentūras līgumisko atbildību reglamentē attiecīgajam līgumam piemērojamās tiesības.

2. Pieņemt nolēmumus, pamatojoties uz šķīrējklauzulu, kas ietverta Aģentūras noslēgtā līgumā, ir Eiropas Savienības Tiesas jurisdikcijā.

3. Ja iestājusies ārpuslīgumiska atbildība, Aģentūra saskaņā ar vispārīgajiem principiem, kas ir kopīgi dalībvalstu tiesību aktiem, atlīdzina katru kaitējumu, ko tās darbinieki nodarījuši, pildot savus pienākumus.

4. Visi strīdi, kas saistīti ar minēto zaudējumu atlīdzināšanu, ir Eiropas Savienības Tiesas jurisdikcijā.

5. Darbinieku personisko atbildību pret Aģentūru reglamentē attiecīgie nosacījumi, kas attiecas uz Aģentūras personālu.

37. pants

Valodu lietošanas kārtība

1. Uz Aģentūru attiecas Padomes Regulas Nr. 1 noteikumi [19]. Dalībvalstis un pārējās struktūras, ko tās norīko, var vērsties pie Aģentūras un saņemt atbildi jebkurā Eiropas Savienības iestāžu oficiālajā valodā pēc savas izvēles.

2. Aģentūras darbībai vajadzīgos tulkošanas pakalpojumus sniedz Eiropas Savienības iestāžu Tulkošanas centrs.

38. pants

Personas datu aizsardzība

1. Personas datu apstrādi Aģentūrā reglamentē Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 [20].

2. Administratīvā padome pieņem īstenošanas pasākumus, kas minēti Regulas (EK) Nr. 45/2001 24. panta 8. punktā. Administratīvā padome var pieņemt papildu pasākumus, kas vajadzīgi, lai Aģentūra varētu piemērot Regulu (EK) Nr. 45/2001.

---

19 Regula Nr. 1, ar ko nosaka Eiropas Atomenerģijas kopienā lietojamās valodas (OV 17, 6.10.1958., 401. lpp.).

20 Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

39. pants

Sadarbība ar trešām valstīm un starptautiskām organizācijām

1. Rīkojoties tikai tiktāl, lai sasniegtu šajā regulā aprakstītos mērķus, Aģentūra var sadarboties ar trešo valstu kompetentajām iestādēm vai ar starptautiskajām organizācijām, vai abējādi. Šādā nolūkā Aģentūra, saņēmusi Komisijas iepriekšēju atļauju, ar šīm trešo valstu iestādēm un starptautiskajām organizācijām var noslēgt darba vienošanās. Šādas vienošanās ne Savienībai, ne tās dalībvalstīm nerada juridiskas saistības.

2. Aģentūra ir atvērta to trešo valstu dalībai, kuras ar Savienību noslēgušas attiecīgus nolīgumus. Saskaņā ar šo nolīgumu attiecīgajiem noteikumiem tiek izstrādāta kārtība, ar ko jo īpaši nosaka, kā pēc būtības, kādā apjomā un kādā veidā minētās valstis piedalīsies Aģentūras darbā, arī noteikumi par šo valstu dalību Aģentūras iniciatīvās, finanšu iemaksām un personālsastāvu. Attiecībā uz personāla jautājumiem minētā kārtība visos gadījumos ir saskaņā ar Civildienesta noteikumiem.

3. Administratīvā padome pieņem stratēģiju attiecībām ar trešām valstīm vai starptautiskām organizācijām Aģentūras kompetencē esošos jautājumos. Komisija, noslēdzot attiecīgu darba vienošanos ar Aģentūras izpilddirektoru, nodrošina, ka Aģentūra darbojas savu pilnvaru un pastāvošā institucionālā satvara ietvaros.

40. pants

Drošības noteikumi par klasificētas informācijas un sensitīvas neklasificētas informācijas aizsardzību

Apspriežoties ar Komisiju, Aģentūra pieņem savus drošības noteikumus, kuros piemēroti drošības principi, kas ietverti Komisijas drošības noteikumos par Eiropas Savienības klasificētas informācijas (ESKI) un sensitīvas neklasificētas informācijas aizsardzību, kuri noteikti Komisijas Lēmumos (ES, *Euratom*) 2015/443 un 2015/444. Tas cita starpā attiecas uz noteikumiem par šādas informācijas apmaiņu, apstrādi un glabāšanu.

41. pants

Mītnes nolīgums un darbības nosacījumi

1. Nepieciešamos pasākumus attiecībā uz Aģentūras izvietošanu uzņēmējā dalībvalstī un aprīkojumu, kas minētajai dalībvalstij ir jādara pieejams, kā arī īpašos noteikumus, ko uzņēmējā dalībvalstī piemēro izpilddirektoram, Administratīvās padomes locekļiem, Aģentūras personālam un viņu ģimenes locekļiem, nosaka mītnes nolīgumā starp Aģentūru un dalībvalsti, kurā atrodas mītne, un šo nolīgumu noslēdz pēc tam, kad saņemts Administratīvās padomes apstiprinājums, bet ne vēlāk kā [divus gadus pēc šīs regulas stāšanās spēkā].

2. Aģentūras mītnes dalībvalsts nodrošina [...] apstākļus, lai sekmētu pienācīgu Aģentūras darbību, tostarp atrašanās vietas pieejamību, adekvātas izglītības iestādes darbinieku bērniem un atbilstošu piekļuvi darba tirgum, sociālajai drošībai un medicīniskajai aprūpei gan bērniem, gan laulātajiem.

42. pants

Administratīvā kontrole

Aģentūras darbību saskaņā ar LESD 228. pantu pārrauga Ombuds.

III SADAĻA
KIBERDROŠĪBAS SERTIFIKĀCIJAS SATVARS

43. pants

***Eiropas kiberdrošības sertifikācijas* satvars** [...]

1. **Eiropas kiberdrošības sertifikācijas satvars ir izveidots, lai uzlabotu iekšējā tirgus darbības nosacījumus, palielinot kiberdrošības līmeni Savienībā. Ar to tiek radīta pārvaldība, kas dod iespēju ES līmenī izmantot saskaņotu pieeju attiecībā uz Eiropas kiberdrošības sertifikācijas shēmām nolūkā izveidot IKT procesu, produktu un pakalpojumu digitālu vienoto tirgu.**

2. **Eiropas kiberdrošības sertifikācijas satvars definē mehānismu nolūkā izveidot** [...] Eiropas kiberdrošības sertifikācijas shēm**as** [...] **un** apliecināt, ka IKT **procesi**, produkti un pakalpojumi, kas ir [...] **izvērtēti** saskaņā ar šādām shēm**ām**, atbilst noteiktajām **drošības** prasībām [...]**, ar mērķi visā to dzīves ciklā aizsargāt** tādu glabāto, pārsūtīto vai apstrādāto datu vai funkciju, vai pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, ko piedāvā izmantot minētie produkti, procesi **un** pakalpojumi [...], vai kam, tos izmantojot, var piekļūt.

44. pants

Eiropas kiberdrošības sertifikācijas shēmas izveidošana un pieņemšana

1. Pēc Komisijas **vai saskaņā ar 53. pantu izveidotās Eiropas Kiberdrošības sertifikācijas grupas ("Grupa")** lūguma *ENISA* sagatavo Eiropas kiberdrošības sertifikācijas kandidātshēmu, kas atbilst šīs regulas 45., 46. un 47. pantā noteiktajām prasībām.[...]

1.a Sagatavot Eiropas kiberdrošības sertifikācijas kandidātshēmu Grupai var ierosināt dalībvalstis vai ieinteresēto personu organizācijas. Grupa šādus priekšlikumus izvērtē pēc kritērijiem, ko tā noteikusi vadlīnijās saskaņā ar 53. panta 3. punkta ca) apakšpunktu, un var pieprasīt, lai *ENISA* sagatavo Eiropas kiberdrošības sertifikācijas kandidātshēmu.

2. *ENISA*, veidojot šā panta 1. punktā minētās kandidātshēmas, **pārredzamās apspriešanās procedūrās** apspriežas ar visām attiecīgajām ieinteresētajām personām un cieši sadarbojas ar Grupu. Grupa sniedz *ENISA* palīdzību un ekspertu padomus [...] saistībā ar kandidātshēmas izveidi **un pieņem atzinumu par kandidātshēmu pirms tās iesniegšanas Komisijai** [...]. ***ENISA* nodrošina, ka kandidātshēmas atbilst piemērojamajam saskaņotajam standartam, ko izmanto atbilstības novērtēšanas struktūras akreditācijā.**

3. **Pirms** [...] kandidātshēmas, kas izveidota saskaņā ar šā panta 2. punktu, **nosūtīšanas** [...] Komisijai *ENISA* **vislielākajā mērā ņem vērā Grupas atzinumu**.

4. Pamatojoties uz *ENISA* ierosināto kandidātshēmu, Komisija saskaņā ar 55. panta 2. punktu var pieņemt īstenošanas aktus, kuros paredzētas Eiropas kiberdrošības sertifikācijas shēmas IKT **procesiem,** produktiem un pakalpojumiem, kas atbilst 45., 46. un 47. panta prasībām.

5. [...]

44.a pants

Eiropas kiberdrošības sertifikācijas shēmas uzturēšana

1. Aģentūra uztur īpaši šim nolūkam izveidotu tīmekļa vietni, kurā tā sniedz informāciju par Eiropas kiberdrošības sertifikācijas shēmām, sertifikātiem un ES atbilstības apliecinājumiem, kas izdoti, ievērojot 47.a pantu, un veido publicitāti.

2. Ciešā sadarbībā ar Grupu Aģentūra vismaz reizi 5 gados pārskata pieņemtās Eiropas kiberdrošības sertifikācijas shēmas, ņemot vērā no ieinteresētajām pusēm saņemto atgriezenisko informāciju. Ja to uzskata par nepieciešamu, Komisija vai Grupa var Aģentūrai pieprasīt uzsākt pārskatītas kandidātshēmas izstrādes procesu saskaņā ar 44. panta 2. un 3. punktu.

45. pants

Eiropas kiberdrošības sertifikācijas shēmu drošības mērķi

Eiropas kiberdrošības sertifikācijas shēmu veido tā, lai attiecīgā gadījumā [...] **sasniegtu vismaz** šādus drošības mērķus:

a) uzglabātus, pārsūtītus vai citādi apstrādātus datus pasargāt no nejaušas vai neatļautas glabāšanas, apstrādes, piekļuves vai izpaušanas **visā procesa, produkta vai pakalpojuma dzīves ciklā**;

b) uzglabātus, pārsūtītus vai citādi apstrādātus datus pasargāt no nejaušas vai neatļautas iznīcināšanas [...], pazušanas vai pārveidošanas **vai pieejamības trūkuma visā procesa, produkta vai pakalpojuma dzīves ciklā**;

c) [...] pilnvarotas personas, programmas vai mašīnas var piekļūt vienīgi tādiem datiem, pakalpojumiem vai funkcijām, attiecībā uz kuriem viņiem ir piešķirtas piekļuves tiesības;

d) reģistrēt, kuriem datiem, funkcijām vai pakalpojumiem ir [...] **piekļūts, tie ir izmantoti vai citādi apstrādāti** un kad un kurš to ir darījis;

e) [...] ir iespējams pārbaudīt, kuriem datiem, pakalpojumiem vai funkcijām ir piekļūts, [...] tie ir izmantoti **vai citādi apstrādāti** un kad un kurš to ir darījis;

f) gadījumos, kad noticis fizisks vai tehnisks incidents, laikus atjaunot datu, pakalpojumu un funkciju pieejamību un piekļuvi tiem;

g) [...] IKT **procesiem,** produktiem un pakalpojumiem ir nodrošināta atjaunināta programmatūra **un aparatūra** [...] bez **publiski zināmām** vājajām vietām, un tiem ir mehānismi, kas nodrošina drošus [...] atjauninājumus**;**

ga) IKT procesi, produkti un pakalpojumi ir izstrādāti, ražoti un piegādāti saskaņā ar drošības prasībām, kas norādītas konkrētajā shēmā.

46. pants

Eiropas kiberdrošības sertifikācijas shēmu apliecinājuma līmeņi

1. Eiropas kiberdrošības sertifikācijas shēmas var būt ar vienu vai vairākiem šādiem apliecinājuma līmeņiem: pamata, būtisks un/vai augsts attiecībā uz IKT **procesiem,** produktiem un pakalpojumiem [...]. **Apliecinājuma līmenis atbilst riska līmenim, kas saistīts ar IKT procesa, produkta vai pakalpojuma paredzamo lietojumu.**

2. Pamata, būtiskais un augstais apliecinājuma līmenis [...] **attiecas uz sertifikātu vai ES atbilstības apliecinājumu, kas izdoti Eiropas kiberdrošības sertifikācijas shēmas kontekstā, kurā katram apliecinājuma līmenim paredzētas attiecīgas drošības prasības, tostarp drošības funkcijas un atbilstošs centienu intensitātes līmenis IKT procesu, produktu vai pakalpojumu izvērtējumam. Sertifikātu vai ES atbilstības apliecinājumu raksturo šāda norāde uz tehniskajām specifikācijām, standartiem un saistītajām procedūrām, tostarp uz tehniskajām kontrolēm, kuru nolūks ir samazināt kiberdrošības incidentu risku un novērst tos:**

a) **ar Eiropas kiberdrošības sertifikātu vai ES atbilstības apliecinājumu, kam ir norāde uz** apliecinājuma līmeni "pamata"**, sniedz apliecinājumu, ka IKT procesi, produkti un pakalpojumi atbilst attiecīgajām drošības prasībām, tostarp drošības funkcijām, un ka tie ir izvērtēti līdz līmenim, kura mērķis ir minimizēt zināmos pamata riskus attiecībā uz kiberincidentiem un kiberuzbrukumiem. Izvērtējuma darbības ietver vismaz tehniskās dokumentācijas pārskatīšanu vai – ja tas nav piemērojams – alternatīvas darbības ar līdzvērtīgu ietekmi** [...];

b) **ar Eiropas kiberdrošības sertifikātu, kam ir norāde uz** apliecinājuma līmeni "būtisks", **sniedz apliecinājumu, ka IKT procesi, produkti un pakalpojumi atbilst attiecīgajām drošības prasībām, tostarp drošības funkcijām, un ka tie ir izvērtēti līdz līmenim, kura mērķis ir minimizēt zināmos kiberriskus, kiberincidentus un kiberuzbrukumus, ko veic subjekti ar ierobežotām prasmēm un resursiem. Izvērtējuma darbības ietver vismaz: pārskatīšanu saistībā ar publiski zināmu vājo vietu neattiecināmību un pārbaudi par to, vai ar IKT procesiem, produktiem vai pakalpojumiem ir pareizi īstenotas vajadzīgās drošības funkcijas; vai, ja tas nav piemērojams, tās ietver alternatīvas darbības ar līdzvērtīgu ietekmi** [...];

c) **ar Eiropas kiberdrošības sertifikātu, kam ir norāde uz** apliecinājuma līmeni "augsts", sniedz **apliecinājumu, ka IKT procesi, produkti un pakalpojumi atbilst attiecīgajām drošības prasībām, tostarp drošības funkcijām, un ka tie ir izvērtēti līdz līmenim, kura mērķis ir minimizēt sarežģītu kiberuzbrukumu risku, ko veic subjekti ar būtiskām prasmēm un resursiem. Izvērtējuma darbības ietver vismaz: pārskatīšanu saistībā ar publiski zināmu vājo vietu neattiecināmību, pārbaudi par to, vai ar IKT procesiem, produktiem vai pakalpojumiem ir pareizi īstenotas vajadzīgās drošības funkcijas – augstākajā līmenī –, un izvērtējumu ar ielaušanās testiem par to, vai tie ir noturīgi pret prasmīgu uzbrucēju uzbrukumiem; vai, ja tas nav piemērojams, tās ietver alternatīvas darbības ar līdzvērtīgu ietekmi** [...].

2.a Eiropas kiberdrošības sertifikācijas shēmā var noteikt vairākus izvērtējuma līmeņus atkarībā no tā, cik stingra un dziļa ir izvērtēšanas metodika. Katrs no izvērtējuma līmeņiem atbilst vienam no apliecinājuma līmeņiem un tiek definēts ar uzticamības komponentu atbilstošu kombināciju.

47. pants

Eiropas kiberdrošības sertifikācijas shēmu elementi

1. Eiropas kiberdrošības sertifikācijas shēmā ir **vismaz** šādi elementi:

a) sertifikācijas **shēmas** priekšmets un tvērums, tostarp ietverto IKT **procesu,** produktu un pakalpojumu tipi vai kategorijas**, kā arī skaidrojums par to, kā sertifikācijas shēma atbilst paredzamo mērķgrupu vajadzībām**;

b) [...] atsauce uz [...] starptautiskiem, **Eiropas vai valsts** standartiem **, kas izmantoti izvērtējumā. Ja standarti nav pieejami, sniedz atsauci uz** [...] tehniskajām specifikācijām**, kas atbilst Regulas 1025/2012 II pielikuma prasībām, vai, ja tādas nav pieejamas, uz tehniskajām specifikācijām vai citām kiberdrošības prasībām, kas ir definētas shēmā**;

c) attiecīgā gadījumā viens vai vairāki apliecinājuma līmeņi;

ca) attiecīgā gadījumā specifiskas vai papildu prasības, ko piemēro atbilstības novērtēšanas struktūrām, lai nodrošinātu, ka tām ir tehniskā kompetence izvērtēt kiberdrošības prasības;

d) konkrēti izvērtēšanas kritēriji un izmantotās metodes, tostarp izvērtēšanas veidi, ko izmanto, lai pierādītu, ka 45. pantā minētie konkrētie mērķi ir sasniegti;

e) **attiecīgā gadījumā** sertifikācijai nepieciešamā informācija, kas pieteikuma iesniedzējam jāsniedz **vai citādi jādara pieejama** atbilstības novērtēšanas struktūrām;

f) ja shēmā paredzētas zīmes vai marķējumi, – šādu zīmju vai marķējumu izmantošanas nosacījumi;

g) [...] noteikumi par sertifikātu **vai ES atbilstības apliecinājuma** prasību ievērošanas uzraudzību, tostarp mehānismi, kas izmantojami, lai pierādītu noteikto kiberdrošības prasību pastāvīgu ievērošanu;

h) **attiecīgā gadījumā** nosacījumi **sertifikāta** piešķiršanai **un atjaunošanai, kā arī** sertifikācijas tvēruma saglabāšanai, turpmākai izmantošanai, paplašināšanai **vai** samazināšanai;

i) noteikumi par sekām, ko rada sertificētu **vai pašnovērtētu** IKT produktu un pakalpojumu neatbilstība [...] **shēmas** prasībām;

j) noteikumi par kārtību, kādā jāziņo par iepriekš neidentificētām IKT **procesu,** produktu un pakalpojumu kiberdrošības vājajām vietām un kā tās jānovērš;

k) **attiecīgā gadījumā** noteikumi par uzskaites datu glabāšanu atbilstības novērtēšanas struktūrās;

l) to valsts **vai starptautisko** kiberdrošības sertifikācijas shēmu identifikācija, kas attiecas uz viena un tā paša veida vai kategoriju IKT **procesiem,** produktiem un pakalpojumiem**, drošības prasībām un izvērtēšanas kritērijiem un metodēm**;

m) izsniegtā sertifikāta **vai ES atbilstības apliecinājuma saturs;**

ma) ES atbilstības apliecinājuma un tehniskās dokumentācijas par visu attiecīgo informāciju glabāšanas laikposms, kas noteikts IKT produktu ražotājam vai pakalpojumu sniedzējam;

mb[...]) maksimālais sertifikātu derīguma termiņš;

mc[...]) izpaušanas politika attiecībā uz piešķirtajiem, grozītajiem un atsauktajiem sertifikātiem;

md[...]) nosacījumi sertifikācijas shēmu savstarpējai atzīšanai sadarbībā ar trešām valstīm;

me[...]) attiecīgā gadījumā salīdzinošās novērtēšanas mehānisma noteikumi struktūrām, kuras izdod Eiropas kiberdrošības sertifikātus par augstu apliecinājuma līmeni [...], ievērojot 48. panta 4.a punktu.

2. Shēmas noteiktās prasības nedrīkst būt pretrunā piemērojamajām juridiskajām prasībām, īpaši prasībām, kas izriet no saskaņotajiem Savienības tiesību aktiem.

3. Ja tas ir paredzēts konkrētā Savienības aktā, sertifikāciju **vai ES atbilstības apliecinājumu** atbilstīgi Eiropas kiberdrošības sertifikācijas shēmai var izmantot, lai pierādītu pieņēmumu par atbilstību minētā tiesību akta prasībām.

4. Ja saskaņoto Savienības tiesību aktu nav, dalībvalstu tiesību aktos var arī paredzēt, ka Eiropas kiberdrošības sertifikācijas shēmu var izmantot, lai noteiktu pieņēmumu par atbilstību juridiskajām prasībām.

47.a pants

Atbilstības pašnovērtējums

1. Eiropas kiberdrošības sertifikācijas shēmā var atļaut veikt atbilstības novērtējumu, par ko atbildīgs ir tikai pats IKT produktu ražotājs vai pakalpojumu sniedzējs. Šādu atbilstības novērtējumu attiecina tikai uz IKT produktiem un pakalpojumiem ar zemu risku, kas atbilst pamata atbilstības līmenim.

2. IKT produktu ražotājs vai pakalpojumu sniedzējs var izdot ES atbilstības apliecinājumu, kurā ir norādīts, ka atbilstība shēmā izklāstītajām prasībām ir pierādīta. Sagatavojot šādu apliecinājumu, IKT produktu ražotājs vai pakalpojumu sniedzējs uzņemas atbildību par IKT produkta vai pakalpojuma atbilstību shēmā izklāstītajām prasībām.

3. IKT produktu ražotājs vai pakalpojumu sniedzējs attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā noteiktajā laikposmā glabā 50. panta 1. punktā minētajai valsts kiberdrošības sertifikācijas iestādei pieejamu ES atbilstības apliecinājumu un tehnisko dokumentāciju par visu attiecīgos informāciju, kas saistīta ar IKT produktu vai pakalpojumu atbilstību shēmai. ES atbilstības apliecinājuma kopiju iesniedz valsts kiberdrošības sertifikācijas iestādei un *ENISA*.

4. ES atbilstības apliecinājuma izdošana ir fakultatīva, ja Savienības vai dalībvalstu tiesību aktos nav norādīts citādi.

5. ES atbilstības apliecinājums, kas izdots saskaņā ar šo pantu, tiek atzīts visās dalībvalstīs.

48. pants

Kiberdrošības sertifikācija

1. IKT **procesus,** produktus un pakalpojumus, kas ir sertificēti atbilstīgi Eiropas kiberdrošības sertifikācijas shēmai, kas pieņemta saskaņā ar 44. pantu, uzskata par atbilstīgiem minētās shēmas prasībām.

2. Sertifikācija ir fakultatīva, ja vien Savienības **vai dalībvalstu tiesību aktos** nav norādīts citādi.

3. Saskaņā ar šo pantu Eiropas kiberdrošības sertifikātu **ar pamata vai būtisku apliecinājuma līmeni** izdod 51. pantā minētās atbilstības novērtēšanas struktūras, pamatojoties uz kritērijiem, kuri iekļauti saskaņā ar 44. pantu pieņemtajā Eiropas kiberdrošības sertifikācijas shēmā.

4. Atkāpjoties no 3. punkta, pienācīgi pamatotos gadījumos konkrēta Eiropas kiberdrošības **sertifikācijas** shēma var paredzēt, ka atbilstīgi šai shēmai izveidotu Eiropas kiberdrošības sertifikātu var izdot tikai publiska struktūra. Šāda [...] struktūra ir viena no tālāk minētajām:

a) 50. panta 1. punktā minēta valsts **kiberdrošības** sertifikācijas [...] iestāde;

b) **publiska** struktūra, kas ir akreditēta kā atbilstības novērtēšanas struktūra saskaņā ar 51. panta 1. punktu [...]

c) [...].

4.a Gadījumos, kad Eiropas kiberdrošības sertifikācijas shēmā saskaņā ar 44. pantu noteikts augsts apliecinājuma līmenis, sertifikātu var izdot tikai 50. panta 1. punktā minēta valsts kiberdrošības sertifikācijas iestāde vai, ja ir turpmāk minētie nosacījumi, 51. pantā minēta atbilstības novērtēšanas struktūra:

a) ja valsts kiberdrošības sertifikācijas iestāde iepriekš apstiprinājusi katru atsevišķu sertifikātu, ko izdevusi atbilstības novērtēšanas struktūra; vai

b) ja valsts kiberdrošības sertifikācijas iestāde atbilstības novērtēšanas struktūrai iepriekš devusi vispārēju deleģējumu attiecībā uz šo uzdevumu.

5. Fiziska vai juridiska persona, kas par saviem IKT **procesiem,** produktiem vai pakalpojumiem iesniedz pieteikumu sertifikācijas mehānismā, [...] 51. pantā minētajai atbilstības novērtēšanas struktūrai **vai 50. pantā minētajai valsts kiberdrošības sertifikācijas iestādei, ja šī iestāde ir sertifikāta izdevēja struktūra, dara pieejamu** visu sertifikācijas procedūrā nepieciešamo informāciju.

5.a Sertifikāta turētājs sertifikāta izdevēju struktūru informē par jebkādām vēlāk atklātām IKT procesa, produkta vai pakalpojuma vājajām vietām vai neatbilstībām, kuras varētu ietekmēt ar sertifikāciju saistītās prasības. Struktūra šo informāciju bez liekas kavēšanās pārsūta valsts kiberdrošības sertifikācijas iestādei.

6. Sertifikātus izdod uz laikposmu, [...] **kas noteikts konkrētajā sertifikācijas shēmā,** un tos var atjaunot [...], ja vien joprojām ir ievērotas attiecīgās prasības.

7. Eiropas kiberdrošības sertifikāts, kas izsniegts atbilstīgi šim pantam, tiek atzīts visās dalībvalstīs.

49. pants

Valsts kiberdrošības sertifikācijas shēmas un sertifikāti

1. Neskarot 3. punktu, tādu IKT **procesu,** produktu un pakalpojumu valsts kiberdrošības sertifikācijas shēmas un saistītās procedūras, uz kuriem attiecas Eiropas kiberdrošības sertifikācijas shēma, zaudē spēku no datuma, kas noteikts saskaņā ar 44. panta 4. punktu pieņemtā īstenošanas aktā. Tādu IKT **procesu,** produktu un pakalpojumu valsts kiberdrošības sertifikācijas shēmas un saistītās procedūras, uz kuriem neattiecas Eiropas kiberdrošības sertifikācijas shēma, paliek spēkā arī turpmāk.

2. Dalībvalstis neievieš jaunas valsts kiberdrošības sertifikācijas shēmas IKT **procesiem,** produktiem un pakalpojumiem, uz kuriem jau attiecas spēkā esoša Eiropas kiberdrošības sertifikācijas shēma.

3. Spēkā esošie sertifikāti, kas izsniegti atbilstīgi valsts kiberdrošības sertifikācijas shēmām **un uz ko attiecas Eiropas kiberdrošības sertifikācijas shēma**, paliek spēkā līdz to termiņa beigām.

50. pants

Valsts* kiberdrošības *sertifikācijas [...] iestādes

1. Katra dalībvalsts [...] **savā teritorijā izraugās vienu vai vairākas** valsts **kiberdrošības** sertifikācijas [...] **iestādes vai – savstarpēji vienojoties ar citu dalībvalsti – izraugās minētajā citā dalībvalstī izveidotu vienu vai vairākas iestādes, kas būs atbildīgas par pārraudzības uzdevumiem dalībvalstī, kura to izraudzījusies**.

2. Katra dalībvalsts informē Komisiju par to, kuras **iestādes ir [...] izraudzītas, un par uzdevumiem, kuri tām uzticēti.**

3. **Neskarot 48. panta 4. punkta a) apakšpunktu un 4.a punktu,** [...] **k**atra valsts **kiberdrošības** sertifikācijas [...] iestāde organizatoriskās, tiesiskās struktūras un lēmumu pieņemšanas ziņā ir neatkarīga no tās pārraudzītajiem subjektiem.

3.a Dalībvalstis nodrošina, ka valsts kiberdrošības sertifikācijas iestādes darbībās, kas saistītas ar sertifikātu izdošanu saskaņā ar 48. panta 4. punkta a) apakšpunktu un 4.a punktu, tiek ievērots uzdevumu un pienākumu strikts nodalījums no uzraudzības darbībām šajā pantā un ka abas darbības funkcionē neatkarīgi viena no otras.

4. Dalībvalstis nodrošina, ka valsts **kiberdrošības** sertifikācijas [...] iestāžu rīcībā ir pietiekami līdzekļi, lai tās varētu īstenot savas pilnvaras un efektīvi un rezultatīvi veikt tām uzticētos uzdevumus.

5. Lai šīs regulas īstenošana būtu rezultatīva, ir vērts noteikt, ka šīs iestādes aktīvi, efektīvi, rezultatīvi un drošā veidā piedalās saskaņā ar 53. pantu izveidotajā Eiropas Kiberdrošības sertifikācijas grupā.

6. Valsts **kiberdrošības** sertifikācijas [...] iestādes:

a) [...]

aa) pārrauga to IKT produktu ražotāju vai pakalpojumu sniedzēju 47.a panta 2. un 3. punktā un attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā izklāstītos pienākumus, kuri veic uzņēmējdarbību šo iestāžu attiecīgajās teritorijās, un nodrošina šo pienākumu izpildi;

b) [...] **neskarot 51. panta 1.b punktu, palīdz valsts akreditācijas struktūrām pārraudzīt un uzraudzīt** šajā regulā paredzēto atbilstības novērtēšanas struktūru darbību [...];

ba) pārrauga un uzrauga 48. panta 4. punktā minēto struktūru darbību;

bb) izsniedz atļauju 51. panta 1.b punktā minētajām atbilstības novērtēšanas struktūrām un ierobežo, aptur vai atsauc esošu atļauju gadījumos, kad nav ievērotas šīs regulas prasības;

c) izskata sūdzības, ko fiziskas vai juridiskas personas iesniegušas saistībā ar [...] **valsts kiberdrošības sertifikācijas iestādes vai – saskaņā ar 48. panta 4.a punktu – atbilstības novērtēšanas struktūru** izdotiem sertifikātiem, pienācīgā mērā izmeklē sūdzības priekšmetu un samērīgā termiņā informē sūdzības iesniedzēju par lietas virzību un izmeklēšanas rezultātiem;

d) sadarbojas ar citām valsts **kiberdrošības** sertifikācijas [...] iestādēm vai citām publiskām iestādēm, piemēram, daloties informācijā par IKT **procesu,** produktu un pakalpojumu varbūtēju neatbilstību šīs regulas prasībām vai konkrētām Eiropas kiberdrošības sertifikācijas shēmām;

e) uzrauga būtiskas norises kiberdrošības sertifikācijas jomā.

7. Katrai valsts **kiberdrošības** sertifikācijas [...] iestādei ir vismaz šādas pilnvaras:

a) pieprasīt, lai atbilstības novērtēšanas struktūras**,** [...] Eiropas kiberdrošības sertifikātu turētāji **un ES atbilstības apliecinājuma izdevēji** sniegtu informāciju, ko tā pieprasījusi sava uzdevuma izpildei;

b) atbilstības novērtēšanas struktūrās**,** [...] Eiropas kiberdrošības sertifikātu turētāju **un ES atbilstības apliecinājuma izdevēju** struktūrās veikt izmeklēšanas, izmantojot revīzijas, lai pārbaudītu atbilstību III sadaļas noteikumiem;

c) saskaņā ar valsts tiesību aktiem veikt atbilstošus pasākumus, lai nodrošinātu, ka atbilstības novērtēšanas struktūras**,** [...] sertifikātu turētāji **un ES atbilstības apliecinājuma izdevēji** ievēro šīs regulas vai Eiropas kiberdrošības sertifikācijas shēmas prasības;

d) iegūt piekļuvi visām atbilstības novērtēšanas struktūru un Eiropas kiberdrošības sertifikātu turētāju telpām, lai tajās veiktu izmeklēšanu saskaņā ar Savienības vai dalībvalstu procesuālajiem tiesību aktiem;

e) saskaņā ar valsts tiesību aktiem atsaukt sertifikātus**, kurus izdevusi valsts kiberdrošības sertifikācijas iestāde vai – saskaņā ar 48. panta 4.a punktu – atbilstības novērtēšanas struktūras** un kuros nav ievērota atbilstība šai regulai vai Eiropas kiberdrošības sertifikācijas shēmai;

f) saskaņā ar valsts tiesību aktiem piemērot sankcijas, kas paredzētas 54. pantā, un nekavējoties pieprasīt izbeigt pārkāpumus saistībā ar šajā regulā noteikto pienākumu neievērošanu.

8. Valsts **kiberdrošības** sertifikācijas [...] iestādes sadarbojas savā starpā un ar Komisiju un jo īpaši apmainās ar informāciju, pieredzi un labu praksi attiecībā uz kiberdrošības sertifikācijas un tehniskiem jautājumiem, kas skar IKT **procesu,** produktu un pakalpojumu kiberdrošību.

51. pants

Atbilstības novērtēšanas struktūras

1. Atbilstības novērtēšanas struktūrām valsts akreditācijas struktūra, kuru izraugās saskaņā ar Regulu (EK) Nr. 765/2008, piešķir akreditāciju tikai tad, ja tās atbilst šīs regulas pielikumā izklāstītajām prasībām.

1.a Gadījumos, kad Eiropas kiberdrošības sertifikātu ir izdevusi valsts kiberdrošības sertifikācijas iestāde, ievērojot 48. panta 4. punkta a) apakšpunktu un 4.a punktu, valsts kiberdrošības sertifikācijas iestādes sertifikācijas struktūru akreditē kā atbilstības novērtēšanas struktūru, ievērojot šā panta 1. punktu.

1.b Attiecīgā gadījumā valsts kiberdrošības sertifikācijas iestāde savus uzdevumus atļauj veikt atbilstības novērtēšanas struktūrām, ja tās atbilst specifiskām vai papildu prasībām, kas izklāstītas Eiropas sertifikācijas shēmā, ievērojot 47. panta 1. punkta ca) apakšpunktu.

2. Akreditāciju piešķir uz laikposmu, kas nav ilgāks par pieciem gadiem, un to var atjaunot ar tādiem pašiem nosacījumiem, ja atbilstības novērtēšanas struktūra ir ievērojusi šajā pantā izklāstītās prasības. Ja atbilstības novērtēšanas struktūru akreditācijas nosacījumi nav vai vairs netiek izpildīti vai ja atbilstības novērtēšanas struktūras veiktie pasākumi pārkāpj šo regulu, akreditācijas struktūras **saprātīgā termiņā veic visus atbilstošos pasākumus, lai ierobežotu, apturētu vai** atsauktu akreditāciju, ievērojot šā panta 1. punktu.

52. pants

Paziņošana

1. Par katru Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta saskaņā ar 44. pantu, valsts **kiberdrošības** sertifikācijas [...] iestādes Komisijai paziņo, kuras [...] atbilstības novērtēšanas struktūras ir akreditētas **un attiecīgā gadījumā, ievērojot 51. panta 1.b punktu,** saņēmušas atļauju izsniegt sertifikātus konkrētos apliecinājuma līmeņos, kas aprakstīti 46. pantā, un bez liekas kavēšanās paziņo par tajā vēlāk veiktām izmaiņām.

2. Gadu pēc Eiropas kiberdrošības sertifikācijas shēmas stāšanās spēkā Komisija *Oficiālajā Vēstnesī* publicē to atbilstības novērtēšanas struktūru sarakstu, par kurām paziņots.

3. Ja Komisija paziņojumu saņem pēc tam, kad ir beidzies **2.** punktā [...] minētais termiņš, tā divu mēnešu laikā pēc minētā paziņojuma saņemšanas dienas *Eiropas Savienības Oficiālajā Vēstnesī* publicē grozījumus 2. punktā minētajā sarakstā.

4. Valsts **kiberdrošības** sertifikācijas [...] iestāde var iesniegt Komisijai pieprasījumu no šā panta 2. punktā minētā saraksta svītrot atbilstības novērtēšanas struktūru, par kuru paziņojusi minētā dalībvalsts. Mēneša laikā no dienas, kad saņemts valsts **kiberdrošības** sertifikācijas [...] iestādes pieprasījums, Komisija publicē *Eiropas Savienības Oficiālajā Vēstnesī* atbilstošos grozījumus sarakstā.

5. Pieņemot īstenošanas aktus, Komisija var noteikt nosacījumus, formātus un procedūras, kas jāievēro saistībā ar šā panta 1. punktā minēto paziņošanu. Minētos īstenošanas aktus pieņem saskaņā ar 55. panta 2. punktā noteikto pārbaudes procedūru.

53. pants

Eiropas Kiberdrošības sertifikācijas grupa

1. Izveido Eiropas Kiberdrošības sertifikācijas grupu ("Grupa").

2. Grupu veido valstu **kiberdrošības** sertifikācijas [...] iestāžu **pārstāvji vai citu attiecīgo valsts iestāžu pārstāvji**. [...] **Katrs Grupas pārstāvis var pārstāvēt ne vairāk kā vienu citu dalībvalsti**.

3. Grupai ir šādi uzdevumi:

a) dot padomus un palīdzēt Komisijai tās darbā, lai nodrošinātu šīs sadaļas konsekventu īstenošanu un piemērošanu, īpaši attiecībā uz kiberdrošības sertifikācijas politiku, politisko pieeju koordināciju un Eiropas kiberdrošības sertifikācijas shēmu izveidi;

b) palīdzēt, dot padomus *ENISA* un sadarboties ar to saistībā ar kandidātshēmas izveidi atbilstīgi šīs regulas 44. pantam;

ba) pieņemt atzinumu par kandidātshēmu, ievērojot šīs regulas 44. pantu;

c) [...] **pieprasīt** Aģentūrai izveidot Eiropas kiberdrošības sertifikācijas kandidātshēmu atbilstīgi šīs regulas 44. pantam;

ca) izstrādāt un pieņemt vadlīnijas par kritērijiem, saskaņā ar kuriem izvērtē priekšlikumus par [...] Grupai saskaņā ar 44. panta 1.a punktu iesniegtās kandidātshēmas sagatavošanu;

d) pieņemt Komisijai adresētus atzinumus, kas attiecas uz esošo Eiropas kiberdrošības sertifikācijas shēmu uzturēšanu un pārskatīšanu;

e) izvērtēt attiecīgās attīstības tendences kiberdrošības sertifikācijas jomā un īstenot paraugprakses apmaiņu kiberdrošības sertifikācijas shēmu jautājumos;

f) sekmēt valstu **kiberdrošības** sertifikācijas [...] iestāžu sadarbību atbilstīgi šai sadaļai, izmantojot **spēju veidošanu,** informācijas apmaiņu un jo īpaši ieviešot metodes efektīvai informācijas apmaiņai visos kiberdrošības sertifikācijas aspektos**;**

fa) sniegt atbalstu salīdzinošās novērtēšanas mehānisma īstenošanai saskaņā ar Eiropas kiberdrošības sertifikācijas shēmā paredzētajiem noteikumiem, ievērojot šīs regulas 47. panta 1. punkta md) apakšpunktu.

4. Komisija, kurai palīdz *ENISA*, kā paredzēts 8. panta a) apakšpunktā, **kā vadītāja** piedalās Grupas sanāksmes un nodrošina tās sekretariātu.

53.a pants

Tiesības iesniegt sūdzību valsts* kiberdrošības *sertifikācijas [...] iestādē

1. Fiziskām vai juridiskām personām ir tiesības iesniegt sūdzību valsts kiberdrošības sertifikācijas iestādē saistībā ar sertifikātu, ko izdevusi šī pati iestāde vai – saskaņā ar 48. panta 4.a punktu – atbilstības novērtēšanas struktūras.

2. Valsts kiberdrošības sertifikācijas iestāde, kurā ir iesniegta sūdzība, informē sūdzības iesniedzēju par sūdzības izskatīšanas virzību un iznākumu, tostarp par tiesību aizsardzības tiesā iespēju saskaņā ar 53.b pantu.

53.b pants

Tiesības uz efektīvu tiesību aizsardzību tiesā

1. Fiziskām vai juridiskām personām ir tiesības uz efektīvu tiesību aizsardzību tiesā pret valsts kiberdrošības sertifikācijas iestādes juridiski saistošu lēmumu, kas uz tām attiecas.

2. Fiziskām vai juridiskām personām ir tiesības uz efektīvu tiesību aizsardzību tiesā, ja valsts kiberdrošības sertifikācijas iestāde neizskata sūdzību.

3. Tiesvedību pret valsts kiberdrošības sertifikācijas iestādi uzsāk tās dalībvalsts tiesās, kurā iestāde ir izveidota.

54. pants

Sankcijas

Dalībvalstis pieņem noteikumus par sankcijām, ko piemēro par šīs sadaļas un Eiropas kiberdrošības sertifikācijas shēmu noteikumu pārkāpumiem, un veic visus vajadzīgos pasākumus, lai nodrošinātu to piemērošanu. Paredzētās sankcijas ir iedarbīgas, samērīgas un atturošas. Dalībvalstis minētos noteikumus un pasākumus [līdz …/nekavējoties] dara zināmus Komisijai un paziņo tai par visiem turpmākiem grozījumiem, kas tos ietekmē.

IV SADAĻA
NOBEIGUMA NOTEIKUMI

55. pants

Komiteju procedūra

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

2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. panta **4. punkta b) apakšpunktu**.

56. pants

Izvērtēšana un pārskatīšana

1. Ne vēlāk kā piecus gadus pēc 58. pantā minētā datuma un pēc tam reizi piecos gados Komisija novērtē Aģentūras un tās darba ietekmi, rezultativitāti un efektivitāti, kā arī iespējamo vajadzību mainīt Aģentūras pilnvaras un šādu izmaiņu finansiālo ietekmi. Izvērtējumā ņem vērā visu atgriezenisko informāciju, kas sniegta Aģentūrai, atbildot uz tās darbībām. Ja Komisija uzskata, ka Aģentūras turpmāka pastāvēšana vairs nav pamatota, ņemot vērā tai izvirzītos mērķus, piešķirtās pilnvaras un uzticētos uzdevumus, tā var ierosināt grozīt šīs regulas noteikumus, kuri attiecas uz Aģentūru.

2. Izvērtējumā nosaka arī III sadaļas noteikumu ietekmi, efektivitāti un rezultativitāti attiecībā uz mērķiem, kas paredz nodrošināt pienācīgi augstu IKT produktu un pakalpojumu kiberdrošības līmeni Savienībā un uzlabot iekšējā tirgus darbību.

3. Komisija nosūta izvērtējuma ziņojumu kopā ar saviem secinājumiem Eiropas Parlamentam, Padomei un Administratīvajai padomei. Minētā izvērtējuma ziņojuma konstatējumus publisko.

57. pants

Atcelšana un pēctecība

1. Regula (EK) Nr. 526/2013 tiek atcelta no [...].

2. Atsauces uz Regulu (EK) Nr. 526/2013 un uz *ENISA* uzskata par atsaucēm uz šo regulu un Aģentūru.

3. Aģentūra pārņem visas ar Regulu (EK) Nr. 526/2013 izveidotās Aģentūras īpašumtiesības, nolīgumus, juridiskos pienākumus, darba līgumus, finansiālās saistības un pasīvus. Visi spēkā esošie Administratīvās padomes un Valdes pieņemtie lēmumi paliek spēkā ar nosacījumu, ka tie nav pretrunā šīs regulas noteikumiem.

4. Aģentūru izveido uz nenoteiktu laikposmu, no [...].

5. Izpilddirektors, kas iecelts saskaņā ar Regulas (EK) Nr. 526/2013 24. panta 4. punktu, ir Aģentūras izpilddirektors atlikušo viņa pilnvaru termiņu.

6. Administratīvās padomes locekļi un viņu aizstājēji, kas iecelti saskaņā ar Regulas (EK) Nr. 526/2013 6. pantu, ir Aģentūras Administratīvās padomes locekļi un viņu aizstājēji atlikušo viņu pilnvaru termiņu/laiku.

58. pants

Stāšanās spēkā

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

1.a Šo regulu piemēro no [...], izņemot 50., 51., 52., 53.a, 53.b un 54. pantu, kurus piemēro no [24 mēneši pēc regulas publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*].

2. Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē,

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

PIELIKUMS

ATBILSTĪBAS NOVĒRTĒŠANAS STRUKTŪRĀM IZPILDĀMĀS PRASĪBAS

Atbilstības novērtēšanas struktūras, kuras vēlas akreditēties, izpilda šādas prasības:

1. Atbilstības novērtēšanas struktūra ir izveidota saskaņā ar valsts tiesību aktiem un ir juridiska persona.

2. Atbilstības novērtēšanas struktūra ir trešās personas struktūra, kas nav atkarīga no organizācijas vai IKT produktiem vai pakalpojumiem, ko tā novērtē.

3. Struktūra, kas pieder uzņēmumu apvienībai vai profesionālajai federācijai, kura pārstāv uzņēmumus, kas iesaistīti novērtējamo IKT produktu vai pakalpojumu izstrādē, ražošanā, piegādē, uzstādīšanā, lietošanā vai apkalpošanā, var tikt uzskatīta par atbilstības novērtēšanas struktūru, ja ir pierādīta tās neatkarība un interešu konflikta neesība.

4. Atbilstības novērtēšanas struktūra, tās augstākā vadība un personāls, kas atbild par atbilstības novērtēšanas uzdevumu izpildi, nav vērtējamo IKT produktu vai pakalpojumu izstrādātāji, ražotāji, piegādātāji, uzstādītāji, pircēji, īpašnieki, lietotāji vai apkalpotāji vai minēto personu pilnvaroti pārstāvji. Tas neliedz izmantot vērtējamos produktus, ja tie nepieciešami atbilstības novērtēšanas struktūras darbībai, un izmantot tos personiskām vajadzībām.

5. Atbilstības novērtēšanas struktūra, tās augstākā vadība un darbinieki, kas atbild par atbilstības novērtēšanas uzdevumiem, nav tieši saistīti ar šo IKT produktu vai pakalpojumu izstrādi, izgatavošanu vai konstruēšanu, tirdzniecību, uzstādīšanu, lietošanu vai apkalpošanu, kā arī nepārstāv minētajās darbībās iesaistītās personas. Tie neiesaistās darbībās, kas var būt pretrunā to spriedumu neatkarībai un godprātībai atbilstības novērtēšanas darbībās, par kuru veicējiem tie ir izsludināti. Tas īpaši attiecas uz konsultatīvajiem pakalpojumiem.

6. Atbilstības novērtēšanas struktūras nodrošina, ka atbilstības novērtēšanas darbību konfidencialitāti, objektivitāti un neitralitāti neietekmē to meitasuzņēmumu vai apakšuzņēmēju darbības.

7. Atbilstības novērtēšanas iestādes un to darbinieki veic atbilstības novērtēšanas darbības ar visaugstāko profesionālo godprātību un vajadzīgo tehnisko kompetenci konkrētajā jomā bez spiediena un pamudinājumiem, arī finansiāliem, kas varētu ietekmēt viņu lēmumu vai atbilstības novērtēšanas darbību rezultātus, īpaši attiecībā uz personām vai personu grupām, kuras ir ieinteresētas šo darbību rezultātos.

8. Atbilstības novērtēšanas iestāde spēj veikt saskaņā ar šo regulu piešķirtos atbilstības novērtēšanas uzdevumus – vai pati, vai tās uzdevumā kāds cits uz tās atbildību.

9. Atbilstības novērtēšanas struktūras rīcībā katrai atbilstības novērtēšanas procedūrai un katram IKT produktu un pakalpojumu veidam, grupai un apakšgrupai vienmēr ir vajadzīgie:

a) darbinieki ar tehniskām zināšanām un atbilstības novērtēšanas uzdevumu veikšanai pietiekamu un piemērotu pieredzi;

b) atbilstības novērtēšanas procedūru apraksti, kas nodrošina procedūru pārredzamību un iespēju tās atkārtot. Tai ir ieviesta piemērota politika un procedūras, kur uzdevumi, kurus tā veic par atbildīgo izsludinātās struktūras statusā, ir nodalīti no citām darbībām;

c) darbību veikšanas procedūras, kurās pienācīgi ņem vērā uzņēmuma lielumu, nozari, kur tas darbojas, uzbūvi, attiecīgā IKT produkta vai pakalpojuma tehnisko sarežģītību un to, vai ražošana notiek masveidā vai sērijveidā.

10. Atbilstības novērtēšanas struktūrai ir nepieciešamie līdzekļi, lai tā varētu pienācīgi izpildīt tehniskos un administratīvos uzdevumus, kas saistīti ar atbilstības novērtēšanas darbībām, un ir piekļuve visam nepieciešamajam aprīkojumam un iekārtām.

11. Darbiniekiem, kuri atbild par atbilstības novērtēšanas darbībām, ir:

a) laba tehniskā un profesionālā sagatavotība, kas aptver visas atbilstības novērtēšanas darbības;

b) pietiekamas zināšanas par veicamās novērtēšanas prasībām un atbilstošas pilnvaras šo novērtēšanu veikt;

c) pienācīgas piemērojamo prasību un testēšanas standartu zināšanas un izpratne;

d) māka sastādīt sertifikātus, dokumentāciju un ziņojumus, kas apliecina, ka ir veikta novērtēšana.

12. Tiek garantēta atbilstības novērtēšanas struktūru, to augstākās vadības un vērtēšanā iesaistīto darbinieku objektivitāte.

13. Atbilstības novērtēšanas struktūras augstākās vadības un vērtēšanā iesaistīto darbinieku atalgojums nav atkarīgs no novērtējumu skaita vai rezultātiem.

14. Tiek apdrošināta atbilstības novērtēšanas struktūru civiltiesiskā atbildība, ja vien atbildību saskaņā ar valsts tiesību aktiem neuzņemas valsts vai dalībvalsts pati tieši neatbild par atbilstības novērtēšanu.

15. Atbilstības novērtēšanas struktūras darbinieki glabā dienesta noslēpumu, kas skar visu informāciju, kura iegūta, veicot pienākumus, ko uzliek šī regula vai valsts tiesību normas, kas to īsteno, bet ne no to dalībvalstu kompetentajām iestādēm, kurās tiek veiktas tās darbības.

16. Atbilstības novērtēšanas struktūras atbilst **attiecīgā** standarta prasībām**, kurš ir saskaņots Regulā (EK) Nr. 765/2008 attiecībā uz to atbilstības novērtēšanas struktūru akreditāciju, kas veic procesu, produktu vai pakalpojumu sertifikāciju** [...].

17. Atbildības novērtēšanas struktūras nodrošina, ka atbilstības novērtēšanai izmantotās testēšanas laboratorijas atbilst **attiecīgā** standarta prasībām**, kurš ir saskaņots Regulā (EK) Nr. 765/2008 attiecībā uz to laboratoriju akreditāciju, kas veic testēšanu** [...].