Eiropas Savienības
Padome

Briselē, 2018. gada 1. martā
(OR. en)

12183/2/17
REV 2

Starpiestāžu lieta:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139
CSC 276
CSCI 68

PRIEKŠLIKUMS

K-jas dok. Nr.:	COM(2017) 477 final/3
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")

Pielikumā ir pievienots dokuments COM(2017) 477 *final/3*.

Pielikumā: COM(2017) 477 *final/3*

EIROPAS
KOMISIJA

Briselē, 22.2.2018.
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

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")

(Dokuments attiecas uz EEZ)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Eiropas Savienība ir veikusi daudzus pasākumus, kas vairo noturību un uzlabo tās kiberdrošības gatavību. Pirmajā ES kiberdrošības stratēģijā[1], ko pieņēma 2013. gadā, tika noteikti stratēģiskie mērķi un konkrēti pasākumi, ar kuriem paredzēts panākt noturību, mazināt kibernoziedzību, attīstīt kiberaizsardzības politiku un spējas, izstrādāt nepieciešamos rūpnieciskos un tehnoloģiskos resursus un Eiropas Savienībā ieviest saskanīgu starptautiskās kibertelpas politiku. Kopš tā laika ir notikušas svarīgas pārmaiņas, proti, ir otrreiz dotas pilnvaras Eiropas Savienības Tīklu un informācijas drošības aģentūrai (*ENISA*)[2] un pieņemta **Direktīva par tīklu un informācijas sistēmu drošību**[3] ("TID direktīva"), kas ir šā priekšlikuma pamatā.

Bez tam **2016. gadā Eiropas Komisija pieņēma paziņojumu "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari"**[4], ar ko tika izziņoti pasākumi, kas vēl vairāk pastiprina sadarbību, dalīšanos informācijā un zināšanās un paaugstina ES noturību un gatavību, ņemot vērā arī izredzes piedzīvot plašapmēra incidentus un Eiropas mēroga kiberdrošības krīzi. Šajā sakarā Komisija paziņoja, ka **izvērtēs** un **pārskatīs** Eiropas Parlamenta un Padomes Regulu (ES) Nr. 526/2013 par *ENISA* un Regulas (EK) Nr. 460/2004 atcelšanu ("*ENISA* regulu"). Vērtēšanas rezultātā varētu nākties Aģentūru reformēt un uzlabot tās jaudas un spēju pastāvīgi atbalstīt dalībvalstis. Tai tiktu operatīvāka un atbildīgāka loma kiberdrošības noturības panākšanā, un tās jaunajās pilnvarās tiktu atzīti jaunie pienākumi, ko tai uzliek TID direktīva.

TID direktīva ir pirmais būtiskais solis riska pārvaldības kultūras veicināšanā, un tā ievieš drošības prasības kā juridisku pienākumu galvenajiem ekonomikas subjektiem, proti, uzņēmumiem, kuri sniedz pamatpakalpojumus ("pamatpakalpojumu sniedzējiem"), un dažu svarīgāko digitālo pakalpojumu sniedzējiem ("digitālo pakalpojumu sniedzējiem"). Drošības prasību ievērošana tiek uzskatīta par būtisku sabiedrības progresējošās digitalizācijas labumu nodrošināšanā, un strauji izplatās satīklotās ierīces (lietu internets jeb *IoT*), tāpēc 2016. gada paziņojumā arī tika ierosināts izveidot informācijas un komunikācijas tehnoloģiju (IKT) produktu un pakalpojumu drošības sertifikācijas regulējumu, lai digitālajā vienotajā tirgū vairotu uzticēšanos un drošību. IKT kiberdrošības sertifikācija kļūst īpaši svarīga, kad arvien plašāk tiek izmantotas tehnoloģijas, kas prasa augstu kiberdrošības līmeni, kā satīkloti un automatizēti auto, elektroniskā veselības aprūpe vai ražošanas automatizācijas vadības sistēmas (*IACS*).

Šos politiskos pasākumus un paziņojumus vēl vairāk nostiprināja 2016. gada **Padomes secinājumi**, atzīstot, ka "kiberdraudi un ievainojamība turpina attīstīties un pastiprināties, kas prasīs nepārtrauktu un ciešāku sadarbību, jo īpaši, pārvarot plaša mēroga pārrobežu

---

1 Eiropas Komisijas un Eiropas Ārējās darbības dienesta kopīgs paziņojums "Eiropas Savienības kiberdrošības stratēģija – atvērta un droša kibertelpa", JOIN(2013).

2 Regula (ES) Nr. 526/2013 par Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*) un ar ko atceļ Regulu (EK) Nr. 460/2004.

3 Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

4 Komisijas paziņojums "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari", COM(2016)0410 *final*.

kiberdrošības incidentus". Secinājumos apstiprināts, ka *ENISA* regula ir viens no ES kibernoturības sistēmas galvenajiem elementiem[5], un Komisija aicināta veikt tālākus pasākumus Eiropas līmeņa sertifikācijas jautājuma risināšanā.

Sertifikācijas sistēmas izveidei būtu vajadzīgs ES līmenī ieviest piemērotu pārvaldības sistēmu, izmantojot arī ekspertu lietpratību, par ko gādātu neatkarīga ES aģentūra. Tādējādi šajā priekšlikumā *ENISA* tiek atzīta par to ES līmeņa iestādi, kurai ir kompetence kiberdrošības jautājumos un būtu jāuzņemas savest kopā un koordinēt valstu kompetentās iestādes, kas darbojas sertifikācijas laukā.

Paziņojumā par **Digitālā vienotā tirgus stratēģijas vidusposma pārskatu 2017. gada maijā** Komisija precizēja, ka 2017. gada septembrī būs pārskatījusi *ENISA* pilnvaras. Tas tiek darīts nolūkā noteikt *ENISA* lomu mainītajā kiberdrošības ekosistēmā un izstrādāt pasākumus kiberdrošības standartu, sertifikācijas un marķēšanas jomā, lai uzlabotu IKT sistēmu kiberdrošību, aptverot arī satīklotos objektus[6]. **Eiropadome 2017. gada jūnija secinājumos**[7] atzinīgi novērtēja Komisijas nodomu septembrī pārskatīt kiberdrošības stratēģiju un līdz 2017. gada beigām ierosināt arī citus mērķētus pasākumus.

Regulas priekšlikums paredz visaptverošu pasākumu kopumu, kas papildinātu iepriekšējo rīcību un palīdzētu sasniegt konkrētus savstarpēji pastiprinošus mērķus:

- pastiprināt dalībvalstu un uzņēmumu **spējas un gatavību**,
- uzlabot **sadarbību un koordināciju** starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām,
- uzlabot **ES līmeņa spējas papildināt dalībvalstu rīcību**, it īpaši pārrobežu kiberkrīžu gadījumā,
- uzlabot pilsoņu un uzņēmumu **izpratni** kiberdrošības jautājumos,
- uzlabot IKT produktu un pakalpojumu **kiberdrošības apliecinājuma vispārējo pārredzamību**[8], lai vairotu uzticēšanos digitālajam vienotajam tirgum un digitālajai inovācijai, un
- nepieļaut ES **sertifikācijas shēmu** un ar tām saistīto drošības prasību un izvērtēšanas kritēriju **nevienveidību** dažādās dalībvalstīs un nozarēs.

Tālāk šajā paskaidrojuma rakstā sīkāk iztirzāti tādi iniciatīvas pamatojuma aspekti kā ierosinātā *ENISA* darbība un kiberdrošības sertifikācija.

---

5 Padomes 2016. gada 15. novembra secinājumi par paziņojumu "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari".

6 Komisijas paziņojums par digitālā vienotā tirgus stratēģijas īstenošanas vidusposma pārskatu, COM(2017) 228.

7 Eiropadomes 2017. gada 22. un 23. jūnija sanāksmes secinājumi, EUCO 8/17.

8 Kiberdrošības apliecinājuma pārredzamība nozīmē, ka lietotāji tiek pietiekami informēti par kiberdrošības rekvizītiem, kas lietotājiem ļauj objektīvi noteikt konkrētā IKT produkta, pakalpojuma vai procesa drošības līmeni.

ENISA

ENISA darbojas kā lietpratības centrs, kura sūtība ir Savienībā uzlabot tīklu un informācijas drošību un atbalstīt dalībvalstu spēju veidošanu.

ENISA tika izveidota 2004. gadā[9], lai tuvinātu vispārējo mērķi visā ES augstā līmenī nodrošināt tīklu un informācijas drošību. 2013. gadā Regula (ES) Nr. 526/2013 deva Aģentūrai jaunas pilnvaras – uz septiņiem gadiem, līdz 2020. gadam. Aģentūra atrodas Grieķijā, proti, administratīvā ēka ir Hēraklejā (Krētā), bet pamatdarbība notiek Atēnās.

Salīdzinājumā ar citām ES aģentūrām *ENISA* ir maza aģentūra ar nelielu budžetu un darbinieku skaitu. Tās pilnvaras tiek piešķirtas uz noteiktu laiku.

ENISA palīdz Eiropas iestādēm, dalībvalstīm un komersantiem **reaģēt uz tīklu un informācijas drošības problēmām, tās risināt un, galvenais, laikus novērst**. Tā veic virkni darbību tās stratēģijā noteiktās piecās jomās[10]:

- Lietpratība – informācijas un ekspertu zināšanu nodrošināšana galvenajos tīklu un informācijas drošības jautājumos.
- Politika – atbalsts politikas veidošanai un iedzīvināšanai Savienībā.
- Spējas – spēju veidošanas atbalste visā Savienībā (piem., apmācība, ieteikumi, izpratnes uzlabošanas pasākumi).
- Kopiena – tīklu un informācijas drošības kopienas veidošana (piemēram, datorapdraudējumu reaģēšanas vienību (*CERT*) atbalstīšana, Eiropas mēroga kibermācību koordinēšana).
- Iespējošana (piem., saistīšanās ar ieinteresētajām personām un starptautiskās attiecības).

TID direktīvas apspriešanas gaitā ES likumdevēji nolēma svarīgas šās direktīvas īstenošanas funkcijas nodot *ENISA*. Konkrēti, Aģentūra nodrošina sekretariātu *CSIRT* tīklam (tas izveidots, lai veicinātu ātru un rezultatīvu operatīvo sadarbību starp dalībvalstīm konkrētos kiberdrošības incidentos un dalīšanos informācijā par riskiem), un tai tiek arī uzdots palīdzēt Sadarbības grupai pildīt savus uzdevumus. Direktīva arī prasa, lai *ENISA* palīdzētu dalībvalstīm un Komisijai ar lietpratību un padomu un atvieglinātu paraugprakses pārņemšanu.

Saskaņā ar *ENISA* regulu Komisija ir veikusi izvērtēšanu, kur ietilpst neatkarīgs pētījums, kā arī sabiedriskā apspriešana. Izvērtējot tika skatīts Aģentūras darbības nozīmīgums, ietekme, rezultativitāte, efektivitāte, saskanība un ES pievienotā vērtība laikposmā no 2013. līdz 2016. gadam tādos aspektos kā veiktspēja, pārvaldība, iekšējā uzbūve un darba metodes.

Sabiedriskajā apspriešanā respondentu vairākums (74 %) *ENISA* darbību visumā vērtē atzinīgi[11]. Lielākā daļa respondentu arī uzskata, ka *ENISA* sasniedz dažādus mērķus (vismaz

---

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

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy.

11 90 ieinteresētās personas no 19 dalībvalstīm, kas piedalījās apspriešanā (88 atbildes un 2 nostājas dokumenti), ieskaitot valsts iestādes no 15 dalībvalstīm un 8 jumta organizācijas, kas pārstāv ievērojamu skaitu Eiropas uzņēmumu.

63 % par katru no mērķiem). *ENISA* pakalpojumus un produktus regulāri (reizi mēnesī vai biežāk) izmanto gandrīz puse respondentu (46 %), un tos atzinīgi vērtē gan tādēļ, ka tie nāk no ES līmeņa iestādes (83 %), gan kvalitātes dēļ (62 %).

Tomēr ievērojams aptaujāto vairākums (88 %) uzskata, ka pašreizējie ES līmenī pieejamie instrumenti un mehānismi nav pietiekami vai ir tikai daļēji pietiekami tagadējo kiberdrošības problēmu risināšanai. Lielais vairums respondentu (98 %) norāda, ka būtu vajadzīga ES iestāde, kas apmierinātu šīs vajadzības, un aģentūru *ENISA* par piemērotāko organizāciju uzskata 99 % respondentu. Bez tam 67,5 % respondentu pauž viedokli, ka aģentūrai *ENISA* varētu būt zināma loma saskaņota tiesiskā satvara izveidē IT produktu un pakalpojumu drošības sertifikācijai.

Vispārējā izvērtēšanā (ne tikai uz sabiedriskās apspriešanas, bet arī uz daudzu individuālu interviju, papildinošu mērķapsekojumu un darbsemināru pamata) tika izdarīti šādi secinājumi:

- *ENISA* mērķi joprojām ir aktuāli. Strauji attīstoties tehnoloģijai, vairojoties apdraudējumam un visā pasaulē samilstot kiberriskiem, ir skaidrs, ka ES ir vajadzīgs veicināt un nostiprināt augsta līmeņa tehnisko lietpratību kiberdrošības jautājumos. Dalībvalstīs ir jāattīsta spēja apdraudējumu izprast un reaģēt uz to, un ir jāsadarbojas dažādu tematisko jomu un iestāžu ieinteresētajām personām.
- Par spīti tam, ka budžets neliels, Aģentūra operatīvajā ziņā ir lietderīgi izmantojusi resursus un izpildījusi uzdevumus. Papildu administratīvās izmaksas gan radījis izvietojums atšķirīgās vietās – Atēnās un Hēraklejā.
- Rezultativitātes ziņā *ENISA* savus mērķus sasniegusi pa daļai. Aģentūra ir sekmīgi palīdzējusi uzlabot tīklu un informācijas drošību Eiropā, piedāvājot spēju veidošanu 28 dalībvalstīs[12], veicinot sadarbību starp dalībvalstīm un tīklu un informācijas drošības ieinteresētajām personām un liekot lietā ekspertu zināšanas, veidojot kopienu un atbalstot politikas veidošanu. Kopumā *ENISA* čakli nodevusies savas darba programmas īstenošanai un bijusi uzticama partnere ieinteresētajām personām sfērā, kurai tikai nesen atzīta tāda liela pārrobežu nozīme.
- *ENISA* jaudāja cik necik ietekmēt plašo tīklu un informācijas drošības jomu, taču tai nav pilnībā izdevies izveidot spēcīgu zīmolu un iemantot pietiekamu pazīstamību, lai taptu atzīta par Eiropas lietpratības centru. Izskaidrojums tam ir *ENISA* plašo pilnvaru un mazo resursu nesamērība. Turklāt *ENISA* joprojām ir vienīgā ES aģentūra ar noteikta termiņa pilnvarām, tādējādi ar ierobežotu spēju attīstīt ilgtermiņa ieceres un pastāvīgi atbalstīt ieinteresētās personas. Tas arī ir pretstatā TID direktīvas normām, kas *ENISA* uztic uzdevumus bez noteikta termiņa. Visbeidzot, izvērtējot tika konstatēts, ka mazrezultativitāti daļēji var skaidrot ar ārējo ekspertu lielo pārsvaru pār štata ekspertiem un grūtībām nolīgt un pieturēt darbā specializētu personālu.

[12] Sabiedriskajā apspriešanā respondentus aicināja norādīt, kurus *ENISA* sasniegumus viņi uzskata par galvenajiem 2013.–2016. gadā. Visu grupu respondenti (kopā 55, to vidū 13 no valsts iestādēm, 20 no privātā sektora un 22 "citi") par *ENISA* galvenajiem sasniegumiem uzskata: 1) mācību *Cyber Europe* koordinēšanu, 2) atbalstu *CERT/CSIRT* ar apmācību un darbsemināriem, kas sekmē koordināciju un apmaiņu, 3) *ENISA* publikācijas (vadlīnijas un ieteikumus, apdraudējuma ainas pārskatus, stratēģiju ziņošanai par incidentiem un krīzes pārvaldību utt.), kas tiek uzskatītas par lietderīgām valstu drošības sistēmu izveidošanā un atjaunināšanā, kā arī par uzziņu avotu politikas veidotājiem un kiberdrošības praktiķiem, 4) palīdzību TID direktīvas popularizēšanā, 5) centienus ar kiberdrošības mēnesi uzlabot izpratni par kiberdrošību.

- Tikpat svarīgs ir izvērtēšanas secinājums, ka *ENISA* pievienotā vērtība galvenokārt izpaužas kā Aģentūras spēja uzlabot sadarbību galvenokārt starp dalībvalstīm, it īpaši ar tīklu un informācijas drošības kopienām (sevišķi *CSIRT*). ES līmenī nav citu struktūru, kas atbalstītu tik plašu tīklu un informācijas drošības jautājumos ieinteresēto personu loku. Taču, tā kā *ENISA* vajadzīgs saviem pasākumiem stingri noteikt prioritātes, darba programmā tā lielāko tiesu vadās pēc dalībvalstu vajadzībām. Rezultātā netiek pietiekami risinātas citu ieinteresēto personu, īpaši nozarē strādājošo, vajadzības. Tas arī ļāvis Aģentūrai apmierināt tikai galveno ieinteresēto personu vajadzības, bet ne panākt lielāku ietekmi. Tādēļ Aģentūras darba pievienotā vērtība nebija vienāda atkarā no ieinteresēto personu vajadzību atšķirībām un no tā, kādā mērā Aģentūra spēja uz tām atsaukties (piem., lielas dalībvalstis pretstatā mazām, dalībvalstis pretstatā nozarei).

Kopumā apspriešanos ar ieinteresētajām personām un izvērtējuma rezultāti liecina, ka *ENISA* resursi un pilnvaras ir jākoriģē, lai tā varētu pienācīgi reaģēt uz tagadējiem un nākošiem izaicinājumiem.

Visa konstatētā dēļ šajā priekšlikumā ir pārskatītas *ENISA* pašreizējās pilnvaras un noteikts jaunu uzdevumu un funkciju kopums nolūkā rezultatīvi un efektīvi atbalstīt dalībvalstu, ES iestāžu un citu ieinteresēto personu pūliņus Eiropas Savienībā nodrošināt drošu kibertelpu. Ierosinātās jaunās pilnvaras cenšas piešķirt Aģentūrai lielāku un nozīmīgāku lomu, īpaši tādu, ka tā arī palīdzētu dalībvalstīm īstenot TID direktīvu un aktīvāk vērstos pret konkrētu apdraudējumu (operatīvās jaudas) un kļūtu par lietpratības centru, kas atbalsta dalībvalstis un Komisiju kiberdrošības sertifikācijas lietās. Priekšlikumā paredzēts:

- *ENISA* saņem pastāvīgas pilnvaras un iegūst stabilu pamatu turpmākam darbam. Pilnvaras, mērķi un uzdevumi paliek regulāri pārskatāmi.
- Ierosinātās pilnvaras precizē *ENISA* lomu būt par ES kiberdrošības aģentūru un uzziņas punktu ES kiberdrošības ekosistēmā, rīkojoties ciešā sadarbībā ar pārējām attiecīgajām tādas ekosistēmas struktūrām.
- Aģentūras organizācija un pārvaldība, kas novērtēta pozitīvi, tiek mēreni pārskatīta, lai nodrošinātu, ka tās darbā labāk atspoguļojas plašākas ieinteresēto personu kopas vajadzības.
- Ierosināto pilnvaru darbības joma tiek stingri noteikta, nostiprinot jomas, kurās Aģentūra ir apliecinājusi nepārprotamu pievienoto vērtību, un pievienojot jaunas jomas, kurām vajadzīgs atbalsts, ņemot vērā jaunās politiskās prioritātes un instrumentus, sevišķi TID direktīvu, ES kiberdrošības stratēģijas pārskatīšanu, gaidāmo ES kiberdrošības plānu sadarbībai kiberkrīžu jomā un IKT drošības sertifikāciju.
    - **ES politikas izstrāde un īstenošana.** *ENISA* saņemtu uzdevumu aktīvi palīdzēt tīklu un informācijas drošības politikas izstrādē, kā arī citās politikas iniciatīvās, kas saistītas ar kiberdrošības elementiem dažādās nozarēs (piem., enerģētikā, transportā, finansēs). Šim nolūkam tai būtu spēcīga padomdevējas loma, kuru tā varētu izpildīt ar neatkarīgiem atzinumiem un priekšdarbiem politikas un tiesību aktu izstrādāšanai un atjaunināšanai. *ENISA* arī atbalstītu ES politiku un tiesību aktus tādās jomās kā elektroniskie sakari, elektroniskā identifikācija un uzticamības pakalpojumi, lai paaugstinātu kiberdrošības līmeni. Īstenošanas posmā, īpaši saistībā ar TID Sadarbības grupu, *ENISA* palīdzētu dalībvalstīm ieviest konsekventu pieeju TID direktīvas īstenošanā pāri robežām un starp nozarēm, kā arī citās attiecīgās politikas jomās un tiesību

aktos. Lai atbalstītu kiberdrošības politikas un tiesību aktu regulāru pārskati, *ENISA* arī nodrošinātu regulāru ziņošanu par ES tiesiskā regulējuma īstenošanu.

- **Spēju veidošana.** *ENISA* palīdzētu uzlabot ES un valstu publisko iestāžu spējas un lietpratību, citastarp reaģēšanā uz incidentiem un ar kiberdrošību saistītu regulatīvu pasākumu pārraudzīšanā. Aģentūrai būtu arī jāpalīdz dažādās nozarēs izveidot informācijas apmaiņas un analīzes centrus (*ISAC*), nodrošinot paraugpraksi un norādījumus par pieejamiem rīkiem un procedūrām, kā arī pienācīgi risinot regulatīvos jautājumus, kas saistīti ar informācijas apmaiņu.
- **Zināšanas un informācija, izpratnes uzlabošana.** *ENISA* kļūtu par ES informācijas mezglu. Tas nozīmētu visā ES veicināt un kopīgot paraugpraksi un iniciatīvas, sakopojot informāciju par kiberdrošību no ES un dalībvalstu iestādēm, aģentūrām un struktūrām. Aģentūra arī darītu pieejamus padomus, norādījumus un paraugpraksi kritisko infrastruktūru drošības sfērā. Pēc ievērojamiem pārrobežu kiberdrošības incidentiem *ENISA* turpinātu apkopot ziņojumus ar mērķi dot norādījumus uzņēmumiem un pilsoņiem visā ES. Šis darba virziens nozīmētu arī regulāru izpratnes uzlabošanas pasākumu organizēšanu, tos koordinējot ar dalībvalstu iestādēm.
- **Ar tirgu saistīti uzdevumi (standartizācija, kiberdrošības sertifikācija).** *ENISA* pildītu vairākas funkcijas, īpaši atbalstot iekšējo tirgu, un veidotu kiberdrošības "tirgus novērošanas centru", analizējot attiecīgas kiberdrošības tirgus tendences, lai labāk saskaņotu pieprasījumu un piedāvājumu, un atbalstot ES politikas izstrādi IKT standartizācijas un IKT kiberdrošības sertifikācijas sfērās. Standartizācijas sfērā tā veicinātu kiberdrošības standartu noteikšanu un ieviešanu. *ENISA* arī izpildītu uzdevumus, kas paredzēti sakarā ar topošo sertifikācijas satvaru (sk. nākamo iedaļu).
- **Pētniecība un inovācija.** *ENISA* liktu lietā savu lietpratību, konsultējot ES un valstu iestādes par prioritāšu noteikšanu pētniecībā un izstrādē, arī saistībā ar publiskā un privātā sektora līgumiskās partnerības izveidi kiberdrošības sfērā (*cPPP*). *ENISA* padomi pētniecībā tiktu izmantoti jaunajā Eiropas Kiberdrošības pētniecības un kompetences centrā saskaņā ar nākamo daudzgadu finanšu shēmu. Pēc Komisijas lūguma *ENISA* arī iesaistītos ES pētniecības un inovācijas finansēšanas programmu īstenošanā.
- **Operatīvā sadarbība un krīžu pārvarēšana.** Šim darba virzienam būtu jābalstās uz pašreizējo profilaktiskās darbības spēju stiprināšanu, it īpaši, modernizējot Eiropas mēroga kiberdrošības mācības (*Cyber Europe*) un rīkojot tās katru gadu, un uz atbalstu operatīvajā sadarbībā *CSIRT* tīkla sekretariāta lomā (tā noteikta TID direktīvā), cita starpā nodrošinot *CSIRT* tīkla IT infrastruktūras un saziņas kanālu pienācīgu darbošanos. Šajā sakarā būtu vajadzīga strukturēta sadarbība ar *CERT-EU*, Eiropas Kibernoziedzības apkarošanas centru (*EC3*) un citām attiecīgām ES struktūrām. Turklāt, veidojot strukturētu sadarbību ciešā fiziskā tuvumā ar *CERT-EU*, tā īstenotu funkciju, kas nodrošina tehnisku palīdzību nopietnu incidentu gadījumos un atbalsta incidentu analīzi. Dalībvalstis pēc pieprasījuma saņemtu palīdzību incidentu pārvarēšanā un atbalstu vājo vietu, artefaktu un incidentu analīzei, lai stiprinātu savas profilakses un reaģēšanas spējas.

- *ENISA* būtu arī zināma loma paketē iekļautajā **ES kiberdrošības plānā**, kur izklāstīts Komisijas ieteikums dalībvalstīm par koordinētu reaģēšanu uz plašapmēra pārrobežu kiberdrošības incidentiem un krīzēm ES līmenī[13]. *ENISA* arī veicinātu sadarbību starp atsevišķām dalībvalstīm, kuras reaģē ārkārtas situācijās, – analizētu un apkopotu valstu ziņojumus par situāciju, balstoties uz Aģentūrai brīvprātīgi piegādāto informāciju no dalībvalstīm un citām struktūrām.

- **IKT produktu un pakalpojumu kiberdrošības sertifikācija**

Lai radītu un saglabātu uzticēšanos un drošību, IKT produktos un pakalpojumos no paša projektēšanas un izstrādes sākuma jābūt iekļautiem drošības elementiem (ieprojektētai drošībai). Patērētājiem un lietotājiem vajadzīga arī iespēja noskaidrot, kāds ir pasūtāmā vai pērkamā produkta vai pakalpojuma drošības apliecinājuma līmenis.

Svarīga loma produktu un pakalpojumu drošības un uzticamības vairošanā ir sertifikācijai, kas nozīmē produktu, pakalpojumu un procesu oficiālu novērtēšanu, ko pēc noteiktiem standartkritērijiem izdara neatkarīga akreditēta struktūra, un atbilstības sertifikāta izdošanu. Drošības izvērtēšana ir visai tehniska lieta, taču sertifikācija kalpo mērķim informēt un pārliecināt pircējus un lietotājus par pērkamo vai lietojamo IKT produktu un pakalpojumu drošības rekvizītiem. Kā jau teikts, tas ir īpaši svarīgi jaunajās sistēmās, kas plaši izmanto ciparu tehnoloģijas un kam vajadzīgs augsts drošības līmenis, kā satīkloti un automatizēti auto, elektroniskā veselība, ražošanas automatizācijas vadības sistēmas (*IACS*)[14] vai viedtīkli.

Pašlaik IKT produktu un pakalpojumu kiberdrošības sertifikācijas aina Eiropas Savienībā ir raiba. Ir vairākas starptautiskas iniciatīvas, piemēram, t. s. informācijas tehnoloģiju drošības novērtēšanas kopīgie kritēriji ("*CC*") (ISO 15408), kas ir starptautisks datordrošības vērtēšanas standarts. Tas balstās uz izvērtēšanu, ko izdara trešās personas, un paredz septiņus izvērtējuma apliecinājuma līmeņus (*EAL*). *CC* un ar to saistītā informācijas tehnoloģiju drošības izvērtēšanas (*CEM*) kopīgā metodika ir tehniskais pamats starptautiskam nolīgumam jeb kopīgo kritēriju atzīšanas kārtībai (*CCRA*), kas nodrošina, ka *CC* sertifikātus atzīst visi *CCRA* parakstītāji. Tomēr *CCRA* pašreizējā redakcijā savstarpēji atzīti tiek tikai izvērtējumi līdz līmenim *EAL 2*. Bez tam nolīgumu parakstījušas tikai 13 dalībvalstis.

12 dalībvalstu sertifikācijas iestādes ir noslēgušas savstarpējās atzīšanas nolīgumu par sertifikātiem, kas saskaņā ar nolīgumu izdoti uz *CC* pamata[15]. Turklāt tagad dalībvalstīs pastāv vai tiek veidotas vairākas IKT sertifikācijas iniciatīvas. Šīs iniciatīvas var būt svarīgas, taču tās rada tirgus sadrumstalotības un sadarbspējas problēmu risku. Rezultātā uzņēmumam, lai varētu piedāvāt savu produktu vairākos tirgos, var būt jāiztur vairākas sertifikācijas procedūras dažādās dalībvalstīs. Piemēram: ja kāds viedskaitītāju ražotājs vēlas savu

---

13 "Plāns" attieksies uz kiberdrošības incidentiem, kuru radītais traucējums ir pārāk plašs, lai dalībvalsts to pārvarētu viena, vai skar divas vai vairāk dalībvalstis ar tik plašu un būtisku ietekmi vai politisko nozīmi, ka ir vajadzīga laicīga politikas koordinācija un reaģēšana Savienības politiskajā līmenī.

14 *JRC* ĢD ir publicējis ziņojumu, kurā liek priekšā sākotnēju kopīgu Eiropas prasību un vispārēju vadlīniju kopumu, kas attiektos uz *IACS* komponentu kiberdrošības sertifikāciju. Pieejams adresē https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf.

15 Informācijas sistēmu drošības augstāko amatpersonu grupā (*SOG-IS*) ietilpst 12 dalībvalstis un Norvēģija, un tā ir izstrādājusi dažus aizsardzības profilus nelielam skaitam produktu, kā elektroniskajam parakstam, ciparu tahogrāfiem un viedkartēm. Dalībnieki sadarbojas, lai koordinētu *CC* aizsardzības profilu standartizāciju, un koordinē aizsardzības profilu izstrādi. Dalībvalstis bieži prasa *SOG-IS* sertifikāciju savos publiskā iepirkuma konkursos.

produkciju tirgot Vācijā, Francijā un Apvienotajā Karalistē, šobrīd viņam ir jāizpilda trīs dažādu sertifikācijas shēmu prasības. Tās ir *Commercial Product Assurance* (*CPA*) Apvienotajā Karalistē, *Certification de Sécurité de Premier Niveau* (*CSPN*) Francijā un uz *CC* balstīts īpašs aizsardzības profils Vācijā.

Šādos apstākļos uzņēmumiem, kuri darbojas vairākās dalībvalstīs, paaugstinās izmaksas un tiek uzlikta ievērojama administratīva nasta. Lai gan sertifikācijas izmaksas var ievērojami atšķirties pēc produkta/pakalpojuma, prasītā izvērtējuma apliecinājuma līmeņa un/vai citiem komponentiem, uzņēmumiem tās mēdz būt ievērojamas. Tā, *BSI Smart Meter Gateway* sertifikāta izmaksas ir vairāk nekā miljons eiro (augstākajā testēšanas un apliecinājuma līmenī, attiecas ne tikai uz vienu produktu, bet arī uz visu apkārtējo infrastruktūru). Apvienotajā Karalistē viedskaitītāja sertifikācijas izmaksas ir turpat EUR 150 000. Francijā izmaksas ir līdzīgas, ap EUR 150 000 vai vairāk.

Galvenās ieinteresētās personas no publiskā un privātā sektora atzina, ka ES mēroga kiberdrošības sertifikācijas shēmas neesības dēļ uzņēmumiem daudzos gadījumos ir jāiztur sertifikācija atsevišķi katrā dalībvalstī un tādējādi veidojas tirgus sadrumstalotība. Svarīgākais ir tas, ka bez saskaņotiem ES tiesību aktiem par IKT produktiem un pakalpojumiem dalībvalstu atšķirīgie kiberdrošības sertifikācijas standarti un paņēmieni var novest pie tā, ka ES praksē izveidojas 28 atsevišķi drošības tirgi – katrs ar savām tehniskajām prasībām, testēšanas metodēm un kiberdrošības sertifikācijas procedūrām. Bez adekvātas rīcības ES līmenī atšķirīgās pieejas valsts līmenī var kļūt par ievērojamu traucēkli digitālā vienotā tirgus sasniegšanai un palēināt vai apturēt pozitīvo ietekmi uz izaugsmi un nodarbinātību.

Sakarā ar aprakstītajām norisēm regulas priekšlikums IKT produktiem un pakalpojumiem izveido Eiropas kiberdrošības sertifikācijas satvaru ("**satvars**") un nosaka *ENISA* būtiskās funkcijas un pienākumus kiberdrošības sertifikācijas sfērā. Priekšlikumā izklāstīts vispārējs normatīvais satvars, kas reglamentē Eiropas kiberdrošības sertifikācijas shēmas. Priekšlikums neievieš tieši izmantojamas sertifikācijas shēmas, bet drīzāk veido sistēmu (satvaru), kurā izstrādāt konkrētas sertifikācijas shēmas konkrētiem IKT produktiem/pakalpojumiem („Eiropas kiberdrošības sertifikācijas shēmas"). Eiropas kiberdrošības sertifikācijas shēmu izveide šajā satvarā ļautu saskaņā ar minētajām shēmām izdotus sertifikātus uzskatīt par derīgiem un atzītiem visās dalībvalstīs un novērst tirgus pašreizējo sadrumstalotību.

Eiropas kiberdrošības sertifikācijas shēmas vispārīgais mērķis ir apliecināt, ka saskaņā ar šo shēmu sertificēti IKT produkti un pakalpojumi atbilst noteiktām kiberdrošības prasībām. Tās, piemēram, varētu attiekties uz to spēju datus (vai tos glabā, sūta vai citādi apstrādā) pasargāt no nejaušas vai neatļautas glabāšanas, apstrādes, piekļuves, izpaušanas, iznīcināšanas, pazušanas vai pārveidošanas. ES kiberdrošības sertifikācijas shēmas izmantotu pastāvošos standartus, kas attiecas uz tehniskajām prasībām un izvērtēšanas procedūrām, kam produktiem jāatbilst, bet ar tām netiktu ieviesti jauni tehniskie standarti.[16] Piemēram, tādiem ražojumiem kā viedkartes, ko patlaban testē pēc starptautiskiem *CC* standartiem saskaņā ar daudzpusējo shēmu *SOG-IS* (aprakstīta pirmāk), ES mēroga sertifikācija šo shēmu padarītu derīgu visā ES.

Priekšlikumā noteikts ne tikai konkrētu drošības mērķu kopums, kas jāņem vērā, izstrādājot konkrētu Eiropas kiberdrošības sertifikācijas shēmu, bet arī šādu shēmu satura minimums. Shēmās būs cita starpā jāizstrādā vairāki specifiski elementi, kas nosaka kiberdrošības sertifikācijas tvērumu un priekšmetu. Tas nozīmē apzināt aptvertās produktu un pakalpojumu grupas, detalizēti noteikt kiberdrošības prasības (piemēram, atsaucoties uz attiecīgajiem

[16] Eiropas standartu gadījumos tas tiek darīts caur Eiropas standartizācijas organizācijām un pēc tam Eiropas Komisija to apstiprina publikācijā *Oficiālajā Vēstnesī* (sk. Regulu Nr. 1025/2012).

standartiem vai tehniskajām specifikācijām), specifiskos vērtēšanas kritērijus un metodes, kā arī apliecinājuma līmeni, ko iecerēts nodrošināt (t. i., pamata, būtisks vai augsts).

Eiropas kiberdrošības sertifikācijas shēmas *ENISA* sagatavos ar Eiropas Kiberdrošības sertifikācijas grupas palīgu un padomu un ciešā sadarbībā ar to (sk. tālāk), un Komisija tās pieņems ar īstenošanas aktiem. Ja tiks konstatēts, ka vajadzīga kiberdrošības sertifikācijas shēma, Komisija lūgs *ENISA* sagatavot shēmu konkrētiem IKT produktiem vai pakalpojumiem. To *ENISA* izstrādās ciešā sadarbībā ar valstu sertifikācijas pārraudzības iestādēm, kas būs pārstāvētas Kiberdrošības sertifikācijas grupā. Dalībvalstis un šī grupa var iesniegt priekšlikumu Komisijai pieprasīt no *ENISA* konkrētu shēmu.

Sertifikācija var būt ļoti dārgs process, un var paaugstināties cenas klientiem un patērētājiem. Sertifikācijas vajadzība var arī būtiski mainīties atkarā no produktu un pakalpojumu lietošanas konkrētā konteksta un tehnoloģisko pārmaiņu straujā tempa. Eiropas kiberdrošības sertifikācijas izmantošanai tāpēc būtu jāpaliek fakultatīvai, ciktāl IKT produktu un pakalpojumu drošības prasības nenosaka Savienības tiesību akti.

Lai nodrošinātu saskaņotību un nepieļautu lieku daudzveidību, IKT produktiem un pakalpojumiem, uz kuriem attiecas Eiropas kiberdrošības sertifikācijas sistēma, valstu kiberdrošības sertifikācijas shēmas vai procedūras vairs netiks piemērotas no datuma, kas būs noteikts īstenošanas tiesību aktā, ar kuru shēma tiks noteikta. Dalībvalstīm turpmāk nebūtu jāievieš jaunas valsts kiberdrošības sertifikācijas shēmas IKT produktiem un pakalpojumiem, uz kuriem attiecas pastāvoša Eiropas kiberdrošības sertifikācijas shēma.

Pēc Eiropas kiberdrošības sertifikācijas shēmu pieņemšanas IKT produktu izgatavotāji un IKT pakalpojumu sniedzēji varēs savu produktu vai pakalpojumu sertifikācijas pieteikumu iesniegt tai atbilstības novērtēšanas struktūrai, kuru izvēlēsies. Atbilstības novērtēšanas struktūras būtu jāakreditē akreditācijas struktūrai, ja tās atbilst noteiktām prasībām. Akreditāciju piešķirs, ilgākais, uz pieciem gadiem un varēs ar tādiem pašiem nosacījumiem atjaunot, ja atbilstības novērtēšanas struktūra atbildīs prasībām. Akreditācijas struktūras akreditāciju atsauks, ja atbilstības novērtēšanas struktūras akreditācijas nosacījumi nebūs vai vairs netiks izpildīti vai atbilstības novērtēšanas struktūras lēmumi pārkāps šo regulu.

Uzraudzības, pārraudzības un izpildes nodrošināšanas uzdevumi priekšlikumā paredzēti dalībvalstīm. Dalībvalstij būs jānodrošina viena sertifikācijas pārraudzības iestāde. Iestādes uzdevums būs pārraudzīt atbilstības novērtēšanas struktūru un to teritorijā izveidoto atbilstības novērtēšanas struktūru izdoto sertifikātu atbilstību šās regulas prasībām un attiecīgajām Eiropas kiberdrošības sertifikācijas shēmām. Valsts sertifikācijas pārraudzības iestādes būs kompetentas izskatīt sūdzības, ko fiziskas vai juridiskas personas iesniedz par sertifikātiem, kurus izdevušas to teritorijā izveidotas atbilstības novērtēšanas struktūras. Tās pienācīgā mērā izmeklēs sūdzības priekšmetu un bez liekas vilcināšanās informēs sūdzētāju par lietas virzību un izskatīšanas rezultātiem. Tās arī sadarbosies ar citām sertifikācijas pārraudzības iestādēm vai citām valsts iestādēm, piemēram, daloties informācijā par IKT produktu un pakalpojumu varbūtēju neatbilstību šās regulas prasībām vai konkrētajām Eiropas kiberdrošības sertifikācijas shēmām.

Visbeidzot, ar šo priekšlikumu tiek izveidota Eiropas Kiberdrošības sertifikācijas grupa, kas sastāv no visu dalībvalstu sertifikācijas pārraudzības iestādēm. Kiberdrošības sertifikācijas grupas galvenais uzdevums ir konsultēt Komisiju jautājumos, kas attiecas uz kiberdrošības sertifikācijas politiku, un kopā ar *ENISA* izstrādāt Eiropas kiberdrošības sertifikācijas shēmu projektus. *ENISA* palīdzēs Komisijai nodrošināt grupai sekretariātu un pastāvīgi atjaunināt Eiropas kiberdrošības sertifikācijas satvarā apstiprināto shēmu publisko uzskaiti. *ENISA* arī saistītos ar standartizācijas iestādēm, lai nodrošinātu apstiprinātajās shēmās izmantoto standartu piemērotību, un noteiktu jomas, kurās trūkst kiberdrošības standartu.

Eiropas kiberdrošības sertifikācijas satvars (“satvars”) dos daudzveidīgu labumu pilsoņiem un uzņēmumiem. Proti:

- Konkrētiem produktiem vai pakalpojumiem izveidotās ES mēroga kiberdrošības sertifikācijas shēmas nodrošinās uzņēmumiem ES kiberdrošības sertifikācijas "vienoto kontaktpunktu". Uzņēmumi varēs savu izstrādājumu sertificēt vienu reizi un saņemt sertifikātu, kas der visās dalībvalstīs. Nebūs pienākuma izstrādājumus pārsertificēt dažādu valstu sertifikācijas iestādēs. Tas ievērojami samazinās uzņēmumu izdevumus, atvieglinās pārrobežu darbību un galu galā mazinās un novērsīs attiecīgo izstrādājumu iekšējā tirgus sadrumstalotību.
- Satvars nosaka Eiropas kiberdrošības sertifikācijas shēmu pārākumu pār valstu shēmām: saskaņā ar šo normu, pieņemtai Eiropas kiberdrošības sertifikācijas shēmai būs virsroka pār visām pastāvošajām paralēlajām valstu shēmām, kas attiecas uz tiem pašiem IKT produktiem vai pakalpojumiem tādā pašā apliecinājuma līmenī. Tas radīs lielāku skaidrību, mazinot valstu kiberdrošības sertifikācijas shēmu patlaban izplatīto pārklāšanos un iespējamo pretrunīgumu.
- Priekšlikums atbalsta un papildina TID direktīvas īstenošanu, dodot uzņēmumiem, uz kuriem attiecas direktīva, ļoti noderīgu rīku, ar ko pierādīt atbilstību TID direktīvas prasībām visā Savienībā. Izstrādājot jaunas kiberdrošības sertifikācijas shēmas, Komisija un *ENISA* īpašu uzmanību pievērsīs vajadzībai nodrošināt, ka kiberdrošības sertifikācijas shēmās atspoguļojas TID direktīvas prasības.
- Priekšlikums veicinās un atvieglinās Eiropas kiberdrošības politikas izveidi, saskaņojot nosacījumus un būtiskās prasības, kas attiecas uz IKT produktu un pakalpojumu kiberdrošības sertifikāciju Eiropas Savienībā. Eiropas kiberdrošības sertifikācijas shēmas atsauksies uz kopīgiem vērtēšanas standartiem vai kritērijiem un testēšanas metodiku. Kaut netieši, tas ievērojami veicinās kopīgu drošības risinājumu ieviešanu ES, tādējādi arī novācot šķēršļus iekšējam tirgum.
- Satvars ir plānots tā, lai kiberdrošības sertifikācijas shēmām nodrošinātu nepieciešamo elastīgumu. Atkarā no konkrētām kiberdrošības vajadzībām produktu vai pakalpojumu var sertificēt atbilstoši augstākam vai zemākam drošības līmenim. Šis elastīgums tiks iestrādāts Eiropas kiberdrošības sertifikācijas shēmās, un būs paredzēti dažādi apliecinājuma līmeņi (t. i., pamata, būtisks un augsts), ko varēs izmantot dažādiem nolūkiem vai dažādos kontekstos.
- Visi minētie elementi kiberdrošības sertifikāciju padarīs pievilcīgāku uzņēmējiem, jo šis ir efektīvs veids, kā informēt par IKT produktu un pakalpojumu kiberdrošības apliecinājuma līmeni. Cik kiberdrošības sertifikācija kļūs lētāka, efektīvāka un komerciāli izdevīgāka, tik uzņēmumiem būs lielāks stimuls sertificēt savas produkcijas aizsardzību pret kiberriskiem, tā veicinot labākas kiberdrošības prakses izplatīšanos IKT produktu un pakalpojumu izstrādē (ieprojektētu kiberdrošību).

- **Saskanība ar spēkā esošajiem noteikumiem konkrētajā politikas jomā**

Tirgus subjektiem tautsaimnieciski un sabiedriski vitāli svarīgajās nozarēs, kā enerģētika, transports, ūdensapgāde, banku pakalpojumi, finanšu tirgus infrastruktūra, veselības aprūpe un digitālā infrastruktūra, kā arī digitālo pakalpojumu (piem., meklētājprogrammu, mākoņdatošanas pakalpojumu un tiešsaistes tirgotavu) sniedzējiem saskaņā ar TID direktīvu ir jāveic pienācīgi drošības risku pārvaldības pasākumi. Priekšlikuma jaunās tiesību normas

papildina TID direktīvas noteikumus un nodrošina saskanību ar tiem, lai konsekventāk veidotu ES kibernoturību, uzlabojot spējas, sadarbību, riska pārvaldību un kiberlietu izpratni.

Turklāt kiberdrošības sertifikācijas noteikumi dod būtisku rīku uzņēmumiem, uz kuriem attiecas TID direktīva, jo savu IKT produktu un pakalpojumu aizsargātību pret kiberdrošības riskiem tie varēs sertificēt, balstoties uz visā ES derīgām un atzītām kiberdrošības sertifikācijas shēmām. Tie arī būs papildinājums *eIDAS* regulā[17] un Radioiekārtu direktīvā[18] minētajām drošības prasībām.

- **Saskanība ar citām Savienības politikas jomām**

Regulā (ES) 2016/679 (Vispārīgā datu aizsardzības regula, "**VDAR**")[19] ir noteikumi par ieviešamiem sertifikācijas mehānismiem un datu aizsardzības zīmogiem un marķējumu, kam uzskatāmi jāparāda datu pārziņu un apstrādātāju veikto apstrādes darbību atbilstība minētajai regulai. Šis regulas priekšlikums neskar datu apstrādes darbību sertifikāciju, arī tad, kad tādas darbības saskaņā ar VDAR ir iestrādātas produktos un pakalpojumos.

Ierosinātā regula nodrošinās saderību ar Regulu (EK) Nr. 765/2008 par akreditācijas un tirgus uzraudzības prasībām[20], atsaucoties uz valsts akreditācijas struktūru un atbilstības novērtēšanas struktūru regulējuma normām. Attiecībā uz pārraudzības iestādēm, ierosinātajā regulā dalībvalstīm būs jānosaka savas sertifikācijas pārraudzības iestādes, kuru pienākums būs pārraudzīt, novērot un nodrošināt noteikumu izpildi. Minētās struktūras darbosies atsevišķi no atbilstības novērtēšanas struktūrām, kā noteikts Regulā (EK) Nr. 765/2008.

2. TIESISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

- **Tiesiskais pamats**

ES rīcības tiesiskais pamats ir Līguma par Eiropas Savienības darbību (LESD) 114. pants, kur runāts par dalībvalstu tiesību aktu tuvināšanu, lai sasniegtu LESD 26. pantā minētos mērķus, proti, iekšējā tirgus pienācīgu darbību.

Iekšējo tirgu kā tiesisko pamatu *ENISA* izveidei ir atbalstījusi Eiropas Savienības Tiesa (lietā C-217/04, Apvienotā Karaliste pret Eiropas Parlamentu un Padomi) un nostiprinājusi 2013. gada regula, kas nosaka Aģentūras pašreizējās pilnvaras. Turklāt darbības, kurās atspoguļotos mērķis paplašināt sadarbību un koordināciju starp dalībvalstīm un vairot ES līmeņa spējas papildināt dalībvalstu rīcību, ietilptu kategorijā "operatīvā sadarbība". Tas ir īpaši noteikts TID direktīvā (kuras tiesiskais pamats ir LESD 114. pants) kā mērķis, kas jāīsteno saistībā ar *CSIRT* tīklu, kur "*ENISA* nodrošina sekretariātu un aktīvi atbalsta sadarbību starp *CSIRT*" (12. panta 2. punkts). Konkrēti, 12. panta 3. punkta f) apakšpunktā kā *CSIRT* tīkla uzdevums ir sīkāk izklāstīta jaunu operatīvās sadarbības veidu apzināšana, arī tādu, kas attiecas uz: i) risku

---

17 Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK.

18 Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Direktīva 2014/53/ES par dalībvalstu tiesību aktu saskaņošanu attiecībā uz radioiekārtu pieejamību tirgū un ar ko atceļ Direktīvu 1999/5/EK.

19 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1.–88. lpp.).

20 Regula (EK) Nr. 765/2008, ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93.

un incidentu kategorijām, ii) laicīgu brīdināšanu, iii) savstarpēju palīdzību, iv) koordinēšanas principiem un kārtību dalībvalstu reaģēšanai uz pārrobežu riskiem un incidentiem.

- IKT produktu un pakalpojumu sertifikācijas shēmu nevienveidība pastāv arī tādēļ, ka trūkst dalībvalstīm piemērojama vienota juridiski saistoša un iedarbīga regulēšanas procesa. Tas kavē IKT produktu un pakalpojumu iekšējā tirgus izveidi un bremzē Eiropas rūpniecības konkurētspēju šajā nozarē. Šā priekšlikuma mērķis ir novērst pašreizējo nevienveidību un ar to saistītos šķēršļus iekšējā tirgū, nodrošinot vienotu satvaru visā ES derīgu kiberdrošības sertifikācijas shēmu izstrādei.

Subsidiaritāte (neekskluzīvas kompetences gadījumā)

Subsidiaritātes princips prasa novērtēt ES rīcības nepieciešamību un pievienoto vērtību. Subsidiaritātes ievērošana šajā jomā jau tika atzīta, pieņemot spēkā esošo *ENISA* regulu[21].

Kiberdrošības jautājums ir visas Savienības kopīgās interesēs. Tīklu un informācijas sistēmu savstarpējā atkarība ir tāda, ka atsevišķi subjekti (publiskā un privātā sektora, ieskaitot indivīdus) bieži nespēj pa vienam pretoties apdraudējumam un tikt galā ar kiberriskiem un incidentu iespējamo ietekmi. No vienas puses, dalībvalstu savstarpējā atkarība, arī kritisko infrastruktūru ekspluatācijā (enerģētika, transports, ūdensapgāde, un tās ir tikai dažas), padara publiskās varas iesaistīšanos Eiropas līmenī ne tikai vēlamu, bet arī vajadzīgu. No otras puses, ES dalība var radīt plašāku pozitīvu efektu ar labas prakses apmaiņu starp dalībvalstīm, un tas var uzlabot Savienības kiberdrošību.

Kopumā, ņemot vērā pašreizējos apstākļos un nākotnes scenārijus, šķiet, ka nolūkā **uzlabot Savienības kolektīvo kibernoturību** nepietiks ar **ES dalībvalstu atsevišķām darbībām un saskaldītu pieeju kiberdrošībai**.

ES rīcība uzskatāma par nepieciešamu arī tālab, lai novērstu kiberdrošības sertifikācijas shēmu pašreizējo nevienveidību. Tas ļautu ražotājiem gūt maksimālu labumu no iekšējā tirgus, ievērojami ietaupīt testēšanas un pārprojektēšanas izmaksas. Kaut arī pašreizējā Informācijas sistēmu drošības augstāko amatpersonu grupas (*SOG-IS*) Savstarpējās atzīšanas nolīguma (*SAN*) jautājumos, piemēram, ir panākusi svarīgus rezultātus šajā ziņā, tā arī uzrāda būtiskus ierobežojumus, kas traucē tai piemērotā veidā ilgtermiņā nodrošināt ilgtspējīgus risinājumus iekšējā tirgus potenciāla pilnīgai izmantošanai.

ES līmeņa rīcības pievienotā vērtība, it īpaši, sekmējot sadarbību starp dalībvalstīm, kā arī starp tīklu un informācijas drošības kopienām, ir atzīta 2016. gada Padomes secinājumos[22], un tā arī skaidri parādās *ENISA* izvērtējumā.

- **Proporcionalitāte**

Priekšlikumā paredzēts vienīgi tas, kas nepieciešams tā politisko mērķu sasniegšanai. Turklāt ES iesaistīšanās apmērs nav par šķērsli valstu darbībām valsts drošības jautājumos. Tāpēc ES rīcība ir pamatota ar subsidiaritātes principu un proporcionalitātes principu.

---

21 Eiropas Parlamenta un Padomes 2013. gada 21. maija Regula (ES) Nr. 526/2013 par Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*) un ar ko atceļ Regulu (EK) Nr. 460/2004.

22 Padomes secinājumi par paziņojumu "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari" (2016. gada 15. novembris).

- **Juridiskā instrumenta izvēle**

Ar šo priekšlikumu tiek pārskatīta Regula (ES) Nr. 526/2013, kurā noteiktas *ENISA* pašreizējās pilnvaras un uzdevumi. Turklāt, ņemot vērā *ENISA* nozīmi ES kiberdrošības sertifikācijas satvara izveidē un pārvaldībā, jaunās *ENISA* pilnvaras un minētais satvars vislabāk ir izveidojami ar vienu vienīgu juridisku instrumentu, izmantojot regulu.

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

***Ex post* izvērtējumi / spēkā esošo tiesību aktu atbilstības pārbaude**

Komisija pēc vērtēšanas shēmas[23] skatīja Aģentūras **nozīmīgumu, ietekmi, rezultativitāti, efektivitāti, saskanību un ES pievienoto vērtību** tādos aspektos kā veiktspēja, pārvaldība, iekšējā uzbūve un darba metodes laikposmā no 2013. līdz 2016. gadam. Galvenos konstatējumus var apkopot šādi (sīkāk sk. ietekmes novērtējumam pievienoto dienestu darba dokumentu par šo jautājumu).

- **Nozīmīgums.** Tehnoloģiju attīstības un jaunu apdraudējumu apstākļos, ņemot vērā ievērojamo vajadzību ES uzlabot kiberdrošību, *ENISA* mērķi ir izrādījušies nozīmīgi. Dalībvalstis un ES iestādes nudien paļaujas uz tās lietpratību kiberdrošības jautājumos. Bez tam dalībvalstīs ir jāattīsta spēja labāk izprast apdraudējumu un reaģēt uz to, un ieinteresētajām personām ir jāsadarbojas dažādās tematiskajās jomās un iestāžu starpā. Kiberdrošība joprojām ir svarīga ES politiskā prioritāte, kurā tiek gaidīta *ENISA* rīcība, taču *ENISA* izveidota kā ES aģentūra ar noteikta termiņa pilnvarām, tāpēc: i) nav iespējama ilgtermiņa plānošana un pastāvīgs atbalsts dalībvalstīm un ES iestādēm; ii) var rasties tiesisks vakuums, jo TID direktīvas noteikumi *ENISA* uztic uzdevumus, kas ir pastāvīgi[24]; iii) trūkst saskanības ar ieceri *ENISA* iesaistīt plašākā ES kiberdrošības ekosistēmā.
- **Rezultativitāte**. Kopumā *ENISA* ir sasniegusi mērķus un izpildījusi uzdevumus. Ar savām pamatdarbībām (spēju veidošana, lietpratēju padoms, kopienas izveide un politikas atbalste) tā devusi ieguldījumu tīklu un informācijas drošībā Eiropā. Katrā pamatdarbībā gan parādījies, kas vēl uzlabojams. Izvērtējumā secināts, ka *ENISA* ir faktiski radījusi spēcīgas un uzticības pilnas attiecības ar dažām ieinteresētajām personām, sevišķi dalībvalstīm un *CSIRT* kopienu. Dalība spēju veidošanas jomā tika uzskatīta par rezultatīvu, it īpaši dalībvalstīs, kurām mazāki resursi. Viena no spilgtākajām ir bijusi plašas sadarbības veicināšana – ieinteresētās personas visnotaļ piekrīt, ka *ENISA* ir pozitīva loma cilvēku tuvināšanā. Taču *ENISA* grūti nācies jūtami ietekmēt visu plašo tīklu un informācijas drošības jomu. Arī tāpēc, ka plašo pilnvaru izlietošanai tai bija doti visai ierobežoti cilvēkresursi un finansiālie līdzekļi. Novērtējumā arī secināts, ka mērķi nodrošināt lietpratēju atzinumus *ENISA* sasniegusi pa daļai, jo bijušas problēmas ekspertu līgšanā (sk. arī tālāk par efektivitāti).
- **Efektivitāte**. Par spīti tam, ka budžets mazs, viens no mazākajiem citu ES aģentūru vidū, Aģentūra ir spējusi dot ieguldījumu precīzi izraudzītu mērķu sasniegšanā, parādīdama, ka resursus izmanto lietderīgi. Izvērtējumā secināts, ka darbības visumā bijušas lietderīgas un skaidri nodalītie pienākumi organizācijā ļāvuši darbus paveikt

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf.

[24] Atsauce uz Tīklu un informācijas sistēmu drošības direktīvas (TID direktīvas) 7., 9., 11., 12. un 19. pantu.

labi. Viena no galvenajām Aģentūras efektivitātes problēmām ir *ENISA* grūtības pieņemt un noturēt darbā augsti kvalificētus ekspertus. Konstatēts, ka tas izskaidrojams ar vairāku faktoru kombināciju, ieskaitot visa publiskā sektora vispārējās grūtības konkurēt ar privāto sektoru mēģinājumos nolīgt augsti kvalificētus ekspertus, līgumu veidu (uz noteiktu laiku), ko Aģentūra galvenokārt varēja piedāvāt, un *ENISA* atrašanās vietas pavājo pievilcību, piemēram, sakarā ar laulāto grūtībām atrast darbu. Izvietojums gan Atēnās, gan Hēraklejā apgrūtināja koordināciju un radīja liekas izmaksas, bet pamatdarbības struktūrvienības pārcelšanās uz Atēnām 2013. gadā uzlaboja Aģentūras darbības efektivitāti.

- **Saskanīgums**. *ENISA* darbības visumā saskanējušas ar ieinteresēto personu politiku un darbībām valstu un ES līmenī, taču ir vajadzīga labāk koordinēta pieeja kiberdrošībai ES līmenī. Nav pilnībā izmantots *ENISA* un citu ES struktūru sadarbības potenciāls. Pārmaiņas ES tiesiskajā un politiskajā vidē mazina pašreizējo pilnvaru saskanīgumu.

- **ES pievienotā vērtība**. *ENISA* pievienotā vērtība galvenokārt izpaužas kā Aģentūras spēja uzlabot sadarbību, galvenokārt starp dalībvalstīm, bet arī ar saistītajām tīklu un informācijas drošības kopienām. ES līmenī nav citu struktūru, kas atbalstītu tik plašu sadarbību starp tīklu un informācijas drošības jautājumos ieinteresētajām personām. Aģentūras pievienotā vērtība variējās atkarā no ieinteresēto personu vajadzībām un līdzekļiem (piemēram, lielās dalībvalstis pretstatā mazajām, dalībvalstis pretstatā nozarei) un Aģentūras nepieciešamības noteikt prioritātes saviem pasākumiem saskaņā ar darba programmu. Izvērtējumā secināts, ka *ENISA* darbības iespējamā neturpināšana būtu visu dalībvalstu neizmantotā iespēja. Tādā gadījumā nebūs iespējams nodrošināt tāda paša līmeņa kopienas veidošanu un sadarbību starp dalībvalstīm kiberdrošības jomā. Bez vairāk centralizētas ES aģentūras aina kļūtu aizvien neviengabalaināka, *ENISA* vietā nākot divpusējai vai reģionālai sadarbībai.

Aplūkojot *ENISA* līdzšinējo veikumu un nākotni, 2017. gada apspriešanā iezīmējas šādas galvenās tendences[25]:

- Lielākā daļa respondentu (74 %) *ENISA* sniegumu laikposmā no 2013. līdz 2016. gadam visumā novērtēja pozitīvi. Lielākā daļa respondentu arī uzskata, ka *ENISA* sasniedz visus mērķus (vismaz 63 % par katru no mērķiem). *ENISA* pakalpojumus un produktus regulāri (reizi mēnesī vai biežāk) izmanto gandrīz puse respondentu (46 %), un tos atzinīgi vērtē tāpēc, ka tie nāk no ES līmeņa iestādes (83 %), un kvalitātes dēļ (62 %).

- Respondenti atzīmēja vairākas nepilnības un ES kiberdrošības nākotnes problēmas, it īpaši piecās jomās (no 16 uzskaitītām): dalībvalstu sadarbība, spēja novērst, atklāt un pārvarēt plašapmēra kiberuzbrukumus, dalībvalstu sadarbība jautājumos, kas saistīti ar kiberdrošību, sadarbība un informācijas apmaiņa starp dažādām ieinteresētajām personām, ieskaitot publiskā un privātā sektora sadarbību, kritiskās infrastruktūras aizsargāšana no kiberuzbrukumiem.

[25] Apspriešanā atbildes sniedza 90 ieinteresētās personas no 19 dalībvalstīm (88 atbildes un 2 nostājas dokumenti), to vidū valsts iestādes no 15 dalībvalstīm, ieskaitot Franciju, Itāliju, Īriju un Grieķiju, un 8 jumta organizācijas, kas pārstāv ievērojamu skaitu Eiropas organizāciju, kā Eiropas Banku federācija, *Digital Europe* (pārstāv ciparu tehnoloģiju rūpniecību Eiropā), Eiropas Telesakaru tīklu operatoru asociācija (*ETNO*). *ENISA* sabiedrisko apspriešanu papildināja vairāki citi avoti, to starpā: i) saturīgas pārrunas ar aptuveni 50 galvenajiem kiberdrošības kopienas locekļiem, ii) *CSIRT* tīkla aptauja, iii) *ENISA* Administratīvās padomes, Valdes un Pastāvīgās ieinteresēto personu grupas aptauja.

- Lielais vairums aptaujāto (88 %) uzskata, ka pašreizējie ES līmenī pieejamie instrumenti un mehānismi nav pietiekami vai ir tikai daļēji pietiekami problēmu atrisināšanai. Lielākā daļa respondentu (98 %) norāda, ka jābūt ES iestādei, kas atsauktos uz šīm vajadzībām, un to vidū aģentūru *ENISA* 99 % respondentu uzskata par piemērotāko organizāciju.

Apspriešanās ar ieinteresētajām personām

- No 2016. gada 12. aprīļa līdz 5. jūlijam Komisija rīkoja sabiedrisko apspriešanu par *ENISA* pārskatīšanu un saņēma 421 atbildi[26]. No tās redzams, ka 67,5 % respondentu pauž viedokli, ka aģentūrai *ENISA* varētu būt zināma loma saskaņota IT produktu un pakalpojumu drošības sertifikācijas satvara izveidē.

2016. gada apspriešanā par kiberdrošības *cPPP*[27] iedaļā par sertifikāciju redzami šādi rezultāti:

- 50,4 % (t. i., 121 no 240) respondentu nezina, vai valstu sertifikācijas shēmas tiek savstarpēji atzītas visās ES dalībvalstīs. 25,8 % (62 no 240) atbildēja „nē", bet 23,8 % (57 no 240) atbildēja "jā".
- 37,9 % respondentu (91 no 240) domā, ka pastāvošās sertifikācijas shēmas neatbalsta Eiropas rūpniecības vajadzības. No otras puses, 17,5 % (42 no 240) – galvenokārt pasaules mēroga uzņēmumi, kas darbojas Eiropas tirgū – pauž pretēju viedokli.
- 49,6 % (119 no 240) respondentu apgalvo, ka nav viegli pierādīt standartu, sertifikācijas shēmu un marķējumu līdzvērtību. 37,9 % (91 no 240) atbildēja „nezinu", bet 12,5 % (30 no 240) atbildēja "jā".

Ekspertu atzinumu pieprasīšana un izmantošana

Komisija izmantoja šādus ārējo ekspertu atzinumus:

- pētījumu par *ENISA* izvērtējumu – *Study on the Evaluation of ENISA (Ramboll/Carsa 2017; SMART no. 2016/0077)*,
- pētījumu par IKT drošības sertifikāciju un marķēšanu – *Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment (PriceWaterhouseCoopers 2017; SMART no. 2016/0029).*

Ietekmes novērtējums

- Ietekmes novērtējuma ziņojumā par šo iniciatīvu tika konstatētas šādas galvenās risināmās problēmas:
- kiberdrošības politikas un pieeju nevienādība dalībvalstīs,

[26] 162 atbildes no privātpersonām, 33 – no pilsoniskās sabiedrības un patērētāju organizācijām; 186 – no nozares pārstāvjiem, 40 – no publiskajām iestādēm, ieskaitot kompetentās iestādes, kas ievieš E-privātuma direktīvu.

[27] 240 ieinteresētās personas no valsts pārvaldes iestādēm, lieliem uzņēmumiem, MVU, mikrouzņēmumiem un pētniecības iestādēm atbildēja uz sadaļu par sertifikāciju.

- kiberdrošības resursu izkliedētība un pieeju nevienādība ES iestādēs, aģentūrās un struktūrās un
- nepietiekama pilsoņu un uzņēmumu izpratne un apziņošana, ko pasliktina valstu un nozaru sertifikācijas shēmu daudzveidības saviešanās.

Jautājumā par *ENISA* pilnvarām ziņojumā tika izvērtēti šādi iespējamie risinājumi:

- pastāvošā stāvokļa saglabāšana, t. i., pilnvaru pagarināšana uz ierobežotu laiku (nulles risinājums),
- *ENISA* pašreizējo pilnvaru notecēšana bez pagarināšanas – *ENISA* izbeigšanās (nekādas politiskas rīcības),
- "reformēta *ENISA*" un
- ES kiberdrošības aģentūra ar pilnīgām operatīvām spējām.

Jautājumā par kiberdrošības sertifikāciju ziņojumā tika izvērtēti šādi iespējamie risinājumi:

- nekādas politiskas rīcības (nulles risinājums),
- neleģislatīvi (ieteikuma tiesību) pasākumi,
- ES tiesību akts, kas izveidotu visām dalībvalstīm obligātu sistēmu uz sistēmas *SOG-IS* pamata, un
- vispārējs ES IKT kiberdrošības drošības sertifikācijas satvars.

Analīzē tika secināts, ka vēlamākais risinājums ir "reformēta *ENISA*" apvienojumā ar vispārēju ES IKT kiberdrošības sertifikācijas satvaru.

Vēlamākais risinājums ir novērtēts kā produktīvākais šādu ES noteikto mērķu sasniegšanai: uzlabot kiberdrošības spējas, gatavību, sadarbību, izpratni, pārredzamību un novērst tirgus sadrumstalotību. Tas arī novērtēts kā visvairāk saskanīgs ar ES kiberdrošības stratēģijas un tai radniecīgo politikas virzienu (piemēram, TID direktīvas) politiskajām prioritātēm un digitālā vienotā tirgus stratēģiju. Apspriešanas procesā izrādījās, ka vēlamāko risinājumu atbalsta arī lielākā daļa ieinteresēto personu. Jāpiebilst, ka ietekmes novērtējumā veiktā analīze rāda, ka vēlamākais risinājums mērķus sasniegtu, ja resursus izmantotu prātīgi.

Komisijas Regulējuma kontroles padome 2017. gada 24. jūlijā vispirms sniedza negatīvu atzinumu, bet pēc atkārtota pieteikuma iesniegšanas 25. augustā sniedza pozitīvu atzinumu. Grozītajā ietekmes novērtējuma ziņojumā bija iekļautas papildu liecības, *ENISA* izvērtējuma galīgie secinājumi un papildu paskaidrojumi par politiskajiem risinājumiem un to ietekmi. Ietekmes novērtējuma galīgā ziņojuma 1. pielikumā ir kopsavilkums par to, kā otrajā atzinumā risinātas Regulējuma kontroles padomes piezīmēs norādītās problēmas. Proti, ziņojums tika atjaunināts, sīkāk atspoguļojot stāvokli ES kiberdrošībā, ieskaitot pasākumus, kas iekļauti kopīgajā paziņojumā "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību", (JOIN(2017) 450), un ir īpaši svarīgi *ENISA*: ES kiberdrošības plāns un Eiropas Kiberdrošības pētniecības un kompetences centrs, kuram Aģentūra piesaistītu savus padomdevējus ES pētniecības vajadzību jautājumos.

Ziņojumā paskaidrots, kā Aģentūras reforma, ieskaitot tās jaunos uzdevumus, labākus nodarbinātības apstākļus un strukturālo sadarbību ar šās jomas ES struktūrām, varētu uzlabot tās pievilcību darba devējas lomā un palīdzētu pārvarēt ekspertu nolīgšanas grūtības. Ziņojuma 6. pielikumā dota pārskatīta aplēse par izdevumiem sakarā ar politiskajiem risinājumiem, kas skar *ENISA*. Jautājumā par sertifikāciju ziņojums ir pārskatīts un tajā sīkāk, arī ar ilustrācijām, paskaidrots vēlamākais risinājums, kā arī dotas aplēses par dalībvalstu un

Komisijas izmaksām sakarā ar jauno sertifikācijas satvaru. Sīkāk paskaidroti apsvērumi, uz kuru pamata *ENISA* šajā jomā izraudzīta par galveno personu tās lietpratības dēļ un tādēļ, ka ir vienīgā ES līmeņa aģentūra, kas nodarbojas ar kiberdrošību. Visbeidzot, tika pārskatīti sertifikācijai veltītie punkti, precizējot aspektus, kas saistīti ar pašreizējās sistēmas *SOG-IS* atšķirībām un ieguvumiem no dažādiem politikas risinājumiem, un paskaidrojot, ka IKT produkta un pakalpojuma veids, uz ko attiecas Eiropas sertifikācijas shēma, tiks noteikts pašā apstiprinātajā shēmā.

Normatīvā atbilstība un vienkāršošana

Neattiecas.

Ietekme uz pamattiesībām

Kiberdrošībai ir būtiska nozīme indivīda privātuma un personas datu aizsardzībā saskaņā ar ES Pamattiesību hartas 7. un 8. pantu. Kiberincidenta gadījumā privātums un personas datu aizsardzība, bez šaubām, ir apdraudēti. Tāpēc kiberdrošība ir nepieciešams priekšnoteikums privātuma ievērošanai un personas datu konfidencialitātei. Šādā rakursā šis priekšlikums, kas tiecas Eiropā uzlabot kiberdrošību, ir svarīgs papildinājums spēkā esošajiem tiesību aktiem, kuri sargā pamattiesības uz privātumu un personas datus. Kiberdrošība ir būtiska arī elektronisko sakaru konfidencialitātes aizsardzībā un tādējādi vārda un informācijas brīvības un ar to saistītās domu, apziņas un reliģijas brīvības izlietošanai.

4. IETEKME UZ BUDŽETU

Sk. finanšu pārskatu.

5. CITI ELEMENTI

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

Komisija uzraudzīs regulas piemērošanu un ik pēc pieciem gadiem iesniegs ziņojumu par tās izvērtēšanu Eiropas Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai. Šie ziņojumi būs publiski pieejami, un tajos būs detalizēti aplūkota regulas faktiskā piemērošana un izpilde.

- **Konkrētu priekšlikuma noteikumu sīkāks skaidrojums**

Regulas I sadaļā ir vispārīgie noteikumi: priekšmets (1. pants), jēdzienu definīcijas (2. pants), ieskaitot atsauces uz attiecīgām definīcijām citos ES aktos, piemēram, Eiropas Parlamenta un Padomes Direktīvā (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (TID direktīva), Eiropas Parlamenta un Padomes Regulā (EK) Nr. 765/2008, ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93, un Eiropas Parlamenta un Padomes Regulā (ES) Nr. 1025/2012 par Eiropas standartizāciju.

Regulas II sadaļa ietver galvenos noteikumus, kas attiecas uz *ENISA* kā "ES kiberdrošības aģentūru".

Sadaļas I nodaļā izklāstītas Aģentūras pilnvaras (3. pantā), mērķi (4. pantā) un uzdevumi (5.–11. pantā).

II nodaļā izklāstīta *ENISA* organizācija un ietverti galvenie noteikumi par tās uzbūvi (12. pantā). Aprakstīts *ENISA* Administratīvās padomes (1. iedaļas 13.–17. pants) un Valdes (2. iedaļas 18. pants) sastāvs, balsošanas kārtība un funkcijas, kā arī izpilddirektora pienākumi (3. iedaļas 19. pants). Ietverti arī noteikumi par Pastāvīgās ieinteresēto personu grupas sastāvu un lomu (4. iedaļas 20. pants). Pēdējais svarīgākais – nodaļas 5. iedaļā sīki izklāstīti Aģentūras darbības noteikumi, arī sakarā ar darba plānošanu, interešu konfliktu, pārredzamību, konfidencialitāti un piekļuvi dokumentiem (21.–25. pants).

III nodaļa attiecas uz Aģentūras budžeta izveidi un struktūru (26. un 27. punkts), kā arī īstenošanas noteikumiem (28. un 29. punkts). Tajā ir arī noteikumi, kas veicina cīņu pret krāpšanu, korupciju un citām nelikumīgām darbībām (30. pants).

IV nodaļa attiecas uz Aģentūras personāla izveidi. Tajā iekļauti vispārīgi civildienesta un Savienības pārējo darbinieku nodarbināšanas kārtības noteikumi un noteikumi par privilēģijām un imunitāti (31. un 32. pants). Tajā arī detaļās izklāstīti noteikumi par Aģentūras izpilddirektora pienākumiem un iecelšanu (33. pants). Ietverti arī noteikumi par to, kā izmantot valstu norīkotus ekspertus vai citus darbiniekus, ko nenodarbina Aģentūra (34. pants).

Visbeidzot, V nodaļā ietverti vispārīgi noteikumi, kas attiecas uz Aģentūru. Tajā noteikts juridiskais statuss (35. pants) un ietverti noteikumi, kas reglamentē tādus jautājumus kā atbildība, valodu lietošana, personas datu aizsardzība (36.–38. pants), kā arī drošības noteikumi par klasificētas informācijas un sensitīvas neklasificētas informācijas aizsardzību (40. pants). Aprakstīti noteikumi, pēc kuriem Aģentūra vadās sadarbībā ar trešām valstīm un starptautiskajām organizācijām (39. pants). Visbeidzot, tajā ietverti arī noteikumi par Aģentūras mītni un darbības apstākļiem, kā arī administratīvo kontroli, ko veic Ombuds (41. un 42. pants).

Regulas III sadaļā ar vispārīgu normu izveidots IKT produktu un pakalpojumu Eiropas kiberdrošības sertifikācijas satvars ("**satvars**") (1. pants). Tajā formulēts Eiropas kiberdrošības sertifikācijas shēmu vispārīgais mērķis, t. i., nodrošināt IKT produktu un pakalpojumu atbilstību noteiktajām kiberdrošības prasībām pēc spējas noteiktā apliecinājuma līmenī pretoties darbībai, kas apdraud glabāto, pārsūtīto vai apstrādāto datu vai funkciju vai pakalpojumu pieejamību, autentiskumu, veselumu vai konfidencialitāti (43. pants). Tajā arī uzskaitīti drošības mērķi, ko cenšas sasniegt Eiropas kiberdrošības sertifikācijas shēmas (45. pants), to vidū – panākt spēju aizsargāt datus no nejaušas vai neatļautas piekļuves vai izpaušanas, iznīcināšanas vai pārveidošanas, un Eiropas kiberdrošības sertifikācijas shēmu saturs (jeb elementi), piemēram, detalizētas norādes par tvērumu, drošības mērķi, izvērtēšanas kritēriji u. c. (47. pants).

III sadaļā ir noteiktas arī Eiropas kiberdrošības sertifikācijas shēmu ieviešanas galvenās tiesiskās sekas, proti, i) pienākums shēmu īstenot valsts līmenī un sertificēšanas fakultatīvums, ii) Eiropas kiberdrošības sertifikācijas shēmu pārākums pār tādu pašu produktu vai pakalpojumu valsts shēmām (48. un 49. pants).

Šajā sadaļā izklāstīta arī Eiropas kiberdrošības sertifikācijas shēmu pieņemšanas kārtība un Komisijas, *ENISA* un Eiropas Kiberdrošības sertifikācijas grupas attiecīgā loma (44. pants). Visbeidzot, šajā sadaļā ir noteikumi, kas reglamentē atbilstības novērtēšanas struktūras, ieskaitot to prasības, pilnvaras un uzdevumus, valsts sertifikācijas pārraudzības iestādes, kā arī sankcijas.

Šajā sadaļā arī tiek nodibināta Kiberdrošības sertifikācijas grupa – būtiska struktūra, kas sastāv no valstu sertifikācijas pārraudzības iestāžu pārstāvjiem, kuru galvenais uzdevums ir kopdarbā ar *ENISA* sagatavot Eiropas kiberdrošības sertifikācijas shēmas un konsultēt

Komisiju vispārīgos vai specifiskos jautājumos, kas attiecas uz kiberdrošības sertifikācijas politiku.

Regulas IV sadaļā ietverti nobeiguma noteikumi par deleģējuma īstenošanu, izvērtēšanas prasībām, atcelšanu un pēctecību, kā arī stāšanos spēkā.

2017/0225 (COD)

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")

(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[28],

ņemot vērā Reģionu komitejas atzinumu[29],

saskaņā ar parasto likumdošanas procedūru,

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

[28] OV C [...], [...], [...]. lpp.
[29] OV C [...], [...], [...]. lpp.

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[30], 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[31], pagarinot Aģentūras pilnvaru termiņu līdz 2012. gada martam. Savukārt ar Regulu (EK) Nr. 580/2011[32] Aģentūras pilnvaru termiņu pagarināja līdz 2013. gada 13. septembrim. 2013. gadā Eiropas Parlaments un Padome pieņēma Regulu (ES)

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

31 Eiropas Parlamenta un Padomes 2008. gada 24. septembra Regula (EK) Nr. 1007/2008, 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.).

32 Eiropas Parlamenta un Padomes 2011. gada 8. jūnija Regula (ES) Nr. 580/2011, 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.).

Nr. 526/2013[33] par *ENISA* un ar ko atceļ Regulu (EK) Nr. 460/2004; ar to Aģentūras pilnvaru termiņš tika pagarināts līdz 2020. gada jūnijam.

(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 ES 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,

[33] Eiropas Parlamenta un Padomes 2013. gada 21. maija Regula (ES) Nr. 526/2013 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.).

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. Iespējami ciešākā sadarbībā ar Savienības iestādēm, struktūrām, birojiem un aģentūrām un dalībvalstīm pildot savus uzdevumus, Aģentūrai būtu aktīvi jāveicina dalībvalstu un Savienības centieni. 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, arī kritiskās infrastruktūras aizsardzības un kibernoturības, jomā. 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, struktūru, biroju un aģentūru centieni veidot un uzlabot spējas un gatavību novērst un atklāt kiberdrošības problēmas 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. Aģentūrai arī būtu jāpalīdz izstrādāt un atjaunināt Savienības un 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 "jāmāca 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, jo īpaši, lai atbalstītu kritiskās infrastruktūras aizsardzību, Aģentūrai

būtu jāveicina nozaru informācijas apmaiņas un analīzes centru (*ISAC*) izveide, nodrošinot paraugpraksi un sniedzot norādījumus par pieejamiem rīkiem un procedūrām, kā arī par to regulatīvo jautājumu risināšanu, kuri saistīti ar informācijas apmaiņu.

(18) Aģentūrai, attiecībā uz informācijas apmaiņu ieviešot kopīgus noteikumus, vienotu valodas lietojumu un terminoloģiju, būtu jāapkopo un jāanalizē valstu *CSIRT* un *CERT-EU* ziņojumi. Aģentūrai būtu arī jāiesaista privātais sektors saistībā ar TID direktīvu, kurā izklāstīti iemesli brīvprātīgai tehniskās informācijas apmaiņai operatīvā līmenī un *CSIRT* tīkla izveidei.

(19) Aģentūrai būtu jāpalīdz nodrošināt Savienības līmeņa reaģēšanu uz plašapmēra pārrobežu 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 viss process, šādas sadarbības mehānismu pārbaudot ikgadējās kiberdrošības mācībās.

(20) Savu darbības uzdevumu izpildē Aģentūrai būtu jāizmanto pieejamā *CERT-EU* lietpratība, izmantojot ciešā fiziskā tuvumā veidotu strukturētu sadarbību ar *CERT-EU*. Strukturētā sadarbība palīdzēs panākt vajadzīgo sinerģiju un attīstīt *ENISA* lietpratību. Attiecīgā gadījumā starp abām organizācijām būtu jāpanāk īpaša vienošanās par šādas sadarbības praktiskas īstenošanas kārtību.

(21) Atbilstīgi darbības uzdevumiem Aģentūrai būtu jāspēj sniegt atbalstu dalībvalstīm, piemēram, sniedzot padomus vai tehnisku palīdzību vai veicot apdraudējumu un incidentu analīzi. 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* izpildīt savus darbības uzdevumus.

(22) Lai regulāras tehniskās sadarbības ietvaros veicinātu situācijas apzināšanos Savienībā, Aģentūrai regulāri būtu jāsagatavo ES kiberdrošības tehniskās situācijas ziņojums par incidentiem un apdraudējumiem, kurš balstīts uz publiski pieejamu informāciju, *ENISA* veikto analīzi un ziņojumiem, ko tai (brīvprātīgi) snieguši dalībvalstu *CSIRT* vai ar TID direktīvu izveidotie vienotie kontaktpunkti, 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) Vairāk nekā vienu dalībvalsti ietekmējušu incidentu *ex-post* tehniskajā izmeklēšanā, ko Aģentūra atbalsta vai veic pēc attiecīgo dalībvalstu pieprasījuma vai pēc vienošanās ar tām, būtu jāorientējas uz turpmāku incidentu novēršanu, un tā būtu jāveic, neskarot nekādas tiesas vai administratīvas procedūras vainas vai atbildības noteikšanai.

(24) Attiecīgajām dalībvalstīm būtu jāsniedz Aģentūrai vajadzīgā informācija un palīdzība, lai izmeklēšanu tā varētu veikt, neskarot Līguma par Eiropas Savienības darbību 346. pantu vai citas sabiedriskās kārtības prasības.

(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 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 ar kiberdrošību saistītās problēmas.

(27) Lai palielinātu Savienības noturību, Aģentūrai, sniedzot padomus, norādījumus un paraugpraksi, būtu jāattīsta izcilība interneta infrastruktūras un kritiskās infrastruktūras drošības jautājumos. 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, struktūrām, birojiem un aģentūrām 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*) 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) Kā dalībniekam, kas turklāt nodrošina *CSIRT* tīkla sekretariātu, Aģentūrai būtu jāatbalsta dalībvalstu *CSIRT* un *CERT-EU* operatīvajā sadarbībā, un tas jādara papildus visiem attiecīgajiem *CSIRT* tīkla uzdevumiem, kas noteikti Tīklu un informācijas drošības (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 ikgadējas 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 un pakalpojumu 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, struktūrām, birojiem un aģentūrām, kā arī attiecīgos gadījumos pēc pieprasījuma dalībvalstīm sniegtu padomus par vajadzību veikt pētījumus tīklu un informācijas drošības, jo īpaši kiberdrošības, jomā.

(37) Kiberdrošības problēmas ir pasaules mēroga jautājumi. Lai uzlabotu 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, struktūrām, birojiem un aģentūrām 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. gadā 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, 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[34]. Personas datu apstrādei Aģentūrā būtu jānotiek saskaņā ar Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti[35]. 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.

(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) Atbilstības novērtēšana ir process, ar ko parāda, vai ir ievērotas ar produktu, procesu, pakalpojumu, sistēmu, personu vai struktūru saistītās konkrētās prasības. Šajā regulā sertifikācija būtu jāuzskata par noteikta veida atbilstības novērtējumu attiecībā uz produkta, procesa, pakalpojuma, sistēmas vai to apvienojumu kiberdrošības iezīmēm ("IKT produkti un pakalpojumi"), ko veic neatkarīga trešā persona, kas nav produkta ražotājs vai pakalpojuma sniedzējs. Sertifikācija pati 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.

(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,

---

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

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

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 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. SAN *SOG-IS* ir visnozīmīgākais sadarbības un savstarpējās atzīšanas modelis drošības sertifikācijas jomā, tomēr tam ir daži būtiski trūkumi, kas saistīti ar tā augstajām izmaksām un ierobežoto tvērumu. Līdz šim ir izstrādāti tikai nedaudzi digitālo produktu aizsardzības profili, piemēram, elektroniskais paraksts, tahogrāfi un viedkartes. Vissvarīgākais ir tas, ka *SOG-IS* 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 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 Savienības 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 produktu un pakalpojumu grupām. Šīs shēmas būtu jāīsteno un jāpārrauga valstu sertifikācijas pārraudzības 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 produkti un pakalpojumi atbilst noteiktām prasībām. Šādas prasības attiecas uz spēju noteiktā apliecinājuma līmenī pretoties darbībām, kas veiktas nolūkā apdraudēt tādu glabāto, pārsūtīto vai apstrādāto datu vai saistīto funkciju, vai pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, ko 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 produktiem un pakalpojumiem piemērojamās kiberdrošības prasības. IKT 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 tehniskajām specifikācijām, būtu jāprecizē kārtība, kādā minētie mērķi tiks sasniegti attiecībā uz konkrētiem IKT produktiem un pakalpojumiem.

(56) Komisijai vajadzētu būt pilnvarotai pieprasīt, lai *ENISA* sagatavo kandidātshēmu konkrētiem IKT 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 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).

(57) Eiropas kiberdrošības sertifikācijas izmantošanai būtu jāpaliek fakultatīvai, ja vien Savienības vai dalībvalstu tiesību aktos nav noteikts citādi. Tomēr, 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.

(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 jāatsauc, ja akreditācijas nosacījumi nav vai vairs netiek izpildīti vai ja atbilstības novērtēšanas struktūras veiktie pasākumi pārkāpj šo regulu.

(59) Ir jāpieprasa, lai visas dalībvalstis izraudzītos vienu kiberdrošības sertifikācijas pārraudzības iestādi, kura pārraudzītu atbilstības novērtēšanas struktūru un to teritorijā izveidoto atbilstības novērtēšanas struktūru izsniegtu sertifikātu atbilstību šīs regulas prasībām un attiecīgajām kiberdrošības sertifikācijas shēmām. Valstu sertifikācijas pārraudzības iestādēm būtu jāizskata sūdzības, ko fiziskas vai juridiskas personas iesniegušas saistībā ar to attiecīgajā teritorijā izveidoto atbilstības novērtēšanas struktūru izsniegtajiem sertifikātiem, 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 sertifikācijas pārraudzības iestādēm vai citām publiskām iestādēm, piemēram, daloties informācijā par IKT produktu un pakalpojumu varbūtēju neatbilstību šās regulas prasībām vai konkrētām kiberdrošības sertifikācijas shēmām.

(60) Lai nodrošinātu Eiropas kiberdrošības sertifikācijas satvara konsekventu piemērošanu, būtu jāizveido Eiropas Kiberdrošības sertifikācijas grupa ("Grupa"), kas sastāv no valstu sertifikācijas pārraudzības iestādēm. 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 Komisijai adresētus atzinumus, kas attiecas uz esošo Eiropas kiberdrošības sertifikācijas shēmu uzturēšanu un pārskatīšanu.

(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.

(62) Būtu jāparedz, ka Aģentūra, atbalstot kiberdrošības sertifikāciju, arī sadarbojas ar Padomes Drošības komiteju un attiecīgo valsts struktūru attiecībā uz klasificētos tīklos izmantojamu kriptogrāfijas produktu apstiprināšanu.

(63) Lai sīkāk precizētu atbilstības novērtēšanas struktūru akreditācijas kritērijus, būtu jādeleģē pilnvaras Komisijai pieņemt aktus saskaņā ar Līguma par Eiropas Savienības darbību 290. pantu. Komisijai būtu jāveic pienācīga apspriešanās sagatavošanas posmā, tostarp ekspertu līmenī. Šīm apspriedēm būtu jānotiek saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu. Konkrēti, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlamentam un Padomei visi dokumenti būtu jāsaņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem vajadzētu būt sistemātiskai piekļuvei Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.

(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 sertifikācijas pārraudzības 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

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

(a) noteikti *ENISA* – ES Kiberdrošības aģentūras (turpmāk "Aģentūra") – mērķi, uzdevumi un organizatoriskie aspekti, un

(b) izklāstīts satvars, kurā jāizveido Eiropas kiberdrošības sertifikācijas shēmas, lai Savienībā IKT 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. *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 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) produktu un pakalpojumu sertifikāciju, kuri ietilpst konkrētās shēmas tvērumā;

(10) "Eiropas kiberdrošības sertifikāts" ir dokuments, ko, apliecinot attiecīgā IKT produkta vai pakalpojuma atbilstību Eiropas kiberdrošības sertifikācijas shēmā noteiktām konkrētām prasībām, izsniegusi atbilstības novērtēšanas struktūra;

(11) "IKT produkts un pakalpojums" ir jebkurš tīklu un informācijas sistēmu elements vai elementu grupa;

(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.

II SADAĻA
ENISA – "ES Kiberdrošības aģentūra"

I NODAĻA
PILNVARAS, MĒRĶI UN UZDEVUMI

3. pants
Pilnvaras

1. Aģentūra veic ar šo regulu uzticētos uzdevumus, lai Savienībā veicinātu augstu kiberdrošības līmeni.

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

3. Aģentūras mērķi un uzdevumi neskar dalībvalstu kompetenci attiecībā uz kiberdrošību un nekādā ziņā darbības, kas attiecas uz sabiedrisko drošību, aizsardzību, valsts drošību, un valsts pasākumus krimināltiesību jomā.

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 politiku.

3. Palīdzot Savienībai, dalībvalstīm un publiskajām un privātajām ieinteresētajām personām palielināt savu tīklu un informācijas sistēmu aizsardzību, attīstīt prasmes un kompetenci kiberdrošības jomā un panākt kibernoturību, Aģentūra Savienībā atbalsta spēju veidošanu un uzlabo gatavību.

4. Aģentūra ar kiberdrošību saistītos jautājumos veicina Savienības līmeņa sadarbību un koordināciju starp dalībvalstīm, Savienības iestādēm, aģentūrām un struktūrām un attiecīgām ieinteresētajām personām, tostarp no privātā sektora.

5. Aģentūra Savienības līmenī palielina kiberdrošības spējas papildināt dalībvalstu rīcību kiberdraudu novēršanā un reaģēšanā uz tiem, it īpaši saistībā ar pārrobežu incidentiem.

6. Aģentūra veicina sertifikācijas izmantošanu, cita starpā palīdzot 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.

5. pants

Uzdevumi saistībā ar Savienības politikas un tiesību aktu izstrādi un īstenošanu

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 pārkāpumiem, 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

Uzdevumi saistībā ar spēju veidošanu

1. Aģentūra palīdz:

(a) dalībvalstīm to centienos uzlabot kiberdrošības problēmu un incidentu novēršanas, atklāšanas, analīzes un risināšanas spējas, sniedzot tām nepieciešamās zināšanas un daloties lietpratībā;

(b) Savienības iestādēm, struktūrām, birojiem un aģentūrām to centienos uzlabot kiberdrošības problēmu un incidentu novēršanas, atklāšanas, analīzes un risināšanas spējas, sniedzot pienācīgu atbalstu ES 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, katru gadu organizējot 7. panta 6. punktā minētās plaša mēroga kiberdrošības mācības Savienības līmenī 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 veicina nozaru, it īpaši Direktīvas (ES) 2016/1148 II pielikumā uzskaitīto nozaru, informācijas apmaiņas un analīzes centru (*ISAC*) izveidi un pastāvīgi tos atbalsta, nodrošinot paraugpraksi un norādījumus par pieejamiem rīkiem un procedūrām, kā arī par to regulatīvo jautājumu risināšanu, kuri saistīti ar informācijas apmaiņu.

7. pants

Uzdevumi saistībā ar Savienības līmeņa operatīvo sadarbību

1. Aģentūra atbalsta operatīvo sadarbību starp kompetentajām publiskajām struktūrām un starp ieinteresētajām personām.

2. Aģentūra sadarbojas operatīvā līmenī un veido sinerģiju ar Savienības iestādēm, struktūrām, birojiem un aģentūrām, 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 aktīvi veicina informācijas apmaiņu un sadarbību starp tā locekļiem.

4. Aģentūra veicina operatīvo sadarbību *CSIRT* tīkla ietvaros, dalībvalstīm sniedzot atbalstu šādi:

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

(b) pēc pieprasījuma sniedzot tehnisko palīdzību, ja noticis incidents, kam ir būtiska vai nozīmīga ietekme;

(c) analizējot vājās vietas, artefaktus un incidentus.

Veicot šos uzdevumus, Aģentūra un *CERT-EU* īsteno strukturētu sadarbību, lai tādējādi no sinerģijas gūtu labumu, it īpaši operatīvajos aspektos.

5. Ja divas vai vairākas attiecīgās dalībvalstis nosūtījušas pieprasījumu, kura vienīgais nolūks ir saņemt padomus par turpmāku incidentu novēršanu, Aģentūra sniedz atbalstu vai veic *ex-post* tehnisko izmeklēšanu pēc skarto uzņēmumu paziņojumiem par incidentiem, kuriem ir būtiska vai nozīmīga ietekme saskaņā ar Direktīvu (ES) 2016/1148. Ja šādi incidenti skar vairāk nekā divas dalībvalstis, Aģentūra, vienojoties ar attiecīgajām dalībvalstīm, šādu izmeklēšanu veic arī pēc pienācīgi pamatota pieprasījuma, ko nosūtījusi Komisija.

Par izmeklēšanas apjomu un procedūru vienojas attiecīgās dalībvalstis un Aģentūra, un šī vienošanās neskar nevienu notiekošu kriminālizmeklēšanu, kas varētu būt bijusi ierosināta par to pašu incidentu. Izmeklēšanas beigās Aģentūra, pamatojoties galvenokārt uz attiecīgo dalībvalstu un uzņēmuma(-u) sniegto informāciju un piezīmēm un vienojoties ar attiecīgajām dalībvalstīm, sagatavo galīgo tehnisko ziņojumu. Kopsavilkums par ziņojumu, kurā galvenā uzmanība pievērsta ieteikumiem par turpmāku incidentu novēršanu, tiks publiskots *CSIRT* tīklā.

6. Aģentūra katru gadu organizē kiberdrošības mācības Savienības līmenī un atbalsta dalībvalstis un ES iestādes, aģentūras un struktūras, pēc to pieprasījuma(-iem) organizējot mācības. Ikgadējās mācības Savienības līmenī ietver tehniskus, operatīvus un stratēģiskus aspektus un palīdz sagatavoties uz sadarbību balstītai reaģēšanai Savienības mērogā tādās situācijās, kad notiktu plašapmēra pārrobežu kiberdrošības incidenti. Aģentūra arī veicina nozaru kiberdrošības mācības un vajadzības gadījumā palīdz tās organizēt sadarbībā ar *ISACS*, un ļauj *ISAC* piedalīties arī Savienības mēroga kiberdrošības mācībās.

7. 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* (brīvprātīgi) vai ar TID direktīvu izveidotie vienotie kontaktpunkti (saskaņā

ar TID direktīvas 14. panta 5. punktu), 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 ziņojumus no valstu avotiem, 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) atbalstot incidenta vai krīzes tehnisko aspektu risināšanu, tostarp atvieglojot tehnisko risinājumu apmaiņu dalībvalstu starpā;

(d) atbalstot ar incidentu vai krīzi saistītās informācijas publiskošanu;

(e) testējot sadarbības plānus, kurus paredzēts izmantot reaģēšanā uz šādiem incidentiem vai krīzēm.

8. *pants*

Uzdevumi saistībā ar tirgu, kiberdrošības sertifikāciju un standartizāciju

Aģentūra:

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

(1) IKT produktiem un pakalpojumiem sagatavojot Eiropas kiberdrošības sertifikācijas kandidātshēmas saskaņā ar šīs regulas 44. pantu;

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

(3) sadarbībā ar valstu sertifikācijas pārraudzības iestādēm un nozares pārstāvjiem apkopojot un publicējot vadlīnijas un izstrādājot labu praksi saistībā ar IKT produktu un pakalpojumu kiberdrošības prasībām;

(b) palīdz izveidot un ieviest Eiropas un starptautiskos riska pārvaldības un IKT produktu un pakalpojumu drošības standartus, kā arī sadarbībā ar dalībvalstīm sagatavot 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

Uzdevumi saistībā ar zināšanām, informāciju un izpratnes veicināšanu

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 ar kiberdrošību saistītās problēmas;

(c) sadarbībā ar ekspertiem no dalībvalstu iestādēm sniedz padomus un norādījumus un dalās ar paraugpraksi attiecībā uz tīklu un informācijas sistēmu drošību, jo īpaši interneta infrastruktūras drošību un tādas infrastruktūras drošību, kas ir Direktīvas (ES) 2016/1148 II pielikumā minēto nozaru pamatā;

(d) apkopo, kārto un īpaši izveidotā portālā publisko Savienības iestāžu, aģentūru un struktūru sniegto informāciju par kiberdrošību;

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

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

(g) ciešā sadarbībā ar dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām organizē regulāras informatīvas kampaņas, lai palielinātu kiberdrošību un uzlabotu šīs informācijas pamanāmību Savienībā.

10. pants

Uzdevumi saistībā ar pētniecību un inovāciju

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

Uzdevumi saistībā ar starptautisko sadarbību

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) pēc Komisijas pieprasījuma veicina paraugprakses apmaiņu attiecīgo starptautisko organizāciju starpā;

(c) pēc pieprasījuma sniedz Komisijai lietpratēju atzinumus.

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; un

(d) Pastāvīgā ieinteresēto personu grupa, kas pilda 20. 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;

(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 iecēlējiestādes 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. 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. Ja vajadzīgs steidzamības dēļ, Valde Administratīvās padomes vārdā var pieņemt konkrētus pagaidu lēmumus, jo īpaši administratīvās pārvaldības lietās, tostarp par iecēlējinstitūcijas pilnvaru deleģējuma apturēšanu un budžeta jautājumiem.

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;

(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;

(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. Izpilddirektors izlemj, vai darbiniekus nepieciešams izvietot vienā vai vairākās dalībvalstīs, lai Aģentūras uzdevumu izpilde būtu rezultatīva un efektīva. Pirms izlemj izveidot vietējo biroju, izpilddirektors saņem Komisijas, Administratīvās padomes un attiecīgās(-o) dalībvalsts(-u) iepriekšēju piekrišanu. Lēmumā norāda vietējā birojā veicamās darbības tvērumu, izvairoties no liekām izmaksām un Aģentūras administratīvo funkciju dublēšanās. Attiecīgā gadījumā vai vajadzības gadījumā ar attiecīgo(-ajām) dalībvalsti(-īm) panāk vienošanos.

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, 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. 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[36] 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.

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.

---

[36] Komisijas 2013. gada 30. septembra Deleģētā regula (ES) Nr. 1271/2013 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.).

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[37] un Lēmumā (ES, *Euratom*) 2015/444[38]. Minētie noteikumi reglamentē klasificētas informācijas apmaiņu, apstrādi un glabāšanu.

25. pants
Piekļuve dokumentiem

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

---

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

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

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

Finansiālie noteikumi

Aģentūrai piemērojamos finansiālos 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 (ES, *Euratom*) Nr. 883/2013[39], 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.

3. *OLAF* var veikt izmeklēšanu, tostarp pārbaudes un inspekcijas uz vietas, saskaņā ar noteikumiem un procedūrām, kas noteiktas Eiropas Parlamenta un Padomes Regulā (ES, *Euratom*) Nr. 883/2013 un Padomes 1996. gada 11. novembra Regulā (*Euratom*, EK) Nr. 2185/96 par pārbaudēm un apskatēm uz vietas, ko Komisija veic, lai aizsargātu Savienības finanšu intereses pret krāpšanu un citām nelikumībām[40], 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.

---

39 Eiropas Parlamenta un Padomes 2013. gada 11. septembra Regula (ES, *Euratom*) Nr. 883/2013 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.).

40 Padomes 1996. gada 11. novembra Regula (*Euratom*, EK) Nr. 2185/96 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 pieci 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 un 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 piecus 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, kas pieņemts pēc Komisijas priekšlikuma.

34. pants

Norīkotie valstu 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 var iegādāties vai atsavināt kustamu un nekustamu īpašumu, kā arī būt par pusi tiesas procesā, vai arī izmantot abas minētās tiesības.

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[41]. 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[42].

---

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

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.

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 padomes apstiprinājums, bet ne vēlāk kā [divus gadus pēc šīs regulas stāšanās spēkā].

---

42 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 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.).

2. Aģentūras mītnes dalībvalsts nodrošina iespējami labākos 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 shēmas

Eiropas kiberdrošības sertifikācijas shēma apliecina, ka IKT produkti un pakalpojumi, kas ir sertificēti saskaņā ar šādu shēmu, atbilst noteiktajām prasībām attiecībā uz to spēju noteiktā apliecinājuma līmenī pretoties darbībai, kas veikta nolūkā apdraudēt tādu glabāto, pārsūtīto vai apstrādāto datu vai funkciju, vai pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, ko piedāvā izmantot minētie produkti, procesi, pakalpojumi un sistēmas vai kam, tos izmantojot, var piekļūt.

44. pants

Eiropas kiberdrošības sertifikācijas shēmas izveidošana un pieņemšana

1. Pēc Komisijas lūguma *ENISA* sagatavo Eiropas kiberdrošības sertifikācijas kandidātshēmu, kas atbilst šīs regulas 45., 46. un 47. pantā noteiktajām prasībām. Dalībvalstis vai saskaņā ar 53. pantu izveidotā Eiropas Kiberdrošības sertifikācijas grupa (“grupa”) var ierosināt Komisijai izveidot Eiropas kiberdrošības sertifikācijas kandidātshēmu.

2. *ENISA*, veidojot šā panta 1. punktā minētās kandidātshēmas, apspriežas ar visām attiecīgajām ieinteresētajām personām un cieši sadarbojas ar Grupu. Grupa sniedz *ENISA* palīdzību un ekspertu padomus, ko *ENISA* pieprasa saistībā ar kandidātshēmas izveidi, un šajā sakarībā vajadzības gadījumā sniedz arī atzinumus.

3. Eiropas kiberdrošības sertifikācijas kandidātshēmu, kas izveidota saskaņā ar šā panta 2. punktu, *ENISA* pārsūta Komisijai.

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

5. *ENISA* uztur īpaši šim nolūkam izveidotu tīmekļa vietni, kurā tā sniedz informāciju par Eiropas kiberdrošības sertifikācijas shēmām un veido publicitāti.

45. pants

Eiropas kiberdrošības sertifikācijas shēmu drošības mērķi

Eiropas kiberdrošības sertifikācijas shēmu veido tā, lai attiecīgā gadījumā tajā ņemtu vērā šādus drošības mērķus:

(a) uzglabātus, pārsūtītus vai citādi apstrādātus datus pasargāt no nejaušas vai neatļautas glabāšanas, apstrādes, piekļuves vai izpaušanas;

(b) uzglabātus, pārsūtītus vai citādi apstrādātus datus pasargāt no nejaušas vai neatļautas iznīcināšanas, pazušanas vai pārveidošanas;

(c) nodrošināt, lai pilnvarotas personas, programmas vai mašīnas varētu piekļūt vienīgi tādiem datiem, pakalpojumiem vai funkcijām, attiecībā uz kuriem viņiem ir piešķirtas piekļuves tiesības;

(d) reģistrēt, kuri dati, funkcijas un pakalpojumi ir nosūtīti, kad un kurš tos ir nosūtījis;

(e) nodrošināt iespēju pārbaudīt, kuriem datiem, pakalpojumiem un funkcijām ir piekļūts, kad tie ir izmantoti un kurš tos ir izmantojis;

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

(g) nodrošināt, lai IKT produktiem un pakalpojumiem būtu atjaunināta datu programmatūra bez zināmām vājajām vietām un lai tiem būtu mehānismi, kas nodrošina drošus programmatūras atjauninājumus.

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, un tie tiks noteikti saskaņā ar šo shēmu piedāvātajiem IKT produktiem un pakalpojumiem.

2. Pamata, būtiskais un augstais apliecinājuma līmenis atbilst šādiem kritērijiem:

(a) pamata apliecinājuma līmenis ir sertifikātiem, kas izsniegti saistībā ar Eiropas kiberdrošības sertifikācijas shēmu, un tas ļauj zināmā mērā paļauties uz uzdotajām vai apgalvotajām IKT produkta vai pakalpojuma kiberdrošības īpašībām, un to raksturo attiecīgas tehniskās specifikācijas, standarti un procedūras, tostarp tehniskā kontrole, kuras mērķis ir samazināt kiberdrošības incidentu risku;

(b) būtisks apliecinājuma līmenis ir sertifikātiem, kas izsniegti saistībā ar Eiropas kiberdrošības sertifikācijas shēmu, un tas ļauj būtiskā mērā paļauties uz uzdotajām vai apgalvotajām IKT produkta vai pakalpojuma kiberdrošības īpašībām, un to raksturo attiecīgas tehniskās specifikācijas, standarti un procedūras, tostarp tehniskā kontrole, kuras mērķis ir būtiski samazināt kiberdrošības incidentu risku;

(c) augsts apliecinājuma līmenis ir sertifikātiem, kas izsniegti saistībā ar Eiropas kiberdrošības sertifikācijas shēmu, un salīdzinājumā ar sertifikātiem, kam ir būtisks apliecinājuma līmenis, tas ļauj augstākā mērā paļauties uz uzdotajām vai apgalvotajām IKT produkta vai pakalpojuma kiberdrošības īpašībām, un to raksturo attiecīgas tehniskās specifikācijas, standarti un procedūras, tostarp tehniskā kontrole, kuras mērķis ir novērst kiberdrošības incidentus.

47. pants

Eiropas kiberdrošības sertifikācijas shēmu elementi

1. Eiropas kiberdrošības sertifikācijas shēmā ir šādi elementi:

(a) sertifikācijas priekšmets un tvērums, arī shēmā ietverto IKT produktu un pakalpojumu tipi vai kategorijas;

(b) detalizēti noteiktas kiberdrošības prasības, pēc kurām izvērtē konkrētus IKT produktus un pakalpojumus, piemēram, atsaucoties uz Savienības vai starptautiskajiem standartiem vai tehniskajām specifikācijām;

(c) attiecīgā gadījumā viens vai vairāki apliecinājuma līmeņi;

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

(e) sertifikācijai nepieciešamā informācija, kas pieteikuma iesniedzējam jāsniedz atbilstības novērtēšanas struktūrām;

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

(g) ja shēmā paredzēta arī uzraudzība, – noteikumi par sertifikācijas prasību ievērošanas uzraudzību, tostarp mehānismi, kas izmantojami, lai pierādītu noteikto kiberdrošības prasību pastāvīgu ievērošanu;

(h) nosacījumi sertifikācijas tvēruma piešķiršanai, saglabāšanai, turpmākai izmantošanai, paplašināšanai un samazināšanai;

(i) noteikumi par sekām, ko rada sertificētu IKT produktu un pakalpojumu neatbilstība sertifikācijas prasībām;

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

(k) noteikumi par uzskaites datu glabāšanu atbilstības novērtēšanas struktūrās;

(l) to valsts kiberdrošības sertifikācijas shēmu identifikācija, kas attiecas uz viena un tā paša veida vai kategoriju IKT produktiem un pakalpojumiem;

(m) izsniegtā sertifikāta saturs.

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 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.

48. pants

Kiberdrošības sertifikācija

1. IKT 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 tiesību aktos nav norādīts citādi.

3. Saskaņā ar šo pantu Eiropas kiberdrošības sertifikātu izdod 51. pantā minētās atbilstības novērtēšanas struktūras, pamatojoties uz kritērijiem, kuri iekļauti saskaņā ar 44. pantu pieņemtā Eiropas kiberdrošības sertifikācijas shēmā.

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

   (a) 50. panta 1. punktā minētā valsts sertifikācijas pārraudzības iestāde;

   (b) struktūra, kas ir akreditēta kā atbilstības novērtēšanas struktūra saskaņā ar 51. panta 1. punktu, vai

   (c) struktūra, kas izveidota saskaņā ar attiecīgās dalībvalsts likumiem, tiesību instrumentiem vai citām oficiālām administratīvajām procedūrām un kas atbilst prasībām, kuras noteiktas tām struktūrām, kas produktus, procesus un pakalpojumus sertificē atbilstīgi standartam ISO/IEC 17065:2012.

5. Fiziska vai juridiska persona, kas par saviem IKT produktiem vai pakalpojumiem iesniedz pieteikumu sertifikācijas mehānismā, sniedz 51. pantā minētajai atbilstības novērtēšanas struktūrai visu sertifikācijas procedūrā nepieciešamo informāciju.

6. Sertifikātus izdod uz laikposmu, kas nav ilgāks par trim gadiem, un tos var atjaunot ar tādiem pašiem nosacījumiem, 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 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 produktu un pakalpojumu spēkā esošās 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 produktiem un pakalpojumiem, uz kuriem jau attiecas spēkā esoša Eiropas kiberdrošības sertifikācijas shēma.

3. Spēkā esošie sertifikāti, kas izsniegti atbilstīgi valsts kiberdrošības sertifikācijas shēmām, paliek spēkā līdz to termiņa beigām.

50. pants

Valsts sertifikācijas pārraudzības iestādes

1. Katra dalībvalsts norīko valsts sertifikācijas pārraudzības iestādi.

2. Katra dalībvalsts informē Komisiju par to, kura iestāde norīkota.

3. Katra valsts sertifikācijas pārraudzības iestāde organizatoriskās, tiesiskās struktūras un lēmumu pieņemšanas ziņā ir neatkarīga no tās pārraudzītajiem subjektiem.

4. Dalībvalstis nodrošina, ka valsts sertifikācijas pārraudzības 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 sertifikācijas pārraudzības iestādes:

   (a) valsts līmenī uzrauga un īsteno šīs sadaļas noteikumu piemērošanu un pārrauga, vai sertifikāti, ko izsniegušas atbilstības novērtēšanas struktūras, kuras izveidotas to attiecīgajās teritorijās, atbilst šajā sadaļā izklāstītajām un attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā paredzētajām prasībām;

   (b) pārrauga un uzrauga šajā regulā paredzēto atbilstības novērtēšanas struktūru darbību, tostarp saistībā ar atbilstības novērtēšanas struktūru paziņojumiem un saistītajiem uzdevumiem, kas izklāstīti šīs regulas 52. pantā;

   (c) izskata sūdzības, ko fiziskas vai juridiskas personas iesniegušas saistībā ar to attiecīgajā teritorijā izveidoto atbilstības novērtēšanas struktūru izsniegtajiem sertifikātiem, pienācīgā mērā izmeklē sūdzības priekšmetu un samērīgā termiņā informē sūdzības iesniedzēju par lietas virzību un izmeklēšanas rezultātiem;

   (d) sadarbojas ar citām valsts sertifikācijas pārraudzības iestādēm vai citām publiskām iestādēm, piemēram, daloties informācijā par IKT produktu un pakalpojumu varbūtēju neatbilstību šās regulas prasībām vai konkrētām Eiropas kiberdrošības sertifikācijas shēmām;

   (e) uzrauga būtiskas norises kiberdrošības sertifikācijas jomā.

7. Katrai valsts sertifikācijas pārraudzības iestādei ir vismaz šādas pilnvaras:

   (a) pieprasīt, lai atbilstības novērtēšanas struktūras un Eiropas kiberdrošības sertifikātu turētāji sniegtu informāciju, ko tā pieprasījusi sava uzdevuma izpildei;

   (b) atbilstības novērtēšanas struktūrās un Eiropas kiberdrošības sertifikātu turētāju 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 vai sertifikātu turētāji 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, 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 sertifikācijas pārraudzības 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 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.

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 šā panta 1. punktā minēto akreditāciju atsauc.

52. pants

Paziņošana

1. Par katru Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta saskaņā ar 44. pantu, valsts sertifikācijas pārraudzības iestādes Komisijai paziņo, kuras akreditētās atbilstības novērtēšanas struktūras akreditētas 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 sertifikācijas pārraudzības iestāde var iesniegt Komisijai pieprasījumu no šā panta 2. punktā minētā saraksta svītrot atbilstības novērtēšanas struktūru, par kuru paziņojusi minētā valsts sertifikācijas pārraudzības iestāde. Mēneša laikā no dienas, kad saņemts valsts sertifikācijas pārraudzības 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 sertifikācijas pārraudzības iestādes. Iestādes pārstāv to vadītāji vai citi augsta līmeņa valstu sertifikācijas pārraudzības iestāžu pārstāvji.

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 kandidātshēmu izveidi atbilstīgi šīs regulas 44. pantam;

(c) ierosināt, lai Komisija pieprasa Aģentūrai izveidot Eiropas kiberdrošības sertifikācijas kandidātshēmu atbilstīgi šīs regulas 44. pantam;

(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 sertifikācijas pārraudzības iestāžu sadarbību atbilstīgi šai sadaļai, izmantojot informācijas apmaiņu un jo īpaši ieviešot metodes efektīvai informācijas apmaiņai visos kiberdrošības sertifikācijas aspektos.

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

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
Komitejas procedūra

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

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

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.*

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

Briselē,

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

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

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/regula")

1.2. Attiecīgās politikas jomas

Politikas joma: 09 – Komunikācijas tīkli, saturs un tehnoloģija

Darbība: 09 02 – Digitālais vienotais tirgus

1.3. Priekšlikuma/iniciatīvas būtība

☒Priekšlikums/iniciatīva attiecas uz **jaunu darbību (III sadaļa – Sertifikācija)**

☐ Priekšlikums/iniciatīva attiecas uz **jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību**[43]

☒Priekšlikums/iniciatīva attiecas uz **esošas darbības pagarināšanu** (**II sadaļa – *ENISA* pilnvaras)**

☐ Priekšlikums/iniciatīva attiecas uz **darbību, kas pārveidota jaunā darbībā**

1.4. Mērķis(-i)

1.4.1. Komisijas daudzgadu stratēģiskie mērķi, kurus plānots sasniegt ar priekšlikumu/iniciatīvu

1. Palielināt dalībvalstu, uzņēmumu un visas ES noturību.

2. Nodrošināt IKT produktu un pakalpojumu ES iekšējā tirgus pienācīgu darbību.

3. Palielināt to ES uzņēmumu konkurētspēju pasaulē, kuri darbojas IKT jomā.

4. Tuvināt dalībvalstu normatīvos un administratīvos aktus, kuri nosaka pienākumu nodrošināt kiberdrošību.

1.4.2. Konkrētais(-ie) mērķis(-i)

Paturot prātā vispārējos mērķus, pārskatītās Kiberdrošības stratēģijas plašākā kontekstā ar šo aktu, kurā ir noteikta *ENISA* darbības joma un pilnvaras un izveidots Eiropas sertifikācijas satvars IKT produktu un pakalpojumu jomā, plānots sasniegt šādus konkrētus mērķus:

1. Pastiprināt dalībvalstu un uzņēmumu **spējas un gatavību**.
2. Uzlabot **sadarbību un koordināciju** starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām.
3. Uzlabot **ES līmeņa spējas, lai papildinātu dalībvalstu rīcību**, it īpaši pārrobežu kiberkrīžu gadījumā.
4. Uzlabot iedzīvotāju un uzņēmumu **izpratni** kiberdrošības jautājumos.
5. Vairot uzticēšanos digitālajam vienotajam tirgum un digitālajai inovācijai, uzlabojot IKT produktu un pakalpojumu **kiberdrošības apliecinājuma vispārējo pārredzamību**[44].

[43] Kā paredzēts Finanšu regulas 54. panta 2. punkta attiecīgi a) vai b) apakšpunktā.

***ENISA* palīdzēs sasniegt minētos mērķus šādi.**

Lielāks politikas veidošanas atbalsts – dod norādījumus un padomus Komisijai un dalībvalstīm, kā atjaunināt un izstrādāt visaptverošu normatīvu regulējumu kiberdrošības jomā, kā arī ar konkrētām nozarēm saistītas politikas un tiesību aktu iniciatīvas, kas ietver ar kiberdrošību saistītus aspektus; ar lietpratību un palīdzību sekmē Sadarbības grupas darbu (Direktīvas (ES) 2016/1148 11. pants); atbalsta politikas izstrādi un īstenošanu elektroniskās identifikācijas un uzticamības pakalpojumu jomā; veicina paraugprakses apmaiņu kompetento iestāžu starpā.

Lielāks spēju veidošanas atbalsts – sniedz atbalstu dalībvalstīm, Savienības iestādēm, struktūrām, birojiem un aģentūrām, lai veidotu un uzlabotu kiberdrošības problēmu un incidentu novēršanu, atklāšanu, analīzi, kā arī spēju reaģēt uz tiem; pēc pieprasījuma palīdz dalībvalstīm izveidot valstu *CSIRT* un valstu kiberdrošības stratēģijas; palīdz Savienības iestādēm izstrādāt un pārskatīt Savienības kiberdrošības stratēģijas; organizē kiberdrošības mācības; palīdz dalībvalstīm ar Sadarbības grupas starpniecību apmainīties ar paraugpraksi; veicina nozaru informācijas apmaiņas un analīzes centru (*ISAC*) izveidi.

Operatīvās sadarbības un krīzes pārvarēšanas atbalsts – izveidojot sistemātiskāku sadarbību ar Savienības iestādēm, struktūrām, birojiem un aģentūrām, kas nodarbojas ar kiberdrošības, kibernoziedzības apkarošanas un privātuma un personas datu aizsardzības jautājumiem, atbalsta sadarbību starp kompetentajām publiskajām iestādēm un starp ieinteresētajām personām; nodrošina *CSIRT* tīkla sekretariātu (Direktīvas (ES) 2016/1148 12. panta 2. punkts), kā arī sekmē operatīvu sadarbību tīklā, kopā ar *CERT-EU* pēc pieprasījuma atbalstot dalībvalstis; organizē regulāras kiberdrošības mācības; palīdz sagatavoties uz sadarbību balstītai reaģēšanai uz plašapmēra pārrobežu kiberdrošības incidentiem vai krīzēm; sadarbībā ar *CSIRT* tīklu veic *ex-post* tehnisko izmeklēšanu pēc nopietniem incidentiem un sniedz ieteikumus par turpmāko rīcību.

Ar tirgu saistīti uzdevumi (standartizācija, sertifikācija) – pilda vairākas funkcijas, īpaši atbalstot iekšējo tirgu: veido kiberdrošības "tirgus novērošanas centru", analizējot attiecīgās kiberdrošības tirgus tendences, lai labāk saskaņotu pieprasījumu un piedāvājumu; atbalsta un veicina Savienības politikas izstrādi un īstenošanu IKT produktu un pakalpojumu kiberdrošības sertifikācijas jomā, veidojot IKT produktu un pakalpojumu Eiropas kiberdrošības sertifikācijas kandidātshēmas, nodrošinot Savienības Kiberdrošības sertifikācijas grupas sekretariātu un sadarbībā ar valsts pārraudzības iestādēm un nozares pārstāvjiem sniedzot vadlīnijas un izstrādājot paraugpraksi attiecībā uz IKT produktu un pakalpojumu drošības prasībām. **Lielāks zināšanu, informācijas un izpratnes veicināšanas atbalsts** – sniedz palīdzību un padomus Komisijai un dalībvalstīm, lai visā Savienībā panāktu augstu zināšanu līmeni jautājumos, kas saistīti ar tīklu un informācijas drošības politiku un tās piemērošanu nozares ieinteresētajām personām. Tas nozīmē arī apkopot, kārtot un īpaši izveidotā portālā publiskot informāciju par tīklu un informācijas sistēmu drošību [jeb kiberdrošību]. Cits svarīgs aspekts ir izpratnes uzlabošanas un informatīvās kampaņas, kuru mērķis ir informēt par kiberdrošības risku jautājumiem plašu sabiedrību.

Lielāks atbalsts pētniecībai un inovācijai – sniedz padomus par pētniecības vajadzībām un prioritāšu noteikšanu kiberdrošības jomā.

---

[44] Kiberdrošības apliecinājuma pārredzamība nozīmē, ka lietotājiem ir pietiekama informācija par kiberdrošības rekvizītiem, kas ļauj objektīvi noteikt konkrētā IKT produkta, pakalpojuma vai procesa drošības līmeni.

Atbalsts starptautiskajai sadarbībai – atbalsta Savienības centienus sadarboties ar trešām valstīm un starptautiskām organizācijām, lai veicinātu starptautisko sadarbību kiberdrošības jomā.

SERTIFIKĀCIJA

Palielinot IKT produktu un pakalpojumu kiberdrošības apliecinājuma vispārējo pārredzamību[45] un tādējādi vairojot uzticēšanos digitālajam vienotajam tirgum un digitālajai inovācijai, **sertifikācijas satvars palīdzēs sasniegt mērķus**. Tam arī vajadzētu palīdzēt izvairīties no ES sertifikācijas shēmu, saistīto drošības prasību un vērtēšanas kritēriju sadrumstalotības dažādās dalībvalstīs un nozarēs.

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

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz finansējuma saņēmējiem / mērķgrupām.

Paredzams, ka stiprināta *ENISA* (atbalsts attiecībā uz spējām, novēršanu, sadarbību un izpratni ES līmenī, tādējādi palielinot vispārējo ES kibernoturību), kā arī atbalsts ES IKT produktu un pakalpojumu sertifikācijas satvaram ļaus panākt ietekmi, kā izklāstīts turpmāk (nepilnīgs saraksts).

Vispārējā ietekme

- Visumā pozitīva ietekme uz iekšējo tirgu – samazināta tirgus sadrumstalotība un uzticēšanās digitālajām tehnoloģijām, ko ļauj panākt labāka sadarbība, saskaņotāku pieeju izmantošana ES kiberdrošības politikas jautājumos un uzlabotas spējas ES līmenī. Tam vajadzētu radīt labvēlīgu ekonomisko ietekmi, jo tas palīdzēs samazināt izmaksas par kiberdrošību/ kibernoziegumu incidentu risināšanu, attiecībā uz ko aplēstā ekonomiskā ietekme Savienībā ir 0,41 % no Eiropas Savienības IKP (t. i., apmēram EUR 55 miljardi).

Konkrēti rezultāti

Palielinātas dalībvalstu un uzņēmumu kiberdrošības spējas un gatavība

- Palielinātas dalībvalstu un uzņēmumu kiberdrošības spējas un gatavība (pateicoties kiberdraudu un incidentu ilgtermiņa stratēģiskai analīzei, norādījumiem un ziņojumiem, lietpratības un labas prakses apmaiņai, apmācības un mācību materiālu pieejamībai, intensīvākām *Cyber Europe* mācībām).

- Uzlabotas privātā sektora dalībnieku spējas, pateicoties atbalstam, ko sniedz informācijas apmaiņas un analīzes centru (*ISAC*) izveide dažādās nozarēs.

- Uzlabota ES un dalībvalstu kiberdrošības gatavība, pateicoties tam, ka ir pieejami *Cyber Europe* mācībās testēti labi sagatavoti un saskaņoti plāni attiecībā uz plašapmēra pārrobežu kiberdrošības incidentiem.

Uzlabota sadarbība un koordinācija starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām

- Uzlabota sadarbība gan publiskajā un privātajā sektorā, gan šo sektoru starpā.

- Konsekventāka pieeja TID direktīvas īstenošanā pāri robežām un starp nozarēm.

- Uzlabota sadarbība sertifikācijas jomā, pateicoties institucionālajam satvaram, kas ļauj izveidot Eiropas kiberdrošības sertifikācijas shēmas un izstrādāt kopēju politiku šajā jomā.

[45] Kiberdrošības apliecinājuma pārredzamība nozīmē, ka lietotājiem ir pietiekama informācija par kiberdrošības rekvizītiem, kas ļauj objektīvi noteikt konkrētā IKT produkta, pakalpojuma vai procesa drošības līmeni.

Uzlabotas ES līmeņa spējas papildināt dalībvalstu rīcību

- Uzlabota ES operatīvā jauda, lai pēc pieprasījuma un attiecībā uz ierobežotu un iepriekš noteiktu pakalpojumu klāstu papildinātu un atbalstītu dalībvalstu rīcību. Paredzams, ka uzlabotās spējas pozitīvi ietekmēs incidentu novēršanu, atklāšanu un reaģēšanu uz tiem gan dalībvalstu, gan Savienības līmenī.

Uzlabota iedzīvotāju un uzņēmumu izpratne kiberdrošības jautājumos

- Uzlabota iedzīvotāju un uzņēmumu vispārējā izpratne kiberdrošības jautājumos.

- Uzlabota spēja izdarīt apzinātu izvēli attiecībā uz IKT produktu un pakalpojumu iegādi, to vērtēšanā balstoties uz kiberdrošības sertifikāciju.

Lielāka uzticēšanās digitālajam vienotajam tirgum un digitālajai inovācijai, ko sniedz IKT produktu un pakalpojumu kiberdrošības apliecinājuma labāka pārredzamība

- Labāka IKT produktu un pakalpojumu kiberdrošības apliecinājuma pārredzamība[46], pateicoties drošības sertificēšanas procedūru vienkāršošanai, kas iespējama ES mēroga satvarā.

- Augstāks IKT produktu un pakalpojumu drošības rekvizītu apliecinājuma līmenis.

- Plašāka drošības sertifikācijas ieviešana, ko sekmē vienkāršotas procedūras, samazinātas izmaksas un tādas ES mēroga uzņēmējdarbības iespējas, ko nekavē tirgus sadrumstalotība.

- Augstāka konkurētspēja ES kiberdrošības tirgū, kas iespējama, jo ir samazinātas izmaksas un administratīvais slogs MVU un novērsti iespējamie šķēršļi iekļūšanai tirgū, kurus radījušas daudzās un dažādās valstu sertifikācijas sistēmas.

Citāda ietekme

- Nevienam mērķim nav paredzama būtiska ietekme uz vidi.

- Attiecībā uz ES budžetu, var paredzēt ieguvumus efektivitātes ziņā, ko sniegtu sadarbības uzlabošana un darbību saskaņošana starp ES iestādēm, aģentūrām un struktūrām.

1.4.4. Rezultātu un ietekmes rādītāji

Norādīt priekšlikuma/iniciatīvas īstenošanas uzraudzībā izmantojamos rādītājus.

(g)

Mērķis: pastiprināt dalībvalstu un uzņēmumu spējas un gatavību

- *ENISA* organizēto mācību skaits.
- *ENISA* nepastarpināti sniegtās palīdzības ģeogrāfiskais pārklājums (valstu un jomu skaits).
- Sagatavotības līmenis, ko dalībvalstis sasniegušas attiecībā uz *CSIRT* gatavību veikt kiberdrošības pasākumus un pārraudzīt ar kiberdrošību saistītos regulatīvos pasākumus.
- Vairāki ES mēroga labas prakses piemēri attiecībā uz *ENISA* nodrošināto kritisko infrastruktūru.

[46] Kiberdrošības apliecinājuma pārredzamība nozīmē, ka lietotājiem ir pietiekama informācija par kiberdrošības rekvizītiem, kas ļauj objektīvi noteikt konkrētā IKT produkta, pakalpojuma vai procesa drošības līmeni.

- Vairāki ES mēroga labas prakses piemēri attiecībā uz *ENISA* nodrošinātiem MVU.
- Kiberdraudu un incidentu ikgadējās stratēģiskās analīzes publicēšana, kas ļauj *ENISA* apzināt jaunās tendences.
- Regulārs *ENISA* ieguldījums Eiropas standartizācijas organizāciju (*ESO*) kiberdrošības darba grupu darbā.

Mērķis: uzlabot sadarbību un koordināciju starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām

- Daudzas dalībvalstis, kas savā politikas izstrādē izmantojušas *ENISA* ieteikumus un atzinumus.
- Daudzas ES iestādes, aģentūras un struktūras, kas savā politikas izstrādē izmantojušas *ENISA* ieteikumus un atzinumus.
- *CSIRT* tīkla darba programmas regulāra īstenošana un labi funkcionējoša *CSIRT* tīkla IT infrastruktūra un saziņas kanāli.
- Daudzi tehniskie ziņojumi, kas pieejami Sadarbības grupai, kura tos arī izmanto.
- Konsekventa pieeja TID direktīvas īstenošanā pāri robežām un starp nozarēm.
- Daudzi *ENISA* veikti novērtējumi par reglamentējošo prasību ievērošanu.
- Daudzi dažādās nozarēs, jo īpaši ar kritisko infrastruktūru saistītās jomās, izveidoti *ISAC*.
- Tādas informācijas platformas izveide un regulāra izmantošana, kurā tiek izplatīta ES iestāžu, aģentūru un struktūru sniegta kiberdrošības informācija.
- Regulārs ieguldījums ES pētniecības un inovācijas darba programmu sagatavošanā.
- Panākta vienošanās par sadarbību starp *ENISA*, *EC3* un *CERT-EU*.
- Vairākas sertifikācijas shēmas, kas iekļautas šajā satvarā un tam atbilstīgi veidotas.

Mērķis: uzlabot ES līmeņa spējas, lai papildinātu dalībvalstu rīcību, it īpaši pārrobežu kiberkrīžu gadījumā

- Kiberdraudu un incidentu ikgadējās stratēģiskās analīzes publicēšana, kas ļauj *ENISA* apzināt jaunās tendences.
- Par tādiem incidentiem apkopotas informācijas publicēšana, par kuriem *ENISA* paziņojusi saskaņā ar TID direktīvu.
- Daudzas Eiropas mēroga mācības, ko koordinē Aģentūra, vairākas dalībvalstis un iesaistītās organizācijas.
- Daudzi pieprasījumi atbalstīt dalībvalstis saistībā ar reaģēšanu ārkārtas situācijās, kuri adresēti *ENISA*, bet kuru izpildi nodrošina Aģentūra.
- Daudzas vājo vietu, artefaktu un incidentu analīzes, ko *ENISA* veic sadarbībā ar *CERT-EU*.
- Tādu ziņojumu pieejamība, kas sagatavoti par situāciju ES mērogā un kas balstīti uz informāciju, ko plašapmēra pārrobežu kiberdrošības incidenta gadījumā *ENISA* pieejamu darījušas dalībvalstis un citi subjekti.

Mērķis: uzlabot iedzīvotāju un uzņēmumu izpratni kiberdrošības jautājumos

- Regulāras ES un valsts mēroga izpratnes veicināšanas kampaņas un regulāri atjaunināti temati atbilstīgi jaunajām mācību vajadzībām.
- Uzlabota ES iedzīvotāju izpratne par kiberdrošību.
- Regulāras viktorīnas, kas uzlabo izpratni par kiberdrošību, un laika gaitā aizvien lielāks pareizo atbilžu īpatsvars.
- Darbiniekiem un organizācijām adresētas regulāras publikācijas par kiberdrošības un kiberhigiēnas labu praksi.

Mērķis: vairot uzticēšanos digitālajam vienotajam tirgum un digitālajai inovācijai, uzlabojot IKT produktu un pakalpojumu kiberdrošības apliecinājuma[47] vispārējo pārredzamību

- Daudzas ES satvarā iekļautas shēmas.
- Samazinātas ar IKT drošības sertifikāta saņemšanu saistītās izmaksas.
- Daudzas un dažādās dalībvalstīs darbojošās atbilstības novērtēšanas struktūras, kas specializējušās IKT sertifikācijas jautājumos.
- Eiropas Kiberdrošības sertifikācijas grupas izveide un regulāri organizētas sanāksmes.
- Vadlīnijas par sertifikāciju saskaņā ar spēkā esošo ES regulējumu.
- Regulāras publikācijas, kurās izanalizētas aktuālākās tendences ES kiberdrošības tirgū.
- Daudzi IKT produkti un pakalpojumi, kas sertificēti atbilstīgi Eiropas IKT drošības sertifikācijas satvara noteikumiem.
- Vairāk tādu galalietotāju, kuriem ir izpratne par IKT produktu un pakalpojumu drošības aspektiem.

(h)

1.4.5. Īstermiņa vai ilgtermiņa vajadzības

Ņemot vērā regulatīvās prasības un strauji mainīgo kiberdrošības apdraudējuma ainu, ir jāpārskata *ENISA* pilnvaras un jānosaka jauns uzdevumu un funkciju kopums, lai tādējādi varētu rezultatīvi un efektīvi atbalstīt dalībvalstu, ES iestāžu un citu ieinteresēto personu pūliņus Eiropas Savienībā nodrošināt drošu kibertelpu. Ierosināto pilnvaru tvērums ir stingri noteikts, nostiprinot jomas, kurās Aģentūra ir apliecinājusi nepārprotamu pievienoto vērtību, un pievienojot jaunas jomas, kurās atbalsts jāsniedz atbilstīgi jaunajām politiskajām prioritātēm un instrumentiem, sevišķi TID direktīvai, pārskatītajai ES kiberdrošības stratēģijai, ES kiberdrošības plānam sadarbībai kiberkrīžu jomā un IKT drošības sertifikācijai. Ierosinātās jaunās pilnvaras tiecas piešķirt Aģentūrai lielāku un nozīmīgāku lomu, īpaši paredzot, ka tā arī palīdzētu dalībvalstīm aktīvāk vērsties pret konkrētu apdraudējumu (operatīvās jaudas) un kļūtu par lietpratības centru, kas atbalsta dalībvalstis un Komisiju kiberdrošības sertifikācijas lietās.

Tajā pašā laikā priekšlikumos ir izveidots Eiropas kiberdrošības sertifikācijas satvars IKT produktiem un pakalpojumiem un noteiktas *ENISA* būtiskās funkcijas un uzdevumi

[47] Kiberdrošības apliecinājuma pārredzamība nozīmē, ka lietotājiem ir pietiekama informācija par kiberdrošības rekvizītiem, kas ļauj objektīvi noteikt konkrētā IKT produkta, pakalpojuma vai procesa drošības līmeni.

kiberdrošības sertifikācijas sfērā. Satvarā ir noteikti kopīgi noteikumi un procedūras, kas attiecībā uz konkrētiem IKT produktiem/pakalpojumiem vai kiberdrošības riskiem ļauj izveidot ES mēroga kiberdrošības sertifikācijas shēmas. Eiropas kiberdrošības sertifikācijas shēmu izveide šajā satvarā ļautu saskaņā ar minētajām shēmām izdotus sertifikātus uzskatīt par derīgiem un atzīt visās dalībvalstīs un novērst tirgus pašreizējo sadrumstalotību.

1.4.6. Savienības iesaistīšanās pievienotā vērtība

Kiberdrošība ir patiesi globāla problēma, tai ir pārrobežu raksturs un aizvien biežāk, ņemot vērā tīklu un informācijas sistēmu savstarpējo atkarību, tā vienlaikus skar vairākas nozares. Kiberdrošības incidentu skaits, sarežģītība un apmērs un to ietekme uz ekonomiku un sabiedrību pieaug, un laikā gaitā līdz ar tehnoloģiju attīstību, piemēram, lietu interneta izplatīšanos, paredzams, ka to kļūs vēl vairāk. Tādējādi nav paredzams, ka nākotnē varētu samazināties vajadzība pēc lielākiem kopējiem dalībvalstu, ES iestāžu, privātā sektora ieinteresēto personu centieniem nolūkā risināt kiberdrošības apdraudējuma problēmu.

Kopš tās izveides 2004. gadā *ENISA* mērķis ir bijis veicināt sadarbību starp dalībvalstīm un TID ieinteresētajām personām, tostarp atbalstīt publiskā un privātā sektora sadarbību. Šis sadarbības atbalsts ietvēra tehnisko darbu, kas bija jāveic, lai ES mērogā iegūtu pilnīgu skatījumu par apdraudējumiem, ekspertu grupas izveidi un kiberincidentu un krīžu pārvarēšanas mācību organizēšanu Eiropas mērogā publiskā un privātā sektora dalībniekiem (jo īpaši "*Cyber Europe*"). TID direktīvā tika noteikti papildu *ENISA* uzdevumi, tostarp *ENISA* uzdevums nodrošināt *CSIRT* tīkla sekretariātu, kas bija vajadzīgs dalībvalstu operatīvajai sadarbībai.

Pievienotā vērtība, ko sniedz rīcība ES līmenī, it īpaši sekmējot sadarbību starp dalībvalstīm, kā arī starp tīklu un informācijas drošības kopienām, ir atzīta 2016. gada Padomes secinājumos[48], un tā arī skaidri parādās *ENISA* 2017. gada izvērtējumā, kurā redzams, ka Aģentūras pievienotā vērtība galvenokārt izpaužas kā tās spēja uzlabot sadarbību galvenokārt starp šīm ieinteresētajām personām. ES līmenī nav citu struktūru, kas atbalstītu tik plašu sadarbību starp TID jautājumos ieinteresētajām personām.

ENISA pievienotā vērtība, ko sniedz kiberdrošības kopienu un ieinteresēto personu apvienošana, redzama arī sertifikācijas jomā. Pieaugot kibernoziedzībai un drošības draudiem, ir izstrādātas valstu iniciatīvas, kurās noteiktas augsta līmeņa kiberdrošības un sertifikācijas prasības attiecībā uz tradicionālās infrastruktūrās izmantotiem IKT komponentiem. Šīm iniciatīvām ir būtiska nozīme, taču līdz ar tām arī parādās vienotā tirgus sadrumstalotības un sadarbspējas problēmu risks. IKT pārdevējam, lai varētu pārdot savu produktu vairāku dalībvalstu tirgos, var būt jāiztur vairākas sertifikācijas procedūras. Pašreizējo sertifikācijas shēmu neefektivitātes/nelietderīguma problēma, visticamāk, netiks atrisināta bez ES iejaukšanās. Ja netiks veikti pasākumi, īsā līdz vidēji ilgā termiņā (nākamajos 5–10 gados), parādoties jaunām sertifikācijas shēmām, tirgus sadrumstalotība, visdrīzāk, kļūs aizvien lielāka. Tādējādi nepietiekama šādu shēmu koordinācija un sadarbspēja samazina digitālā vienotā tirgus potenciālu. Tas apliecina pievienoto vērtību, ko sniedz IKT produktu un pakalpojumu Eiropas kiberdrošības sertifikācijas satvara izveide, ar kuru tiek noteikti tādi nosacījumi, kas ir piemērotākie, lai rezultatīvi risinātu problēmu, kas saistīta ar daudzo sertifikācijas procedūru līdzāspastāvēšanu dažādās

[48] Padomes 2016. gada 15. novembra secinājumi par paziņojumu "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari".

dalībvalstīs, samazinātu sertificēšanas izmaksas un tādējādi ES palielinātu sertifikācijas vispārējo pievilcību gan no komerciālā, gan konkurences viedokļa.

1.4.7. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

Saskaņā ar *ENISA* juridisko pamatu Komisija ir veikusi Aģentūras izvērtēšanu, ietverot gan neatkarīgu pētījumu, gan sabiedrisko apspriešanu. Izvērtējumā secināts, ka *ENISA* mērķi joprojām ir aktuāli. Tehnoloģijām strauji attīstoties, parādoties jauniem draudiem un ievērojamajai vajadzībai uzlabot tīklu un informācijas drošību (TID) visā ES, ir jāsekmē tehniskā lietpratība saistībā ar tīklu un informācijas drošības jautājumu nepārtraukto attīstību. Dalībvalstīs ir jāattīsta spēja izprast šos draudus un reaģēt uz tiem, un dažādu tematisko jomu un iestāžu ieinteresētajām personām ir jāsadarbojas.

Piedāvājot spēju veidošanu 28 dalībvalstīs, veicinot sadarbību starp dalībvalstīm un TID ieinteresētajām personām, Aģentūra ir sekmīgi palīdzējusi uzlabot TID Eiropā; tāpat tā dalījusies lietpratībā, palīdzējusi vedot kopienas un atbalstījusi politikas izstrādi.

ENISA zināmā mērā ir spējusi ietekmēt plašo TID jomu, taču tai nav pilnībā izdevies izveidot spēcīgu zīmolu un iemantot pietiekamu pazīstamību, lai taptu atzīta par galveno Eiropas lietpratības centru. Izskaidrojums tam ir *ENISA* plašās pilnvaras un nesamērīgi mazie resursi. Turklāt *ENISA* joprojām ir vienīgā ES aģentūra ar noteikta termiņa pilnvarām, kas tādējādi ierobežo tās spēju veidot ilgtermiņa ieceres un pastāvīgi atbalstīt ieinteresētās personas. Tas ir pretrunā arī TID direktīvai, kurā paredzēti *ENISA* uzdevumi bez noteikta termiņa.

Patlaban attiecībā uz IKT produktu un pakalpojumu kiberdrošības sertifikāciju nav izveidots Eiropas satvars. Tomēr, pieaugot kibernoziedzībai un drošības draudiem, ir izstrādātas valstu iniciatīvas, kuras savukārt rada vienotā tirgus sadrumstalotības risku.

1.4.8. Saderība un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

Šī iniciatīva ir lielā mērā saskanīga ar spēkā esošo politiku, it īpaši iekšējā tirgus jomā. Tā ir arī atbilstīga vispārējai pieejai kiberdrošības jomā, kā noteikts digitālā vienotā tirgus stratēģijas pārskatā, lai papildinātu visaptverošo pasākumu kopumu, piemēram, ES kiberdrošības stratēģijas pārskatu, plānu sadarbībai kiberkrīžu jomā un kibernoziedzības apkarošanas iniciatīvas. Tas nodrošinātu saskaņotību ar spēkā esošajiem kiberdrošības tiesību aktiem, jo īpaši TID direktīvu, un tā veidota, pamatojoties uz šiem aktiem, tādējādi ar uzlabotām spējām, sadarbību, riska pārvaldību un labāku izpratni par kiberdrošību palielinot kibernoturību ES.

Ierosinātajiem sertifikācijas pasākumiem vajadzētu risināt iespējamās sadrumstalotības problemātiku, ko rada pašreizējās un jaunās valstu sertifikācijas shēmas, un tādējādi sekmēt digitālā vienotā tirgus izveidi. Iniciatīva arī atbalsta un papildina TID direktīvas īstenošanu, direktīvas tvērumā iekļautajiem uzņēmumiem piedāvājot rīku, kuru izmantojot, tie ES mērogā var pierādīt atbilstību TID direktīvas prasībām.

Eiropas IKT kiberdrošības sertifikācijas shēma, kā ierosināts, neskar Vispārīgo datu aizsardzības regulu (VDAR)[49] un jo īpaši attiecīgos noteikumus par sertifikāciju[50], jo tie attiecas uz personas datu apstrādes drošību. Un, visbeidzot, bet ne mazāk svarīgi, ir tas, ka topošajā Eiropas satvarā ierosināto shēmu pamatā, cik vien tas ir iespējams, būtu jāizmanto starptautiskie standarti, lai tādējādi izvairītos no tirdzniecības šķēršļiem un nodrošinātu saskaņotību ar starptautiskajām iniciatīvām.

49 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula).

50 Piemēram, 42. pants (sertifikācija) un 43. pants (sertifikācijas struktūras), kā arī 57., 58. un 70. pants, kuri attiecas uz neatkarīgo pārraudzības iestāžu uzdevumiem un pilnvarām un Eiropas Datu aizsardzības kolēģijas uzdevumiem.

1.5. Ilgums un finansiālā ietekme

☐ **Ierobežota ilguma** priekšlikums/iniciatīva

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

– ☐ Finansiālā ietekme: GGGG.– GGGG.

☒ **Beztermiņa** priekšlikums/iniciatīva

– Īstenošana ar uzsākšanas periodu no 2019. līdz 2020. gadam,

– pēc kura turpinās normāla darbība

1.6. Paredzētie pārvaldības veidi[51]

☒ Komisijas īstenota **tieša pārvaldība** (III sadaļa – Sertifikācija):

– ☐ ko veic izpildaģentūras.

☐ **Dalīta pārvaldība** kopā ar dalībvalstīm

☒ **Netieša pārvaldība**, kurā budžeta īstenošanas uzdevumi uzticēti:

☐ starptautiskām organizācijām un to aģentūrām (precizēt);

☐EIB un Eiropas Investīciju fondam;

☒ Finanšu regulas 208. un 209. pantā minētajām struktūrām (II sadaļa – *ENISA*);

☐ publisko tiesību subjektiem;

☐ privāttiesību subjektiem, kas veic valsts pārvaldes uzdevumus, ja tie sniedz pienācīgas finansiālās garantijas;

☐ struktūrām, kuru darbību reglamentē dalībvalsts privāttiesības, kurām ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuras sniedz pienācīgas finansiālās garantijas;

☐ personām, kurām ir uzticēts veikt īpašas darbības KĀDP ietvaros saskaņā ar Līguma par Eiropas Savienību V sadaļu un kuras ir noteiktas attiecīgā pamataktā.

Piezīmes

Regula skartās jomas: - ierosinātās regulas II sadaļā ir pārskatītas Eiropas Savienības Tīklu un informācijas drošības aģentūras (*ENISA*) pilnvaras, tai piešķirot būtisku lomu attiecībā uz sertifikāciju, - savukārt III sadaļā ir izveidots satvars IKT produktu un pakalpojumu Eiropas kiberdrošības sertifikācijas shēmu izveidei, saistībā ar ko *ENISA* ir svarīga nozīme.

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

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

Norādīt periodiskumu un nosacījumus.

Uzraudzība sāksies uzreiz pēc tiesību akta pieņemšanas, un galvenā uzmanība tiks pievērsta tā piemērošanai. Komisija organizēs sanāksmes ar *ENISA*, dalībvalstu pārstāvjiem (piemēram, ekspertu grupu) un attiecīgajām ieinteresētajām personām, jo īpaši, lai veicinātu ar sertificēšanu saistīto noteikumu īstenošanu, piemēram, par Administratīvās padomes izveidi.

Ja vien ir pieejami pietiekami dati, pirmais izvērtējums būtu jāveic piecus gadus pēc tiesību akta stāšanās spēkā. Tiesību aktā ir iekļauts arī skaidri formulēts noteikums par izvērtēšanu un pārskatīšanu [XXX. pants], kuru Komisija izmantos neatkarīgā izvērtēšanā. Pēc tam Komisija par izvērtējumu ziņos Eiropas Parlamentam un Padomei, vajadzības gadījumā pievienojot priekšlikumu to pārskatīt, kas ļautu noteikt, cik liela ir regulas ietekme un pievienotā vērtība. Tālāk izvērtēšana būtu jāveic ik pēc pieciem gadiem. Izvērtējumā tiks izmantota Komisijas labāka regulējuma metodika. Šajā izvērtēšanā tiks izmantotas mērķtiecīgas diskusijas ar ekspertiem, pētījumi un plaša apspriešanās ar ieinteresētajām personām.

Ik pēc diviem gadiem aģentūras *ENISA* izpilddirektors iesniedz Administratīvajai padomei *ex-post ENISA* darbības izvērtējumu. Aģentūrai arī būtu jāizstrādā turpmākas rīcības plāns atbilstīgi retrospektīvu izvērtējumu secinājumiem un divreiz gadā jāziņo Komisijai par panākumiem. Administratīvajai padomei vajadzētu būt pienākumam rūpīgi uzraudzīt, lai pēc šādiem secinājumiem tiek veikti pienācīgi pasākumi.

Ja ir aizdomas par administratīvām kļūdām Aģentūras darbībā, izmeklēšanu saskaņā ar Līguma 228. pantu var veikt Eiropas Ombuds.

Plānotās uzraudzības datu avoti galvenokārt būtu *ENISA*, Eiropas Kiberdrošības sertifikācijas grupa, Sadarbības grupa, *CSIRT* tīkls un dalībvalstu iestādes. Papildus *ENISA*, Eiropas Kiberdrošības sertifikācijas grupas, Sadarbības grupas, *CSIRT* tīkla ziņojumos (arī *ENISA* gada darbības pārskatos) sniegtajiem datiem vajadzības gadījumā tiks izmantoti īpaši datu vākšanas instrumenti (piemēram, *Eurobarometer*, valsts iestāžu apsekojumi un kiberdrošības mēneša kampaņas un Eiropas mēroga mācību ietvaros sagatavotie pārskati).

2.2. Pārvaldības un kontroles sistēma

2.2.1. Apzinātie riski

Apzinātie riski skar tikai dažas jomas – Savienības aģentūra jau ir izveidota un tās pilnvaras tiek stingri noteiktas, nostiprinot jomas, kurās Aģentūra ir apliecinājusi nepārprotamu pievienoto vērtību, un pievienojot jaunas jomas, kurās atbalsts jāsniedz atbilstīgi jaunajām politiskajām prioritātēm un instrumentiem, sevišķi TID direktīvai, pārskatītajai ES kiberdrošības stratēģijai, ES kiberdrošības plānam sadarbībai kiberkrīžu jomā un IKT drošības sertifikācijai.

Tāpēc priekšlikumā detalizēti izklāstītas Aģentūras funkcijas un parādīti ieguvumi efektivitātes ziņā. Darbības kompetenču un uzdevumu pieaugums nerada risku, jo ar tām tiktu papildināta dalībvalstu rīcība un pēc pieprasījuma attiecībā uz dažiem un iepriekš noteiktiem pakalpojumiem atbalstītas pašas dalībvalstis.

Turklāt Aģentūras ierosinātais modelis saskaņā ar kopīgo pieeju garantē, ka tiek nodrošināta pietiekama kontrole, kas nodrošinātu *ENISA* darbības atbilstību tās mērķiem. Ierosināto izmaiņu radītie funkcionālie un finansiālie riski, šķiet, ir ierobežoti.

Tajā pašā laikā ir jānodrošina pienācīgi finansiālie līdzekļi, lai *ENISA* pildītu uzdevumus, kas tai uzticēti līdz ar jaunajām pilnvarām, tostarp sertifikācijas jomā.

2.2.2. Paredzētās kontroles metodes

Aģentūras pārskati tiks iesniegti Revīzijas palātai apstiprināšanai, un attiecībā uz tiem paredzēts veikt budžeta izpildes apstiprinājuma procedūru un revīzijas.

Turklāt Aģentūras darbības saskaņā ar Līguma 228. panta noteikumiem pārrauga Ombuds.

Skatīt arī 2.1. punktu un 2.2.1. punktu.

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus.

Aģentūras *ENISA* novēršanas pasākumi un citi pretpasākumi tiktu piemēroti šādos gadījumos:

- Maksājumus par visiem pieprasītajiem pakalpojumiem vai pētījumiem pirms apmaksas pārbauda Aģentūras personāls, ņemot vērā visas līgumsaistības, ekonomikas principus un finanšu vai vadības paraugpraksi. Krāpšanas apkarošanas noteikumus (pārraudzība, prasības par ziņošanu u. c.) iekļaus visos nolīgumos un līgumos, ko noslēdz starp Aģentūru un maksājumu saņēmējiem.

- Lai apkarotu krāpšanu, korupciju un citas nelikumīgas darbības, bez ierobežojumiem piemēro noteikumus, kas paredzēti Eiropas Parlamenta un Padomes 2013. gada 11. maija Regulā (ES) Nr. 883/2013 par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*).

- Sešu mēnešu laikā pēc šīs regulas stāšanās spēkā Aģentūra pievienojas Eiropas Parlamenta, Eiropas Savienības Padomes un Eiropas Kopienu Komisijas 1999. gada 25. maija Iestāžu nolīgumam par iekšējo izmeklēšanu, ko veic Eiropas birojs krāpšanas apkarošanai *OLAF*), un nekavējoties sagatavo attiecīgus noteikumus, kas piemērojami visiem Aģentūras darbiniekiem.

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

- Esošās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
		Dif./nedif.[52].	no EBTA valstīm[53]	no kandidātvalstīm[54]	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē
1.a Konkurētspēja izaugsmei un nodarbinātībai	09 02 03 *ENISA* un informācijas un komunikācijas tehnoloģiju drošības sertifikācija	Dif.	JĀ	NĒ	NĒ	NĒ
5 Administratīvie izdevumi	09 01 01 Izdevumi, kas saistīti ar aktīvā nodarbinātībā iesaistītiem darbiniekiem politikas jomā "Komunikācijas tīkli, saturs un tehnoloģija" 09 01 02 Izdevumi, kas saistīti ar aktīvā nodarbinātībā iesaistītiem ārštata darbiniekiem	Nedif.	NĒ	NĒ	NĒ	NĒ

[52] Dif. – diferencētās apropriācijas, nedif. – nediferencētās apropriācijas.
[53] EBTA – Eiropas Brīvās tirdzniecības asociācija.
[54] Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

	politikas jomā "Komunikācijas tīkli, saturs un tehnoloģija" 09 01 02 11 Citi pārvaldības izdevumi					

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

EUR miljonos (trīs zīmes aiz komata)

Daudzgadu finanšu shēmas izdevumu kategorija	1.a	Konkurētspēja izaugsmei un nodarbinātībai

ENISA			**Bāzes gads 2017 (31/12/2016)**		**2019** ***(no 01.07.2019.)***	**2020**	**2021**	**2022**	**KOPĀ**
1. sadaļa: Personāla izdevumi *(tostarp izdevumi saistībā ar darbinieku pieņemšanu darbā, apmācību, sociāli medicīnisko infrastruktūru un ārējie pakalpojumi)*	Saistības	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Maksājumi	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
2. sadaļa: Infrastruktūras un darbības izdevumi	Saistības	1.a	1,770		1,957	2,232	2,461	2,565	**9,215**
	Maksājumi	(2.a)	1,770		1,957	2,232	2,461	2,565	**9,215**
3. sadaļa: Darbības izdevumi	Saistības	(3.a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Maksājumi	(3.b)	3,086		4,694	6,332	6,438	6,564	**24,028**
KOPĀ apropriācijas *ENISA*	Saistības	=1+1.a +3.a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Maksājumi	=2+2.a	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

		+3.b							

Daudzgadu finanšu shēmas izdevumu kategorija	**5**	"Administratīvie izdevumi"

EUR miljonos (trīs zīmes aiz komata)

		2019 *(no 01.07.2019.)*	**2020**	**2021**	**2022**	**KOPĀ**
CNECT ĢD						
• Cilvēkresursi		0,216	0,846	0,846	0,846	**2,754**
• Pārējie administratīvie izdevumi		0,102	0,235	0,238	0,242	**0,817**
KOPĀ CNECT ĢD	Apropriācijas	0,318	1,081	1,084	1,088	**3,571**

Darbinieku izmaksas tika aprēķinātas saskaņā ar plānoto darbā pieņemšanas datumu (nodarbinātība ir plānota no 01.07.2019.).

Resursu perspektīvais plānojums laikposmam pēc 2020. gada ir indikatīvs un neskar Komisijas priekšlikumus par daudzgadu finanšu shēmu laikposmam pēc 2020. gada.

KOPĀ daudzgadu finanšu shēmas **5. IZDEVUMU KATEGORIJAS apropriācijas**	(Saistību summa = maksājumu summa)	0,318	1,081	1,084	1,088	**3,571**

EUR miljonos (trīs zīmes aiz komata)

		2019	2020	2021	2022	KOPĀ
KOPĀ daudzgadu finanšu shēmas **1.–5. IZDEVUMU KATEGORIJAS apropriācijas**	Saistības	16,868	21,727	23,332	24,11	**86,038**
	Maksājumi	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Paredzamā ietekme uz Aģentūras apropriācijām

– ☐Priekšlikums/iniciatīva neparedz izmantot darbības apropriācijas

– ☒Priekšlikums/iniciatīva paredz izmantot darbības apropriācijas šādā veidā:

Saistību apropriācijas EUR miljonos (trīs zīmes aiz komata)

Norādīt mērķus un rezultātus[55] ⇩	**2019**	**2020**	**2021**	**2022**	**KOPĀ**
Pastiprināt dalībvalstu un uzņēmumu spējas un gatavību	1,408	1,900	1,931	1,969	7,208
Uzlabot sadarbību un koordināciju starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām	0,939	1,266	1,288	1,313	4,806
Uzlabot ES līmeņa spējas, lai papildinātu dalībvalstu rīcību, it īpaši pārrobežu kiberkrīžu gadījumā	0,704	0,950	0,965	0,985	3,604
Uzlabot iedzīvotāju un uzņēmumu izpratni kiberdrošības jautājumos	0,704	0,950	0,965	0,985	3,604
Vairot uzticēšanos digitālajam vienotajam tirgum un digitālajai inovācijai, uzlabojot IKT produktu un pakalpojumu kiberdrošības apliecinājuma vispārējo pārredzamību	0,939	1,266	1,288	1,313	4,806
KOPĒJĀS IZMAKSAS	4,694	6,332	6,437	6,565	24,028

[55] * Šajā tabulā parādīti tikai darbības izdevumi 3. sadaļā.

3.2.3. Paredzamā ietekme uz Aģentūras cilvēkresursiem

3.2.3.1. Kopsavilkums

– ☐Priekšlikums/iniciatīva neparedz izmantot administratīvās apropriācijas

– ☒Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādā veidā:

EUR miljonos (trīs zīmes aiz komata)

	2019 (3./4. cet.)	**2020**	**2021**	**2022**
Pagaidu darbinieki (AD kategorija)	4,242	5,695	6,381	6,709
Pagaidu darbinieki (AST kategorija)	1,601	1,998	2,217	2,217
Līgumdarbinieki	2,041	2,041	2,041	2,041
Valstu norīkotie eksperti	0,306	0,447	0,656	0,796
KOPĀ	**8,190**	**10,181**	**11,295**	**11,763**

Darbinieku izmaksas tika aprēķinātas saskaņā ar plānoto darbā pieņemšanas datumu (pašreizējo *ENISA* darbinieku pilnīga nodarbinātība ir plānota no 01.01.2019.). Jauno darbinieku pakāpeniska pieņemšana darbā bija paredzēta no 01.07.2019., pilnīgu nodarbinātību sasniedzot 2022. gadā. Resursu perspektīvais plānojums laikposmam pēc 2020. gada ir indikatīvs un neskar Komisijas priekšlikumus par daudzgadu finanšu shēmu laikposmam pēc 2020. gada.

Paredzamā ietekme uz darbiniekiem (papildu *FTE*) – štatu saraksts

Funkciju grupa un pakāpe	2017 **Pašreiz *ENISA***	2019 (3./4. cet.)	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
AD kopā	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST kopā	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
AST/SC kopā					
PAVISAM KOPĀ	48	12	10	7	3

Uzdevumi papildu AD/AST darbiniekiem, lai sasniegtu tiesību akta mērķus, kas aprakstīti 1.4.2. punktā:

Uzdevumi	AD	AST	*SNE*	Kopā
Politikas un spēju veidošana	8	1		9
Operatīvā sadarbība	8	1	7	16
Sertifikācija (ar tirgu saistīti uzdevumi)	9	3	2	14
Zināšanas, informācija un izpratne	1	1		2
KOPĀ	26	6	9	41

Veicamo uzdevumu apraksts

Uzdevumi	**Vajadzīgie papildu resursi**
ES politikas izstrāde un īstenošana un spēju veidošana	Uzdevumi ietvertu palīdzēšanu Sadarbības grupai, konsekventu atbalsta sniegšanu TID īstenošanai pāri robežām, regulāru ziņošanu par ES tiesiskā regulējuma īstenošanu; padomu došanu un nozaru kiberdrošības iniciatīvu koordinēšanu, tostarp enerģētikas, transporta (piem., aviācijas /autotransporta / jūras satiksmes / satīkloto transportlīdzekļu), veselības aprūpes un finanšu jomā, atbalsta sniegšanu informācijas apmaiņas un analīzes centru (*ISAC*) izveidei dažādās nozarēs.

Operatīvā sadarbība un krīžu pārvarēšana	**Tajā ietilpst šādi uzdevumi:** Nodrošināt *CSIRT* tīkla sekretariātu, cita starpā nodrošinot *CSIRT* tīkla IT infrastruktūru un saziņas kanālu pienācīgu darbošanos. Nodrošināt strukturētu sadarbību ar *CERT-EU*, *EC3* un citām attiecīgajām ES struktūrām. Organizēt **mācības *Cyber Europe***[56] – uzdevumi, kas saistīti ar mācību pārorientēšanu no pasākuma, kas notiek reizi divos gados, uz ikgadēju pasākumu un ar tādu mācību izveidi, kurās incidents tiek aplūkots pilnībā, proti, no sākuma līdz beigām. **Tehniskā palīdzība** – uzdevumi ietvertu strukturētu sadarbību ar *CERT-EU*, kuras ietvaros tiktu sniegta tehniska palīdzība nopietnu incidentu gadījumā un atbalsts incidentu analīzes veikšanā. Šajā sakarībā dalībvalstīm arī varētu sniegt palīdzību incidentu novēršanā un vājo vietu, artefaktu un incidentu analīzē. Veicināt sadarbību starp atsevišķām dalībvalstīm, kuras reaģē ārkārtas situācijās, – analizēt un apkopot valstu ziņojumus par situāciju, balstoties uz Aģentūrai piegādāto informāciju no dalībvalstīm un citiem subjektiem. **"Plāns, kā koordinēti reaģēt uz plašapmēra pārrobežu kiberdrošības incidentiem"** – Aģentūra palīdzēs sagatavoties uz sadarbību balstītai reaģēšanai gan Savienības, gan dalībvalstu līmenī ar kiberdrošību saistītu liela mēroga pārrobežu incidentu vai krīžu gadījumos, izmantojot virkni uzdevumu, no palīdzības saistībā ar situācijas apzināšanos Savienības līmenī līdz incidentu gadījumā izmantojamu sadarbības plānu testēšanai. ***Ex-post* tehniskā izmeklēšana par incidentiem** – sadarbībā ar *CSIRT* tīklu veikt vai veicināt *ex-post* tehnisko izmeklēšanu par incidentiem, ar mērķi, sagatavojot publiskos ziņojumus, sniegt ieteikumus un stiprināt spējas, lai labāk novērstu turpmākus incidentus.

[56] "*Cyber Europe*" ir Eiropā lielākās un visaptverošās ES kiberdrošības mācības, kurās līdz šim piedalījušies vairāk nekā 700 kiberdrošības speciālistu no visām 28 dalībvalstīm. Tās notiek reizi divos gados. *ENISA* izvērtējumā un 2013. gada ES kiberdrošības stratēģijā norādīts, ka, ņemot vērā kiberdraudu strauji mainīgo raksturu, daudzas ieinteresētās personas atbalsta "*Cyber Europe*" pārveidošanu par ikgadēju pasākumu. Tomēr patlaban tas nav iespējams, jo Aģentūras resursi ir ierobežoti.

Ar tirgu saistīti uzdevumi (standartizācija, sertifikācija)	Veicot šos izdevumus, cita starpā būtu aktīvi jāatbalsta sertifikācijas satvarā veiktais darbs, arī jādalās tehniskajā lietpratībā, kas nepieciešama Eiropas kiberdrošības sertifikācijas kandidātshēmu izveidē. Uzdevumos ietilps Savienības politikas izstrādes un īstenošanas atbalsts saistībā ar standartizāciju, sertifikāciju un tirgus novērošanas centru – šajā saistībā jāsekmē elektronisko produktu, sistēmu, tīklu un pakalpojumu riska pārvaldības standartu ieviešana un jāsniedz padomi par tehniskās drošības prasībām pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem. Uzdevumi ietvers arī kiberdrošības tirgus aktuālāko tendenču analīzi.
Zināšanas un informācija, izpratnes uzlabošana	Lai nodrošinātu vienkāršāku piekļuvi labāk strukturētai informācijai par kiberdrošības riskiem un iespējamiem rīkiem to likvidēšanai, priekšlikumā paredzēts jauns uzdevums Aģentūrai, proti, izveidot un uzturēt Savienības "informācijas mezglu". Veicot šos uzdevumus, cita starpā būtu jāapkopo, jākārto un īpaši izveidotā portālā jāpublisko ES iestāžu, aģentūru un struktūru sniegtā informācija par tīklu un informācijas sistēmu drošību, jo īpaši kiberdrošību. Uzdevumi ietvertu arī tādu *ENISA* pasākumu atbalstīšanu, kuru nolūks ir panākt labāku izpratni, kas ļautu Aģentūrai pastiprināt savus centienus.

3.2.3.2. Paredzamās iesaistītā ĢD vajadzības pēc cilvēkresursiem

– ☐ Priekšlikums/iniciatīva neparedz cilvēkresursu izmantošanu

– ☒ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Aplēse izsakāma veselos skaitļos (vai maksimāli ar vienu zīmi aiz komata)

		Papildu darbinieki			
	Bāzes gads / 2017	3./4. cet. 2019	2020	2021	2020
• **Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)**					
09 01 01 01 (Galvenā mītne un Komisijas pārstāvniecības)	1	2	3		
• **Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu *FTE*)**[57]					
09 01 02 01 (*CA*, *SNE*, *INT*, ko finansē no vispārīgajām apropriācijām)	1	2			
KOPĀ		**4**	**3**		

Veicamo uzdevumu apraksts

Ierēdņi un pagaidu darbinieki	Pārstāvēt Komisiju Aģentūras Administratīvajā padomē. Sagatavot Komisijas atzinumu par *ENISA* vienoto programmdokumentu un uzraudzīt tā īstenošanu. Pārraudzīt Aģentūras budžeta sagatavošanu un uzraudzīt tā izpildi. Palīdzēt Aģentūrai izstrādāt tās pasākumus saskaņā ar Savienības politiku, tostarp piedaloties attiecīgajās sanāksmēs. Pārraudzīt IKT produktu un pakalpojumu Eiropas kiberdrošības sertifikācijas shēmu satvara īstenošanu. Uzturēt kontaktus ar dalībvalstīm un citām ieinteresētajām personām attiecībā uz centieniem ieviest sertifikāciju. Sadarboties ar *ENISA* attiecībā uz kandidātshēmām. Sagatavot Eiropas kiberdrošības kandidātshēmas.
Ārštata darbinieki	Iepriekš norādītie

[57] *CA* – līgumdarbinieki, *LA* – vietējie darbinieki, *SNE* – valstu norīkotie eksperti, *INT* – aģentūras darbinieki, *JED* – jaunākie eksperti delegācijās.

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

– ☐ Priekšlikums/iniciatīva atbilst kārtējai daudzgadu finanšu shēmai

– ☒ Pieņemot priekšlikumu/iniciatīvu, jāpārplāno attiecīgā izdevumu kategorija daudzgadu finanšu shēmā

Pieņemot priekšlikumu, jāpārplāno 09 02 03. pants, jo tiek pārskatītas *ENISA* pilnvaras, kas piešķir Aģentūrai jaunus uzdevumus, kuri cita starpā ir saistīti ar TID direktīvas īstenošanu un Eiropas kiberdrošības sertifikācijas satvaru. Attiecīgās summas:

Gads	Paredzēts	Pieprasīts
2019	10,739	16,550
2020	10,954	20,646
2021	Neattiecas	22,248*
2022	Neattiecas	23,023*

* Aplēses. ES finansējums laikposmam pēc 2020. gada tiks izvērtēs, ņemot vērā Komisijas debates par visiem priekšlikumiem, kuri attiecas uz laikposmu pēc 2020. gada. Tas nozīmē, ka tad, kad Komisija ir iesniegusi priekšlikumu nākamajai daudzgadu finanšu shēmai, Komisija iesniegs grozītu tiesību akta finanšu pārskatu, ņemot vērā ietekmes novērtējuma secinājumus[58].

– ☐ Pieņemot priekšlikumu/iniciatīvu, jāpiemēro elastības instruments vai jāpārskata daudzgadu finanšu shēma[59]

3.2.5. Trešo personu iemaksas

– ☐ Priekšlikums/iniciatīva neparedz trešo personu līdzfinansējumu

– ☒ Priekšlikums/iniciatīva paredz šādu līdzfinansējumu:

	Gads **2019**	Gads **2020**	Gads **2021**	Gads **2022**
EBTA	*p.m*[60].	*p.m.*	*p.m.*	*p.m.*

3.3. Paredzamā ietekme uz ieņēmumiem

– ☒ Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus

– ☐ Priekšlikums/iniciatīva finansiāli ietekmē:

58 Saite uz lapu, kurā publicēts ietekmes novērtējums.

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

60 Precīza summa turpmākajiem gadiem būs zināma, kad attiecīgajam gadam tiks noteikts EBTA proporcionalitātes koeficients.

– ☐ pašu resursus

– ☐ dažādus ieņēmumus