Eiropas Savienības
Padome

**Briselē, 2022. gada 22. martā**
**(OR. en)**

**7474/22**

**Starpiestāžu lieta:**
**2022/0085(COD)**

**CYBER 93**
**TELECOM 116**
**JAI 383**
**INST 89**
**INF 32**
**CSC 119**
**CSCI 39**
**DATAPROTECT 81**
**FIN 353**
**BUDGET 2**
**CODEC 349**
**IA 30**

**PRIEKŠLIKUMS**

| | |
|---|---|
| Sūtītājs: | Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ* |
| Saņemšanas datums: | 2022. gada 22. marts |
| Saņēmējs: | Eiropas Savienības Padomes ģenerālsekretārs *Jeppe TRANHOLM-MIKKELSEN* |
| K-jas dok. Nr.: | COM(2022) 122 final |
| Temats: | Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās |

Pielikumā ir pievienots dokuments COM(2022) 122 *final*.

Pielikumā: COM(2022) 122 *final*

EIROPAS
KOMISIJA

Briselē, 22.3.2022.
COM(2022) 122 final

2022/0085 (COD)

Priekšlikums

**EIROPAS PARLAMENTA UN PADOMES REGULA,**

**ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās**

{SWD(2022) 67 final} - {SWD(2022) 68 final}

# PASKAIDROJUMA RAKSTS

## 1. PRIEKŠLIKUMA KONTEKSTS

### • Priekšlikuma pamatojums un mērķi

Ar šo priekšlikumu nosaka regulējumu vienotu kiberdrošības noteikumu un Savienības iestāžu, struktūru un aģentūru noteikumu panākšanai. Tā mērķis ir vēl vairāk uzlabot visu struktūru noturību un spēju reaģēt uz incidentiem. Tas atbilst Komisijas prioritātēm darīt Eiropu gatavu digitālajam laikmetam un veidot nākotnei atbilstošu ekonomiku, kas darbojas iedzīvotāju labā. Turklāt drošas un noturīgas publiskās pārvaldes panākšana ir visas sabiedrības digitālās pārveides pamatā.

Šā priekšlikuma pamatā ir ES Drošības savienības stratēģija (COM(2020) 605 final) un ES kiberdrošības stratēģija digitālajai desmitgadei (JOIN(2020) 18 final).

Ar šo priekšlikumu paredzēts modernizēt esošo *CERT-EU* tiesisko regulējumu un ņemt vērā pēdējo gadu laikā mainījušos un plašāko iestāžu, struktūru un aģentūru digitalizāciju, kā arī pieaugošos kiberdrošības apdraudējumus. Abus šos virzienus vēl vairāk pastiprināja Covid-19 krīze, turklāt incidentu skaits turpina palielināties un daudzi un dažādi avoti īsteno aizvien sarežģītākus uzbrukumus.

Ar šo priekšlikumu *CERT-EU* no datorapdraudējumu reaģēšanas vienības pārdēvē par Savienības iestāžu, struktūru un aģentūru kiberdrošības centru; tas notiek saskaņā ar norisēm dalībvalstīs un pasaulē, kur daudzas *CERT* pārdēvē par kiberdrošības centriem, taču nosaukuma atpazīstamības dēļ tiek saglabāts īsais nosaukums *CERT-EU*.

### • Saskanība ar pašreizējiem noteikumiem konkrētajā politikas jomā

Šā priekšlikuma mērķis ir palielināt Savienības iestāžu, struktūru un aģentūru kiberdrošības noturību pret kiberdraudiem, vienlaikus panākot salāgošanu ar esošajiem tiesību aktiem:

- Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. Tas arī atbilst priekšlikumam Direktīvai (ES) XXXX/XXXX, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148 [TID 2 priekšlikums];
- Regulu (ES) 2019/881 par Eiropas Savienības Kiberdrošības aģentūru un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju (Kiberdrošības aktu);
- priekšlikumu Regulai (ES) XXXX/XXXX par Savienības iestāžu, struktūru, biroju un aģentūru informācijas drošību;
- Komisijas 2021. gada 23. jūnija Ieteikumu par Kopējās kibervienības izveidošanu;
- Komisijas 2017. gada 13. septembra Ieteikumu (ES) 2017/1584 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm.

Pielikumā Komisijas 2017. gada 13. septembra Ieteikumam (ES) 2017/1584 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm ir izklāstīts plāns, kā koordinēti reaģēt uz plašapmēra pārrobežu kiberdrošības incidentiem un krīzēm.

Savā 2021. gada 9. marta rezolūcijā Eiropas Savienības Padome uzsvēra, ka kiberdrošība ir ļoti svarīga publiskās pārvaldes darbībai gan valsts, gan ES līmenī, kā arī sabiedrībai un ekonomikai kopumā, norādot uz noturīga un konsekventa drošības satvara nozīmi ES personāla, datu, sakaru tīklu, informācijas sistēmu un lēmumu pieņemšanas procesu

aizsardzībā. Jo īpaši tas jāpanāk, izmantojot labāku noturību un drošības kultūru Savienības iestādēs, struktūrās un aģentūrās. Jānodrošina pietiekami resursi un spējas, kas attiecas arī uz *CERT-EU* pilnvaru pastiprināšanu.

## 2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

- **Juridiskais pamats**

Šīs regulas juridiskais pamats ir Līguma par Eiropas Savienības darbību (LESD) 298. pants, kur paredzēts, ka, veicot uzdevumus, Savienības iestādes, struktūras, biroji un aģentūras saņem atvērtas, efektīvas un neatkarīgas Eiropas administrācijas atbalstu. Ievērojot Civildienesta noteikumus un nodarbināšanas kārtību, kas pieņemti, pamatojoties uz 336. pantu, Eiropas Parlaments un Padome, pieņemot regulas saskaņā ar parasto likumdošanas procedūru, šajā nolūkā paredz noteikumus.

Informācijas tehnoloģijas Savienības iestādēm, struktūrām un aģentūrām ir sniegušas jaunus veidus, kā strādāt, sazināties ar iedzīvotājiem un uzlabot vispārējo darbību. Tehnoloģiju attīstība turpinās, un līdz ar tām attīstās arī kiberdraudi. Savienības iestādes, struktūras un aģentūras ir kļuvušas par ārkārtīgi pievilcīgiem sarežģītu kiberuzbrukumu mērķiem. Kiberdrošības nodrošināšanas sistēmu un prasību ieviešana, šķiet, sekmē Eiropas administrācijas efektivitāti un neatkarību, lai Savienības iestādes, struktūras, biroji un aģentūras digitālā pasaulē uzdevumus varētu veikt efektīvāk.

Turklāt, kā skaidrots 3. iedaļā iepriekš, pašreizējās atšķirības Savienības iestāžu, struktūru un aģentūru kiberdrošības situācijā un pieejā šajā jomā rada papildu šķēršļus atvērtai, efektīvai un neatkarīgai Eiropas administrācijai. Ja nav kopējas pieejas, Savienības iestāžu, struktūru un aģentūru uzskats par kiberdrošības jautājumiem turpina attīstīties dažādos virzienos. Tādējādi šis juridiskais pamats ir atbilstošs, jo regulas mērķis ir izveidot vienotu kiberdrošības tiesisko regulējumu Savienības iestādēs, struktūrās, birojos un aģentūrās.

- **Subsidiaritāte**

Tomēr regula, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās, ir Savienības ekskluzīvās kompetences jomā.

- **Proporcionalitāte**

Šajā regulā rosinātie noteikumi nav plašāki, kā nepieciešams, lai apmierinoši izpildītu konkrētos mērķus. Paredzētie pasākumi sekmēs vienādi augsta līmeņa kiberdrošības panākšanu, bet nebūs plašāki, kā nepieciešams, lai sasniegtu mērķi, ņemot vērā aizvien lielākos riskus, ar ko saskaras iestādes.

- **Juridiskā instrumenta izvēle**

Tieši piemērojama regula uzskatāma par atbilstošo juridisko instrumentu, kas definēs un racionalizēs Savienības iestādēm, struktūrām un aģentūrām piemērotos pienākumus. Lai būtu iespējams veikt mērķorientētus uzlabojumus, regula ir visatbilstošākais juridiskais instruments.

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

- ***Ex ante* izvērtējumi**

*CERT-EU* ir veikusi to galveno kiberdraudu novērtējumu, kam pašlaik pakļautas vai kam paredzamā nākotnē varētu tikt pakļautas Savienības iestādes, struktūras un aģentūras.

Analīzē izmantoja trīs novērojumu kategorijas:

- mēģinājumi ielauzties Savienības iestāžu, struktūru un aģentūru IT infrastruktūrā (ja tie izdodas, šādus gadījumus uzskata par incidentiem, citos gadījumos tie tāpat tiek reģistrēti kā atklāti mēģinājumi);
- Savienības iestāžu, struktūru un aģentūru tuvumā konstatēti apdraudējumi (piem., ar tām saistītās nozarēs, to ieinteresēto personu kopienās vai Eiropā);
- pasaulē novērotas būtisko apdraudējumu tendences.

Analīzē tika arī apskatīts, kā galvenās notiekošās izmaiņas ietekmē veidus, kā Savienības iestādes pārvalda un izmanto savu IT infrastruktūru un pakalpojumus. Šādas izmaiņas ir:

- tāldarba popularitātes palielināšanās;
- sistēmu migrēšana uz mākoni;
- plašāka IT ārpakalpojumu izmantošana.

Laikā no 2019. līdz 2021. gadam tādu būtisku incidentu[1] skaits, kas skāruši Savienības iestādes, struktūras un aģentūras un ko radījuši paaugstināta pastāvīga apdraudējuma (*advanced persistent threat — APT*) izraisītāji, ir būtiski palielinājies. 2021. gada pirmajā pusē bija tikpat daudz būtisku incidentu kā visā 2020. gadā. To atspoguļo arī kriminālanalīžu (skarto sistēmu vai ierīču satura momentuzņēmumi) skaits, ko *CERT-EU* veica 2020. gadā un kas trīskāršojās salīdzinājumā ar 2019. gadu, un kopš 2018. gada būtisko incidentu skaits ir palielinājies par vairāk nekā desmit reizēm.

2020. gadā *CERT-EU* koordinācijas padome *CERT-EU* noteica jaunu stratēģisku mērķi ar atbilstošu plašumu un dziļumu, lai garantētu visaptverošu kiberaizsardzības līmeni visām iestādēm, struktūrām un aģentūrām, kā arī pastāvīgu pielāgošanos esošajiem vai nākotnes apdraudējumiem, kas ietver uzbrukumus mobilajām ierīcēm, mākoņvidei un lietu interneta ierīcēm.

Papildus *CERT-EU* apdraudējumu analīzei Komisija ir veikusi 20 Savienības iestāžu, struktūru un aģentūru kiberdrošības sistēmu darbības izvērtējumu. Tas deva ieskatu esošajā kiberdrošības praksē un kiberdrošības pārvaldības spējās, izmantojot dažu tehnisku drošības kontroles pasākumu ārējo salīdzinošo vērtēšanu.

Šis izvērtējums bija balstīts uz anketām, kurās atbildes sniedza šīs iestādes, struktūras un aģentūras, publiski pieejamiem datiem un Savienības iestāžu, struktūru un aģentūru tieši sniegtiem datiem. Tas dod pietiekamu ieskatu esošajā situācijā, lai secinātu tālāk norādīto:

- kiberdrošības gatavības pakāpe, IT infrastruktūras lielums un spēju līmenis izvērtētajās Savienības iestādēs, struktūrās un aģentūrās ir ļoti dažāds;
- lai gan kopumā Savienības iestāžu, struktūru un aģentūru ir atklāšanas un reaģēšanas spējas ir labā gatavībā, to kiberdrošības pārvaldības spējās ir atšķirīgs integrētās riska pārvaldības līmenis;
- lai gan kopējais kiberdrošības satvars (stratēģija, politika un noteikumu bāze) izvērtētajās Savienības iestādēs, struktūrās un aģentūrās ir labi iesakņojies galvenajās kiberdrošības jomās, kas uzskaitītas regulas I pielikumā, dažu Savienības iestāžu,

[1] Būtisks incidents ir jebkāds incidents, ja vien tam nav ierobežota ietekme un, visticamāk, to jau labi izprot attiecībā uz metodi vai tehnoloģiju.

struktūru un aģentūru darbības nepārtrauktības pārvaldības, atbilstības nodrošināšanas, revīzijas un pastāvīgu uzlabojumu spējas nav pietiekami attīstītas;

- tika konstatēts, ka tehniski pasākumi, kas uzskatāmi par paraugpraksi, novērtētajās Savienības iestādēs, struktūrās un aģentūrās netiek piemēroti vienmērīgi.

Kopumā 20 Savienības iestāžu, struktūru un aģentūru analīzes rezultāti liecina, ka to pārvaldība, kiberhigiēna, vispārējās spējas un gatavības līmenis ir izteikti nehomogēni. Tāpēc visām Savienības iestādēm, struktūrām un aģentūrām ir jāīsteno kiberdrošības pamatpasākumi, kas ir ļoti svarīgi, lai novērstu šo gatavības līmeņu atšķirību un lai visās Savienības iestādēs, struktūrās un aģentūrās panāktu vienādi augsta līmeņa kiberdrošību.

Savienības tiesību akti līdz šim ir bijuši vērsti uz Savienības iestāžu, struktūru un aģentūru kiberdrošību un visaptveroši pievērsušies kiberdrošības apdraudējumiem un jaunajiem digitalizācijas sekmētajiem IT riskiem.

- **Apspriešanās ar ieinteresētajām personām**

Komisija ir apspriedusies ar ieinteresētajām personām Savienības iestādēs, struktūrās un aģentūrās, kā arī ar dalībvalstu pārstāvjiem Padomē un Eiropas Parlamenta ieinteresētajām personām. 2021. gada 25. jūnijā dalībvalstu pārstāvji un attiecīgās ieinteresētās personas no Savienības iestādēm, struktūrām un aģentūrām piedalījās darbseminārā, ko organizēja Komisija, lai apspriestu topošā regulas priekšlikuma saturu.

- **Ietekmes novērtējums**

Šis priekšlikums ietekmēs Savienības iestādes, struktūras un aģentūras. Tādējādi īpašs ietekmes novērtējums nav nepieciešams, jo tas neattieksies uz dalībvalstīm.

- **Pamattiesības**

Eiropas Savienība ir apņēmusies panākt augstu pamattiesību aizsardzības standartu ievērošanu. Visa informācijas apmaiņa, kas balstās uz šo regulu, notiks uzticamā vidē, pilnībā ievērojot tiesības uz persondatu aizsardzību, kas paredzētas Eiropas Savienības Pamattiesību hartas 8. pantā, un attiecīgos datu aizsardzības tiesību aktus, jo īpaši Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725.

## 4. IETEKME UZ BUDŽETU

Tirgus standarti un pētījumi[2] liecina, ka tiešie izdevumi par kiberdrošību ir robežās no 4 % līdz 7 % no kopējiem organizāciju IT izdevumiem. Tomēr *CERT-EU* veiktā apdraudējumu analīze šā tiesību akta priekšlikuma atbalstam liecina, ka starptautiskās struktūras un politiskās organizācijas saskaras ar lielākiem riskiem un ka tāpēc 10 % tēriņi par kiberdrošību no kopējiem IT izdevumiem šķistu atbilstošāks mērķrādītājs. Šādu darbību precīzas izmaksas nevar noteikt, jo nav sīkas informācijas par Savienības iestāžu, struktūru un aģentūru IT izdevumiem un attiecīgo ar kiberdrošību saistīto tēriņu daļu.

Lai gan tādējādi ir iespējams, ka daudzas Savienības iestādes, struktūras un aģentūras kiberdrošībai tērē mazāk, nekā vajadzētu, šī regula pati par sevi neradīs minēto kārtējo izdevumu pieaugumu. Pat bez regulas katrai vienībai būtu jānodrošina pienācīgs kiberdrošības

[2] Avots: *Gartner*, "Identifying the Real Information Security Budget" (2016). Tas papildina netiešos izdevumus par IT drošību, piemēram, par tīklu drošību (ugunsmūriem, pretvīrusu programmām utt.) un sistēmas īpašnieka atbildību (riska novērtējums, drošības kontroles īstenošana utt.). 2020. gada dokumentā norādīts, ka finanšu iestāžu tēriņi par kiberdrošību veido 10–11 % no izdevumiem par IT, avots: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

līmenis. Ar regulu turpina iepriekšējo sadarbību *CERT-EU* koordinācijas padomē un formalizē informācijas apmaiņas līmeni, kas daļēji pastāv jau šobrīd. Kā norādīts tiesību akta priekšlikuma finanšu pārskatā, *CERT-EU* plašākās lomas izpildei būs nepieciešami papildu resursi, un šie resursi būtu jāpārdala no Savienības iestādēm, struktūrām un aģentūrām, kas saņem *CERT-EU* pakalpojumus.

## 5. CITI ELEMENTI

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

Iestāžu kiberdrošības padomei (IKP) ar *CERT-EU* palīdzību būtu jāpārskata šīs regulas darbība, jāveic izvērtējumi un Komisijai jāiesniedz ziņojums ar konstatējumiem. Komisijai būtu jānodrošina regulāra ziņošana Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai.

*CERT-EU* var sagatavot norādījumu dokumentu vai ieteikuma projektu, ko IKP var izlemt pieņemt. Norādījumu dokuments ir ieteikuma dokuments visām Savienības iestādēm, struktūrām un aģentūrām vai kādai to grupai, bet ieteikums ir paredzēts atsevišķām Savienības iestādēm, struktūrām un aģentūrām. Aicinājums rīkoties ir *CERT-EU* ieteikuma dokuments, kurā aprakstīti neatliekami drošības pasākumi, kurus Savienības iestādes, struktūras un aģentūras ir aicinātas veikt noteiktā laika posmā.

- **Detalizēts konkrētu priekšlikuma noteikumu skaidrojums**

Vispārīgi noteikumi

Regulā ir noteikti pasākumi, kuru mērķis ir panākt vienādi augsta līmeņa kiberdrošību, un tā ir piemērojama Savienības iestādēm, struktūrām un aģentūrām, lai tās varētu veikt tām uzticētos uzdevumus atvērti, efektīvi un neatkarīgi (1.–3. pants, 23.–25. pants).

Vienādi augsta līmeņa kiberdrošības pasākumi

Savienības iestādēm, struktūrām un aģentūrām ir pienākums izveidot iekšēju kiberdrošības riska pārvaldības, vadības un kontroles sistēmu, kas nodrošina iedarbīgu un piesardzīgu visu kiberdrošības risku pārvaldību. Iestādes, struktūras un aģentūras arī pieņem kiberdrošības pamatparametrus, lai novērstu visus sistēmā konstatētos riskus, veiktu regulārus kiberdrošības gatavības pakāpes novērtējumus un pieņemtu kiberdrošības plānu. (4.–8. pants).

Iestāžu kiberdrošības padome

Izveido Iestāžu kiberdrošības padomi, un tā atbild par šīs regulas īstenošanas uzraudzību Savienības iestādēs, struktūrās un aģentūrās, kā arī *CERT-EU* vispārējo prioritāšu un mērķu īstenošanas uzraudzību un *CERT-EU* stratēģiskā virziena noteikšanu (9.–11. pants).

*CERT-EU*

*CERT-EU* dod ieguldījumu visu Savienības iestāžu, struktūru un aģentūru IT vides drošībā, sniedzot tām padomus, palīdzot novērst, atklāt un mazināt incidentus un reaģēt uz tiem, kā arī rīkojoties kā to kiberdrošības informācijas apmaiņas un reaģēšanas uz incidentiem koordinēšanas centrs. (12.–17. pants).

Sadarbība un ziņošanas pienākumi

Regula nodrošina sadarbību un informācijas apmaiņu starp *CERT-EU* un Savienības iestādēm, struktūrām un aģentūrām, lai veidotu uzticību un pārliecību. Šajā nolūkā *CERT-EU* var prasīt Savienības iestādēm, struktūrām un aģentūrām sniegt būtisku informāciju, un *CERT-EU* var apmainīties ar konkrētu informāciju par incidentiem ar Savienības iestādēm, struktūrām un

aģentūrām, lai sekmētu līdzīgu kiberdraudu vai incidentu atklāšanu bez skartās organizācijas piekrišanas. *CERT-EU* var apmainīties ar konkrētu informāciju par incidentu, kas atklāj kiberdrošības incidenta mērķa identitāti, tikai ar skartās organizācijas piekrišanu.

Visas Savienības iestādes, struktūras un aģentūras bez liekas kavēšanās, bet ne vēlāk kā 24 stundas pēc tam, kad par to uzzinājušas, paziņo *CERT-EU* par būtiskiem kiberdraudiem, būtiskām ievainojamībām un būtiskiem incidentiem. (18.–22. pants).

2022/0085 (COD)

Priekšlikums

**EIROPAS PARLAMENTA UN PADOMES REGULA,**

**ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās**

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 298. pantu,

ņemot vērā Eiropas Atomenerģijas kopienas dibināšanas līgumu un jo īpaši tā 106.a pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Digitālajā laikmetā informācijas un komunikācijas tehnoloģijas ir atvērtas, efektīvas un neatkarīgas Savienības administrācijas stūrakmens. Tehnoloģiju attīstība un digitālo sistēmu lielāka sarežģītība un starpsavienotība palielina kiberdrošības riskus, padarot Savienības administrāciju neaizsargātāku pret kiberdraudiem un incidentiem, un tas beigu beigās apdraud administrācijas darbības nepārtrauktību un spēju aizsargāt savus datus. Plašāka mākoņpakalpojumu izmantošana, IT visās dzīves jomās, augsta digitalizācijas pakāpe, attālinātais darbs un tehnoloģiju un savienojamības attīstība ir kļuvusi par visu Savienības administratīvo vienību darbību pamatiezīmi, tomēr digitālā noturība šajās darbībās vēl nav pietiekami integrēta.

(2) Kiberdraudi, ar ko saskaras Savienības iestādes, struktūras un aģentūras, pastāvīgi attīstās. Apdraudētāju izmantotā taktika, paņēmieni un procedūras pastāvīgi attīstās, bet šādu uzbrukumu galvenie motīvi ir gandrīz nemainīgi — nozagt vērtīgu, neatklātu informāciju, lai pelnītu naudu, manipulēt ar sabiedrības nostāju vai apdraudēt digitālo infrastruktūru. Kiberuzbrukumu biežums palielinās, bet kampaņas kļūst aizvien sarežģītākas un automatizētākas, vēršas pret atklātām, uzbrukumam pieejamām vietām, kuras paplašinās, un ātri izmanto ievainojamības.

(3) Savienības iestāžu, struktūru un aģentūru IT vide ir savstarpēji saistīta, tajā ir integrētas datu plūsmas, un tās lietotāji cieši sadarbojas. Šī starpsavienojamība nozīmē, ka jebkurš traucējums pat tad, ja tas sākotnēji rodas tikai vienā Savienības iestādē, struktūrā vai aģentūrā, var kļūt plašāks, iespējams, radot tālejošas un ilgstošas negatīvas sekas citām iestādēm, struktūrām vai aģentūrām. Turklāt noteiktu iestāžu, struktūru un aģentūru IT vide ir savienota ar dalībvalstu IT vidi, attiecīgi, ja vienā Savienības vienībā notiek incidents, tas rada risku dalībvalstu IT vides kiberdrošībai, kā arī otrādi.

(4) Savienības iestādes, struktūras un aģentūras ir pievilcīgs mērķis, kas saskaras ar ļoti prasmīgiem apdraudētājiem, kam ir daudz resursu, kā arī ar citiem apdraudējumiem. Vienlaikus šajās vienībās ir ļoti atšķirīga līmeņa un gatavības pakāpes kibernoturība un spēja atklāt ļaunprātīgas kiberdarbības un reaģēt uz tām. Tādējādi Eiropas

administrācijas darbībai ir nepieciešama Savienības iestāžu, struktūru un aģentūru vienādi augsta līmeņa kiberdrošība, kas jāsasniedz ar kiberdrošības pamatparametriem (kiberdrošības noteikumu kopuma minimums, kurš tīkla un informācijas sistēmām un to operatoriem un lietotājiem jāievēro, lai minimizētu kiberdrošības riskus), informācijas apmaiņu un sadarbību.

(5) Ar direktīvu [TID 2 priekšlikumu], ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā, tiek plānots vēl vairāk uzlabot publisku un privātu struktūru, valstu kompetento iestāžu un struktūru un Savienības kopējo kiberdrošības noturību un spēju reaģēt uz incidentiem. Tāpēc Savienības iestādēm, struktūrām un aģentūrām jāseko šim paraugam, nodrošinot, ka noteikumi atbilst direktīvai [TID 2 priekšlikumam] un tās vērienīguma līmenim.

(6) Lai panāktu vienādi augsta līmeņa kiberdrošību, katrai Savienības iestādei, struktūrai un aģentūrai jāizveido iekšējās kiberdrošības riska pārvaldības, vadības un kontroles sistēma, kas nodrošina iedarbīgu un piesardzīgu visu kiberdrošības risku pārvaldību, kā arī ņem vērā darbības nepārtrauktību un krīzes vadību.

(7) Tā kā Savienības iestāžu, struktūru un aģentūru vidū pastāv atšķirības, ir vajadzīga elastīga īstenošana, jo nav universāla risinājuma. Vienādi augsta līmeņa kiberdrošības pasākumiem nebūtu jāietver pienākumi, kas tieši traucē Savienības iestāžu, struktūru un aģentūru misijas īstenošanai vai mazina to institucionālo autonomiju. Tāpēc šīm iestādēm, struktūrām un aģentūrām būtu jāizveido sava kiberdrošības riska pārvaldības, vadības un kontroles sistēma un jāpieņem savi pamatparametri un kiberdrošības plāni.

(8) Lai izvairītos no nesamērīga finansiāla un administratīva sloga radīšanas Savienības iestādēm, struktūrām un aģentūrām, kiberdrošības riska pārvaldības prasībām vajadzētu būt samērīgām ar risku, ko rada attiecīgā tīklu un informācijas sistēma, ņemot vērā jaunākos sasniegumus saistībā ar šādiem pasākumiem. Ikvienai Savienības iestādei, struktūrai un aģentūrai vajadzētu plānot piešķirt pienācīgu sava IT budžeta daļu kiberdrošības līmeņa uzlabošanai; ilgtermiņā būtu jācenšas sasniegt aptuveni 10 % mērķrādītāju.

(9) Lai panāktu vienādi augsta līmeņa kiberdrošību, šī joma jāuzrauga ikvienas Savienības iestādes, struktūras un aģentūras visaugstākā līmeņa vadībai, kam būtu jāapstiprina kiberdrošības pamatparametri, kuros būtu jāņem vērā tajā sistēmā konstatētie riski, kas jāizveido katrā iestādē, struktūrā un aģentūrā. Kiberdrošības kultūras jautājums, t. i., kiberdrošības ikdienas prakse, ir neatņemama kiberdrošības pamatparametru daļa visās Savienības iestādēs, struktūrās un aģentūrās.

(10) Savienības iestādēm, struktūrām un aģentūrām būtu jānovērtē riski, kas skar attiecības ar piegādātājiem un pakalpojumu sniedzējiem, tostarp datu glabāšanas un apstrādes pakalpojumu vai pārvaldītu drošības pakalpojumu sniedzējiem, un būtu jāpieņem atbilstīgi pasākumi to novēršanai. Šiem pasākumiem vajadzētu būt kiberdrošības pamatparametru daļai un sīkāk precizētiem *CERT-EU* izdotajos norādījumu dokumentos vai ieteikumos. Nosakot pasākumus un pamatnostādnes, pienācīgi būtu jāņem vērā relevantie ES tiesību akti un rīcībpolitika, ieskaitot TID sadarbības grupas izdotos riska novērtējumus un ieteikumus, piemēram, ES koordinēto riska novērtējumu, kā arī ES rīkkopu 5G drošībai. Turklāt varētu būt nepieciešama attiecīgo IKT produktu, pakalpojumu un procesu sertifikācija saskaņā ar konkrētām ES kiberdrošības sertifikācijas shēmām, kas pieņemtas atbilstīgi Regulas (ES) 2019/881 49. pantam.

(11) Savienību iestāžu un struktūru ģenerālsekretāri 2011. gada maijā nolēma izveidot Savienības iestāžu, struktūru un aģentūru datorapdraudējumu reaģēšanas vienības (*CERT-EU*) iepriekšējas konfigurācijas grupu, kuru uzrauga iestāžu koordinācijas padome. 2012. gada jūlijā ģenerālsekretāri apstiprināja praktiskos pasākumus un vienojās saglabāt *CERT-EU* kā pastāvīgu vienību, kas arī turpmāk palīdzēs uzlabot Savienības iestāžu, struktūru un aģentūru informācijas tehnoloģiju drošības kopējo līmeni un būs piemērs skaidrai iestāžu sadarbībai kiberdrošības jomā. 2012. septembrī *CERT-EU* tika izveidota kā Eiropas Komisijas darba grupa ar pilnvarām iestāžu līmenī. 2017. gada decembrī Savienības iestādes un struktūras noslēdza iestāžu vienošanos par *CERT-EU* organizāciju un darbību[3]. Šī vienošanās būtu turpmāk jāattīsta, lai atbalstītu šīs regulas īstenošanu.

(12) *CERT-EU* no datorapdraudējumu reaģēšanas vienības būtu jāpārdēvē par Savienības iestāžu, struktūru un aģentūru kiberdrošības centru saskaņā ar norisēm dalībvalstīs un pasaulē, kur daudzas *CERT* pārdēvē par kiberdrošības centriem, taču nosaukuma atpazīstamības dēļ būtu jāsaglabā īsais nosaukums *CERT-EU*.

(13) Daudzi kiberuzbrukumi ir daļa no plašākām kampaņām, kas vērstas pret Savienības iestādēm, struktūrām un aģentūrām vai interešu kopienām, kuras ietver Savienības iestādes, struktūras un aģentūras. Lai nodrošinātu preventīvu atklāšanu, reaģēšanu uz incidentiem vai mazināšanas pasākumus, Savienības iestādēm, struktūrām un aģentūrām būtu jāpaziņo *CERT-EU* par nozīmīgiem kiberdraudiem, nozīmīgām ievainojamībām un nozīmīgiem incidentiem un jānorāda atbilstošas tehniskas detaļas, kas ļauj noteikt vai mazināt līdzīgus kiberdraudus, ievainojamības un incidentus citās Savienības iestādēs, struktūrās un aģentūrās, kā arī reaģēt uz tiem. Ievērojot tādu pašu pieeju kā to, kas paredzēta direktīvā [TID 2 priekšlikumā], vienībām, uzzinot par būtisku incidentu, sākotnējais paziņojums *CERT-EU* būtu jāiesniedz 24 stundu laikā. Šādai informācijas apmaiņai būtu jāļauj *CERT-EU* izplatīt informāciju citām Savienības iestādēm, struktūrām un aģentūrām, kā arī attiecīgajiem partneriem, lai palīdzētu aizsargāt Savienības IT vidi un Savienības partneru IT vidi pret līdzīgiem incidentiem, apdraudējumiem un ievainojamībām.

(14) Papildus lielāka uzdevumu skaita un plašākas lomas piešķiršanai *CERT-EU* būtu jāizveido Iestāžu kiberdrošības padome (IKP), kurai būtu jāsekmē vienādi augsta līmeņa kiberdrošība Savienības iestādēs, struktūrās un aģentūrās, uzraugot šīs regulas īstenošanu Savienības iestādēs, struktūrās un aģentūrās, kā arī uzraugot *CERT-EU* vispārējo prioritāšu un mērķu īstenošanu un sniedzot *CERT-EU* norādes par stratēģisko virzienu. IKP būtu jānodrošina iestāžu pārstāvība, kā arī aģentūru un struktūru pārstāvju dalība, izmantojot Savienības aģentūru tīklu.

(15) *CERT-EU* būtu jāatbalsta pasākumu īstenošana vienādi augsta līmeņa kiberdrošības panākšanai, iesniedzot norādījumu dokumentu un ieteikumu priekšlikumus IKP vai aicinot rīkoties. Šādi norādījumu dokumenti un ieteikumi būtu jāapstiprina IKP. Vajadzības gadījumā *CERT-EU* būtu jāaicina rīkoties, aprakstot neatliekamus drošības pasākumus, kurus Savienības iestādes, struktūras un aģentūras tiek mudinātas veikt noteiktā laika posmā.

(16) IKP būtu jāuzrauga atbilstība šai regulai, kā arī jāveic pasākumi pēc norādījumu dokumentu, ieteikumu un *CERT-EU* aicinājumu rīkoties publiskošanas. Tehniskos jautājumos IKP būtu jāsaņem atbalsts no tehniskajām padomdevēju grupām, kas nokomplektētas pēc IKP ieskatiem un kam būtu jāstrādā ciešā sadarbībā ar *CERT-EU*,

[3] OV C 12, 13.1.2018., 1.–11. lpp.

Savienības iestādēm, struktūrām un aģentūrām, kā arī, ja nepieciešams, citām ieinteresētajām personām. Ja vajadzīgs, IKP būtu jāpieņem nesaistoši brīdinājumi un jāiesaka revīzijas.

(17) *CERT-EU* būtu jāuztic uzdevums dot ieguldījumu visu Savienības iestāžu, struktūru un aģentūru IT vides drošībā. *CERT-EU* būtu jārīkojas kā nozīmētā koordinatora ekvivalentam Savienības iestādēs, struktūrās un aģentūrās, lai panāktu ievainojamību koordinētu paziņošanu Eiropas ievainojamību reģistram, kas minēts direktīvas [TID 2 priekšlikuma] 6. pantā.

(18) 2020. gadā *CERT-EU* koordinācijas padome *CERT-EU* noteica jaunu stratēģisku mērķi, lai garantētu visaptverošu kiberaizsardzības līmeni visām Savienības iestādēm, struktūrām un aģentūrām ar atbilstošu tvērumu un dziļumu, kā arī pastāvīgu pielāgošanos esošajiem vai nākotnes apdraudējumiem, kas ietver uzbrukumus mobilajām ierīcēm, mākoņvidei un lietu interneta ierīcēm. Stratēģiskais mērķis iever arī plaša spektra drošības operāciju centrus (DOC), kas uzrauga tīklus, un īpaši bīstamu apdraudējumu nepārtrauktu uzraudzību. *CERT-EU* būtu jāatbalsta lielāku Savienības iestāžu, struktūru un aģentūru IT drošības grupas, tostarp attiecībā uz nepārtrauktu uzraudzību zemākajā līmenī. *CERT-EU* būtu jāsniedz visi pakalpojumi mazām un dažām vidēja lieluma Savienības iestādēm, struktūrām un aģentūrām.

(19) *CERT-EU* arī būtu jāpilda loma, kas direktīvā [TID 2 priekšlikumā] tai paredzēta saistībā ar sadarbību un informācijas apmaiņu ar datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu. Turklāt saskaņā ar Komisijas Ieteikumu (ES) 2017/1584[4] *CERT-EU* būtu jāsadarbojas un jākoordinē reakcija ar attiecīgajām ieinteresētajām personām. Lai sekmētu augsta līmeņa kiberdrošību visā Savienībā, *CERT-EU* būtu jādalās ar atbilstošām valstu iestādēm ar konkrētu informāciju par incidentiem. *CERT-EU* būtu arī jāsadarbojas ar citām publiskām un privātām struktūrām, kas ietver NATO, ja saņemta iepriekšēja IKP atļauja.

(20) Atbalstot operatīvo kiberdrošību, *CERT-EU* būtu jāizmanto Eiropas Savienības Kiberdrošības aģentūras pieejamā lietpratība, izmantojot strukturētu sadarbību, kā paredzēts Eiropas Parlamenta un Padomes Regulā (ES) 2019/881[5]. Attiecīgā gadījumā starp abām vienībām būtu jāpanāk īpaša vienošanās par šādas sadarbības praktiskas īstenošanas kārtību un jāizvairās no darbību dublēšanās. *CERT-EU* būtu arī jāsadarbojas ar Eiropas Savienības Kiberdrošības aģentūru saistībā ar apdraudējumu analīzi un regulāri jākopīgo savs ziņojums par esošo apdraudējuma situāciju ar aģentūru.

(21) Lai atbalstītu Kopējo kibervienību, kas izveidota saskaņā ar Komisijas 2021. gada 23. jūnija ieteikumu[6], *CERT-EU* būtu jāsadarbojas un jāapmainās ar informāciju ar ieinteresētajām personām, lai sekmētu operatīvo sadarbību un ļautu esošajiem tīkliem realizēt visu savu potenciālu Savienības aizsardzībā.

---

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

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

[6] Komisijas Ieteikums C(2021) 4520 (2021. gada 23. jūnijs) par Kopējās kibervienības izveidošanu.

(22) Visi atbilstoši šai regulai izmantotie persondati būtu jāapstrādā saskaņā ar datu aizsardzības tiesību aktiem, kas ietver arī Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725[7].

(23) *CERT-EU* un Savienības iestādēm, struktūrām un aģentūrām informācija būtu jāapstrādā atbilstoši noteikumiem, kas norādīti regulā [ierosinātajā regulā par informācijas drošību]. Lai nodrošinātu koordināciju drošības jautājumos, par visu saziņu ar *CERT-EU*, ko aizsāk vai prasa valsts drošības un izlūkošanas dienesti, būtu bez liekas kavēšanās jāpaziņo Komisijas Drošības direktorātam un IKP priekšsēdētājam.

(24) Tā kā *CERT-EU* pakalpojumi un uzdevumi ir visu Savienības iestāžu, struktūru un aģentūru interesēs, katrai Savienības iestādei, struktūrai un aģentūrai, kam ir tēriņi IT jomā, būtu jādod taisnīgs ieguldījums šo pakalpojumu un uzdevumu izpildē. Šis ieguldījums neskar Savienības iestāžu, struktūru un aģentūru budžeta autonomiju.

(25) IKP ar *CERT-EU* palīdzību būtu jāpārskata un jāizvērtē šīs regulas īstenošana un konstatējumi būtu jāziņo Komisijai. Balstoties uz šo devumu, Komisijai būtu jāziņo Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai,

IR PIEŅĒMUŠI ŠO REGULU.

## I nodaļa
## VISPĀRĪGI NOTEIKUMI

### *1. pants*
### ***Priekšmets***

Šī regula nosaka:

(a) Savienības iestāžu, struktūru un aģentūru pienākumus izveidot iekšēju kiberdrošības riska pārvaldības, vadības un kontroles sistēmu;

(b) Savienības iestāžu, struktūru un aģentūru kiberdrošības riska pārvaldības un ziņošanas pienākumus;

(c) ES iestāžu, struktūru un aģentūru kiberdrošības centra (*CERT-EU*) un Iestāžu kiberdrošības padomes (IKP) organizācijas un darbības noteikumus.

### *2. pants*
### ***Darbības joma***

Šo regulu piemēro kiberdrošības riska pārvaldībai, vadībai un kontrolei visās Savienības iestādēs, struktūrās un aģentūrās un *CERT-EU* un Iestāžu kiberdrošības padomes organizācijai un darbībai.

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

*3. pants*

***Definīcijas***

Šajā regulā piemēro šādas definīcijas:

(1) "Savienības iestādes, struktūras un aģentūras" ir Savienības iestādes, struktūras un aģentūras, kas izveidotas ar vai balstoties uz Līgumu par Eiropas Savienību, Līgumu par Eiropas Savienības darbību vai Eiropas Atomenerģijas kopienas dibināšanas līgumu;

(2) "tīklu un informācijas sistēma" ir tīklu un informācijas sistēma direktīvas [TID 2 priekšlikuma] 4. panta 1. punkta nozīmē;

(3) "tīklu un informācijas sistēmu drošība" ir tīklu un informācijas sistēmu drošība direktīvas [TID 2 priekšlikuma] 4. panta 2. punkta nozīmē;

(4) "kiberdrošība" ir kiberdrošība direktīvas [TID 2 priekšlikuma] 4. panta 3. punkta nozīmē;

(5) "visaugstākā līmeņa vadība" ir vadītājs, pārvaldības vai koordinācijas un uzraudzības struktūra visaugstākajā administratīvajā līmenī, ņemot vērā augsta līmeņa pārvaldības kārtību katrā Savienības iestādē, struktūrā vai aģentūrā;

(6) "incidents" ir incidents direktīvas [TID 2 priekšlikuma] 4. panta 5. punkta nozīmē;

(7) "būtisks incidents" ir jebkāds incidents, ja vien tam nav ierobežota ietekme un, visticamāk, to jau labi izprot attiecībā uz metodi vai tehnoloģiju;

(8) "būtisks uzbrukums" ir jebkāds incidents, kura gadījumā nepieciešams vairāk resursu, nekā ir pieejams skartajā Savienības iestādē, struktūrā vai aģentūrā un *CERT-EU*;

(9) "incidenta risināšana" ir incidenta risināšana direktīvas [TID 2 priekšlikuma] 4. panta 6. punkta nozīmē;

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

(11) "būtiski kiberdraudi" ir kiberdraudi, kad ir nolūks, iespēja un spējas izraisīt būtisku incidentu;

(12) "ievainojamība" ir ievainojamība direktīvas [TID 2 priekšlikuma] 4. panta 8. punkta nozīmē;

(13) "būtiska ievainojamība" ir ievainojamība, kas, visticamāk, izraisīs būtisku incidentu, ja to izmantos;

(14) "kiberdrošības risks" ir jebkāds racionāli identificējams apstāklis vai notikums, kas var nelabvēlīgi ietekmēt tīklu un informācijas sistēmu drošību;

(15) "Kopējā kibervienība" ir virtuāla un fiziska sadarbības platforma dažādām kiberdrošības kopienām Savienībā ar uzsvaru uz operatīvo un tehnisko koordināciju cīņai pret būtiskiem pārrobežu kiberdraudiem un incidentiem Komisijas 2021. gada 23. jūnija ieteikuma nozīmē;

(16) "kiberdrošības pamatparametri" ir minimālo kiberdrošības noteikumu kopums, kam jāatbilst tīklu un informācijas sistēmām un kas jāievēro to operatoriem un lietotājiem, lai samazinātu kiberdrošības riskus.

## II nodaļa
## PASĀKUMI VIENĀDI AUGSTA LĪMEŅA KIBERDROŠĪBAI

*4. pants*

***Riska pārvaldība, vadība un kontrole***

1. Katra Savienības iestāde, struktūra un aģentūra, īstenojot savu institucionālo autonomiju, izveido savu iekšējo kiberdrošības riska pārvaldības, vadības un kontroles sistēmu (“sistēma”), kas atbalsta konkrētās vienības misiju. Šo darbu uzrauga konkrētās vienības visaugstākā līmeņa vadība, lai nodrošinātu iedarbīgu un piesardzīgu visu kiberdrošības risku pārvaldību. Sistēma ir ieviesta ne vēlāk kā …. [15 mēneši pēc šīs regulas stāšanās spēkā].

2. Sistēma ietver visu attiecīgās iestādes, struktūras vai aģentūras IT vidi, arī jebkādu IT vidi organizācijas telpās, ārpakalpojumu aktīvus un pakalpojumus mākoņdatošanas vidē vai trešās personas mitinātus aktīvus vai pakalpojumus, mobilās ierīces, korporatīvos tīklus, uzņēmumu tīklus, kas nav pievienoti internetam, un jebkādas IT videi pievienotas ierīces. Sistēmā ņem vērā darbības nepārtrauktību, krīzes vadību un piegādes ķēdes drošību, kā arī tādu cilvēku radītu risku pārvaldību, kuri varētu ietekmēt attiecīgās Savienības iestādes, struktūras vai aģentūras kiberdrošību.

3. Katras Savienības iestādes, struktūras un aģentūras visaugstākā līmeņa vadība nodrošina uzraudzību attiecībā uz savas organizācijas atbilstību pienākumiem, kas saistīti ar kiberdrošības riska pārvaldību, vadību un kontroli, neskarot citu vadības līmeņu oficiālos pienākumus, kas saistīti ar atbilstību prasībām un riska pārvaldību to atbildības jomās.

4. Katra Savienības iestāde, struktūra un aģentūra ievieš iedarbīgus mehānismus, kuru mērķis ir nodrošināt, ka pienācīga to IT budžeta procentuālā daļa tiek tērēta par kiberdrošību.

5. Katra Savienības iestāde, struktūra un aģentūra ieceļ vietējo kiberdrošības speciālistu vai līdzvērtīgu darbinieku, kas rīkojas kā tās vienotais kontaktpunkts attiecībā uz visiem kiberdrošības aspektiem.

*5. pants*

***Kiberdrošības pamatparametri***

1. Katras Savienības iestādes, struktūras un aģentūras visaugstākā līmeņa vadība apstiprina konkrētās vienības kiberdrošības pamatparametrus, kuru mērķis ir novērst 4. panta 1. punktā minētajā sistēmā minētos riskus. Tas tiek darīts tā, lai atbalstītu vienības misiju un īstenota tās institucionālo autonomiju. Kiberdrošības pamatparametrus ievieš ne vēlāk kā …. [18 mēneši pēc šīs regulas stāšanās spēkā], un tajos ietver I pielikumā uzskaitītās jomas un II pielikumā uzskaitītos pasākumus.

2. Katras Savienības iestādes, struktūras un aģentūras augstā vadība regulāri piedalās īpašās apmācībās, lai gūtu zināšanas un prasmes, kas ir pietiekamas, lai izprastu un novērtētu kiberdrošības riska un pārvaldības praksi, kā arī to ietekmi uz organizācijas darbību.

*6. pants*

***Gatavības novērtējumi***

Katra Savienības iestāde, struktūra un aģentūra vismaz reizi trīs gados veic kiberdrošības gatavības novērtējumu, kurā iekļauj visus IT vides elementus, kā aprakstīts 4. pantā, ņemot vērā relevantos norādījumu dokumentus un ieteikumus, kas pieņemti saskaņā ar 13. pantu.

*7. pants*

***Kiberdrošības plāni***

1. Pēc gatavības novērtējuma secinājumu izdarīšanas, kā arī ņemot vērā aktīvus un riskus, kas konstatēti saskaņā ar 4. pantu, katras Savienības iestādes, struktūras un aģentūras visaugstākā līmeņa vadība pēc riska pārvaldības, vadības un kontroles sistēmas un kiberdrošības pamatparametru izveides bez liekas kavēšanās apstiprina kiberdrošības plānu. Šā plāna mērķis ir palielināt attiecīgās vienības vispārējo kiberdrošību, un tādējādi tas sekmē vienādi augsta līmeņa kiberdrošības panākšanu vai uzlabošanu visās Savienības iestādēs, struktūrās un aģentūrās. Lai atbilstoši institucionālajai autonomijai atbalstītu vienības misiju, plānā iekļauj vismaz I pielikumā minētās jomas, II pielikumā minētos pasākumus, kā arī pasākumus, kas saistīti ar gatavību incidentiem, reaģēšanu uz incidentiem un atgūšanos no tiem, piemēram, drošības uzraudzību un datu reģistrēšanu. Plānu pārskata ne retāk kā reizi trīs gados pēc gatavības novērtējumiem, ko veic saskaņā ar 6. pantu.
2. Kiberdrošības plānā ietver darbinieku atbildības jomas un pienākumus attiecībā uz tā īstenošanu.
3. Kiberdrošības plānā ņem vērā visus *CERT-EU* izdotos norādījumu dokumentus un ieteikumus.

*8. pants*

***Īstenošana***

1. Pēc gatavības novērtējumu pabeigšanas Savienības iestādes, struktūras un aģentūras tos iesniedz Iestāžu kiberdrošības padomei. Pēc drošības plānu pabeigšanas Savienības iestādes, struktūras un aģentūras par pabeigšanu informē Iestāžu kiberdrošības padomi. Pēc padomes pieprasījuma tās ziņo par noteiktiem šīs nodaļas aspektiem.
2. Saskaņā ar 13. pantu izdotie norādījumu dokumenti un ieteikumi sekmē šajā nodaļā izklāstīto noteikumu īstenošanu.

## III nodaļa
## IESTĀŽU KIBERDROŠĪBAS PADOME

*9. pants*

***Iestāžu kiberdrošības padome***

1. Izveido Iestāžu kiberdrošības padomi (IKP).
2. IKP ir atbildīga par:
   (a) šīs regulas īstenošanas uzraudzību Savienības iestādēs, struktūrās un aģentūrās;
   (b) *CERT-EU* vispārējo prioritāšu un mērķu īstenošanas uzraudzību un *CERT-EU* stratēģiskā virziena noteikšanu.

3. IKP sastāv no trīs pārstāvjiem, ko pēc IKT Padomdevējas komitejas rosinājuma izvirza Eiropas Savienības aģentūru tīkls (ESAT), lai pārstāvētu tādu aģentūru un struktūru intereses, kas uztur savu IT vidi, un no viena pārstāvja, ko iecēlusi katra no tālāk norādītajām iestādēm:

   (a) Eiropas Parlaments;

   (b) Eiropas Savienības Padome;

   (c) Eiropas Komisija;

   (d) Eiropas Savienības Tiesa;

   (e) Eiropas Centrālā banka;

   (f) Eiropas Revīzijas palāta;

   (g) Eiropas Ārējās darbības dienests;

   (h) Eiropas Ekonomikas un sociālo lietu komiteja;

   (i) Eiropas Reģionu komiteja;

   (j) Eiropas Investīciju banka;

   (k) Eiropas Savienības Kiberdrošības aģentūra.

   Dalībniekiem var palīdzēt aizvietotājs. Citu iepriekš minēto organizāciju vai citu Savienības iestāžu, struktūru un aģentūru pārstāvjus priekšsēdētājs drīkst uzaicināt piedalīties IKP sanāksmēs bez balsošanas tiesībām.

4. IKP pieņem iekšējo reglamentu.

5. Saskaņā ar iekšējo reglamentu no visu dalībnieku vidus IKP ieceļ priekšsēdētāju uz četru gadu periodu. Priekšsēdētāja aizvietotājs kļūst par pilntiesīgu IKP locekli uz tādu pašu laika periodu.

6. IKP tiekas pēc priekšsēdētāja iniciatīvas, pēc *CERT-EU* pieprasījuma vai pēc kāda tās locekļa lūguma.

7. Katram IKP loceklim ir viena balss. IKP lēmumus pieņem ar vienkāršu balsu vairākumu, izņemot šajā regulā paredzētos gadījumus. Priekšsēdētājs nebalso, ja vien nav saņemts vienlīdzīgs balsu skaits un priekšsēdētāja balss ir izšķirošā.

8. IKP var rīkoties saskaņā ar vienkāršu rakstveida procedūru, ko uzsāk atbilstoši iekšējam IKP reglamentam. Saskaņā ar šo procedūru attiecīgais lēmums tiek uzskatīts par pieņemtu priekšsēdētāja noteiktajā laika periodā, ja vien kāds loceklis neiebilst.

9. *CERT-EU* vadītājs vai vadītāja aizvietotājs piedalās IKP sanāksmēs, ja vien IKP nelemj citādi.

10. IKP sekretariāta pakalpojumus nodrošina Komisija.

11. Pēc IKT Padomdevējas komitejas ierosinājuma ESAT izvirzītie pārstāvji informē Savienības aģentūras un kopuzņēmumus par IKP lēmumiem. Visām Savienības aģentūrām un struktūrām ir tiesības informēt pārstāvjus vai IKP priekšsēdētāju par jebkuru jautājumu, ko tās uzskata par tādu, kas būtu jādara zināms IKP.

12. IKP var rīkoties saskaņā ar vienkāršu rakstveida procedūru, kuru uzsāk priekšsēdētājs un kuras gadījumā attiecīgais lēmums tiek uzskatīts par apstiprinātu priekšsēdētāja noteiktajā laika periodā, ja vien kāds loceklis neiebilst.

13. IKP var izvirzīt izpildkomiteju, kas palīdz IKP veikt tās darbu, kā arī deleģēt izpildkomitejai dažus savus uzdevumus un pilnvaras. IKP pieņem izpildkomitejas reglamentu, kas ietver tās uzdevumus un pilnvaras, kā arī locekļu pilnvaru laiku.

*10. pants*
***IKP uzdevumi***

Īstenojot savus pienākumus, IKP jo īpaši:

(a) pārskata no *CERT-EU* pieprasītus ziņojumus par šīs regulas īstenošanu Savienības iestādēs, struktūrās un aģentūrās;

(b) pamatojoties uz *CERT-EU* vadītāja priekšlikumu, apstiprina *CERT-EU* gada darba programmu un uzrauga tās īstenošanu;

(c) pamatojoties uz *CERT-EU* vadītāja priekšlikumu, apstiprina *CERT-EU* pakalpojumu katalogu;

(d) pamatojoties uz *CERT-EU* vadītāja priekšlikumu, apstiprina *CERT-EU* darbību ieņēmumu un izdevumu gada finanšu plānu, kas ietver arī personāla komplektēšanu;

(e) pamatojoties uz *CERT-EU* vadītāja priekšlikumu, apstiprina pakalpojumu līmeņa nolīgumu nosacījumus;

(f) pārbauda un apstiprina *CERT-EU* vadītāja sagatavoto gada pārskatu par *CERT-EU* darbībām un līdzekļu pārvaldību;

(g) apstiprina un uzrauga galvenos *CERT-EU* darbības rādītājus, kas definēti pēc *CERT-EU* vadītāja priekšlikuma;

(h) apstiprina sadarbības kārtību, pakalpojumu līmeņa vienošanās vai līgumus starp *CERT-EU* un citām vienībām atbilstoši 17. pantam;

(i) veido tik daudz tehnisko padomdevēju grupu, cik nepieciešams, lai palīdzētu veikt IKP darbu, apstiprina to pilnvaras un ieceļ to attiecīgos priekšsēdētājus.

*11. pants*
***Atbilstība***

IKP uzrauga šīs regulas un pieņemto norādījumu dokumentu, ieteikumu un aicinājumu rīkoties īstenošanu Savienības iestādēs, struktūrās un aģentūrās. Ja IKP konstatē, ka Savienības iestādes, struktūras vai aģentūras nav iedarbīgi piemērojušas vai īstenojušas šo regulu vai norādījumu dokumentus, ieteikumus un aicinājumus rīkoties, kas izdoti saskaņā ar šo regulu, tā, neskarot attiecīgās Savienības iestādes, struktūras vai aģentūras iekšējās procedūras, drīkst:

(a) izdot brīdinājumu; ja tas nepieciešams nopietna kiberdrošības riska dēļ, brīdinājuma saņēmēju loku atbilstoši ierobežo;

(b) ieteikt attiecīgam revīzijas dienestam veikt revīziju.

## IV nodaļa
## *CERT-EU*

### *12. pants*
### *CERT-EU misija un uzdevumi*

1. *CERT-EU* ir autonoms starpiestāžu kiberdrošības centrs visām Savienības iestādēm, struktūrām un aģentūrām, un tā misija ir dot ieguldījumu visu Savienības iestāžu, struktūru un aģentūru IT vides drošībā, dodot tām padomus par kiberdrošību un palīdzot novērst, atklāt un mazināt incidentus un reaģēt uz tiem, kā arī rīkojoties kā to kiberdrošības informācijas apmaiņas un reaģēšanas uz incidentiem koordinēšanas centram.

2. *CERT-EU* Savienības iestāžu, struktūru un aģentūru vajadzībām veic šādus uzdevumus:

   (a) sniedz tām atbalstu šīs regulas īstenošanā un sekmē šīs regulas piemērošanas koordinēšanu, izmantojot 13. panta 1. punktā uzskaitītos pasākumus vai IKP pieprasītus *ad hoc* ziņojumus;

   (b) sniedz tām atbalstu ar tā pakalpojumu katalogā aprakstīto kiberdrošības pakalpojumu pakotni ("pamatpakalpojumi");

   (c) uztur partneru un kolēģu tīklu, lai sekmētu pakalpojumu sniegšanu, kā norādīts 16. un 17. pantā;

   (d) pievērš IKP uzmanību visiem jautājumiem, kas saistīti ar šīs regulas, kā arī norādījumu dokumentu, ieteikumu un aicinājumu rīkoties, īstenošanu;

   (e) ziņo par kiberdraudiem, ar ko saskaras Savienības iestādes, struktūras un aģentūras, un sekmē kibersituācijas apzināšanos ES.

3. *CERT-EU* atbalsta Kopējo kibervienību, kas izveidota saskaņā ar Komisijas 2021. gada 23. jūnija ieteikumu, tostarp šādās jomās:

   (a) gatavība, incidentu koordinēšana, informācijas apmaiņa un reaģēšana uz krīzi tehniskā līmenī ar Savienības iestādēm, struktūrām un aģentūrām saistītos gadījumos;

   (b) operatīvā sadarbība saistībā ar datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu, kā arī savstarpējo palīdzību un plašāku kiberdrošības kopienu;

   (c) kiberdraudu izlūkdati, arī situācijas apzināšanās;

   (d) jebkurš gadījums, kad vajadzīgas *CERT-EU* tehniskā zinātība par kiberdrošību.

4. *CERT-EU* iesaistās strukturētā sadarbībā ar Eiropas Savienības Kiberdrošības aģentūru saistībā ar spēju veidošanu, operatīvo sadarbību un kiberdraudu ilgtermiņa stratēģisko analīzi saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/881.

5. *CERT-EU* var sniegt tālāk norādītos pakalpojumus, kas nav aprakstīti pakalpojumu katalogā ("maksas pakalpojumi"):

   (a) pakalpojumi, kas sekmē Savienības iestāžu, struktūru un aģentūru IT vides kiberdrošību un nav minēti 2. punktā, pamatojoties uz pakalpojumu līmeņa nolīgumiem un atkarībā no pieejamajiem resursiem;

(b) pakalpojumi, kas sekmē kiberdrošības darbības vai Savienības iestāžu, struktūru un aģentūru projektus, izņemot pakalpojumus to IT vides aizsardzībai, pamatojoties uz rakstveida līgumiem un iepriekš saņemot IKP apstiprinājumu;

(c) pakalpojumi, kas sekmē IT vides drošību organizācijās, kuras nav Savienības iestādes, struktūras un aģentūras, bet cieši sadarbojas ar Savienības iestādēm, struktūrām un aģentūrām, piemērām, izpilda atbilstoši Savienības tiesību aktiem uzticētus uzdevumus vai pienākumus, pamatojoties uz rakstveida līgumiem un iepriekš saņemot IKP apstiprinājumu.

6. *CERT-EU* var organizēt kiberdrošības mācības vai ieteikt piedalīties esošās mācībās ciešā sadarbībā ar Eiropas Savienības Kiberdrošības aģentūru, kad vien iespējams, lai pārbaudītu Savienības iestāžu, struktūru un aģentūru kiberdrošības līmeni.

7. *CERT-EU* var sniegt palīdzību Savienības iestādēm, struktūrām un aģentūrām saistībā ar incidentiem klasificētā IT vidē, ja to nepārprotami pieprasa attiecīgā organizācija.

*13. pants*

***Norādījumu dokumenti, ieteikumi un aicinājumi rīkoties***

1. *CERT-EU* atbalsta šīs regulas īstenošanu, izdodot:

(a) aicinājumus rīkoties, kuros apraksta neatliekamus drošības pasākumus, ko Savienības iestādes, struktūras un aģentūras tiek mudinātas veikt noteiktā laika posmā;

(b) IKP adresētus priekšlikumus norādījumu dokumentiem, kas paredzēti visām Savienības iestādēm, struktūrām un aģentūrām vai kādai to grupai;

(c) IKP adresētus priekšlikumus ieteikumiem, kas paredzēti atsevišķām Savienības iestādēm, struktūrām un aģentūrām.

2. Norādījumu dokumenti un ieteikumi var ietvert:

(a) kiberdrošības riska pārvaldības un kiberdrošības pamatparametru nosacījumus vai uzlabojumus;

(b) gatavības novērtējuma un kiberdrošības plānu kārtību;

(c) attiecīgā gadījumā plaši lietotu tehnoloģiju, arhitektūras un saistītās paraugprakses izmantošanu ar mērķi panākt sadarbspēju un kopējus standartus direktīvas [TID 2 priekšlikuma] 4. panta 10. punkta nozīmē.

3. IKP var pieņemt norādījumu dokumentus vai ieteikumus pēc *CERT-EU* priekšlikuma.

4. IKP var uzdot *CERT-EU* izdot, atsaukt vai mainīt norādījumu dokumentu vai ieteikumu priekšlikumus, vai aicinājumu rīkoties.

*14. pants*

**CERT-EU *vadītājs***

*CERT-EU* vadītājs regulāri iesniedz ziņojumus IKP un IKP priekšsēdētājam par *CERT-EU* darbības rezultātiem, finanšu plānošanu, ieņēmumiem, budžeta izpildi, pakalpojumu līmeņa nolīgumiem un noslēgtajiem rakstveida nolīgumiem, sadarbību ar partneriem un darbinieku veiktajām misijām, tostarp arī 10. panta 1. punktā minētos ziņojumus.

*15. pants*

***Finanšu un personāla jautājumi***

1. Pēc vienprātīga IKP apstiprinājuma saņemšanas Komisija ieceļ *CERT-EU* vadītāju. Pirms *CERT-EU* vadītāja iecelšanas par visiem šā procesa posmiem apspriežas ar IKP; tas jo īpaši attiecas uz paziņojuma par vakanci sagatavošanu, pieteikumu izskatīšanu un atlases komitejas nozīmēšanu šai amata vietai.

2. Administratīvo un finanšu procedūru piemērošanā *CERT-EU* vadītājs darbojas Komisijas pakļautībā.

3. *CERT-EU* veiktos uzdevumus un darbības, ieskaitot pakalpojumus, kurus *CERT-EU* atbilstoši 12. panta 2., 3., 4. un 6. punktam un 13. panta 1. punktam sniedz Savienības iestādēm, struktūrām un aģentūrām, kuras finansē no daudzgadu finanšu shēmas izdevumu kategorijas, kas paredzēta Eiropas publiskajai pārvaldei, finansē no īpašas Komisijas budžeta pozīcijas. *CERT-EU* paredzētās amata vietas sīki izklāsta Komisijas štatu saraksta zemsvītras piezīmē.

4. Savienības iestādes, struktūras un aģentūras, kas nav minētas 3. punktā, veic ikgadēju finansiālu iemaksu *CERT-EU*, lai apmaksātu atbilstoši šim 3. punktam sniegtos *CERT-EU* pakalpojumus. Attiecīgās iemaksas pamatojas uz IKP orientējošo informāciju, par ko vienojas ar katru vienību un *CERT-EU* pakalpojumu līmeņa nolīgumiem. Iemaksas ir taisnīga un samērīga daļa no sniegto pakalpojumu kopējām izmaksām. Tās saņem 3. punktā minētā atsevišķā budžeta pozīcija, un tās saņem kā piešķirtos ieņēmumus saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES, Euratom) 2018/1046[8] 21. panta 3. punkta c) apakšpunktu.

5. Regulas 12. panta 5. punktā minēto uzdevumu izmaksas atgūst no Savienības iestādēm, struktūrām un aģentūrām, kas saņem *CERT-EU* pakalpojumus. Ieņēmumus novirza uz budžeta izmaksu pozīcijām.

*16. pants*

**CERT-EU *sadarbība ar partneriem dalībvalstīs***

1. *CERT-EU* sadarbojas un apmainās ar informāciju ar partneriem dalībvalstīs, tostarp *CERT*, valstu kiberdrošības centriem, *CSIRT* un vienotajiem kontaktpunktiem, kas minēti direktīvas [TID 2 priekšlikuma] 8. pantā, saistībā ar kiberdraudiem, ievainojamībām un incidentiem, iespējamajiem pretpasākumiem un visiem jautājumiem, kas ir būtiski, lai uzlabotu Savienības iestāžu, struktūru un aģentūru IT vides aizsardzību, arī izmantojot direktīvas [TID 2 priekšlikuma] 13. pantā minēto *CSIRT* tīklu.

2. Lai sekmētu līdzīgu kiberdraudu vai incidentu atklāšanu, *CERT-EU* drīkst apmainīties ar konkrētu informāciju par incidentu ar partneriem dalībvalstīs bez skartās organizācijas piekrišanas. *CERT-EU* drīkst apmainīties ar konkrētu informāciju par incidentu, kas atklāj kiberdrošības incidenta mērķa identitāti, tikai ar skartās organizācijas piekrišanu.

---

[8] Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2018/1046 (2018. gada 18. jūlijs) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam, ar kuru groza Regulas (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 un Lēmumu Nr. 541/2014/ES un atceļ Regulu (ES, Euratom) Nr. 966/2012 (OV L 193, 30.7.2018., 1. lpp.).

*17. pants*

**CERT-EU *sadarbība ar partneriem trešās valstīs***

1. Saistībā ar rīkiem un metodēm, piemēram, paņēmieniem, taktiku, procedūrām un paraugpraksi, kā arī saistībā ar kiberdraudiem un ievainojamībām *CERT-EU* drīkst sadarboties ar partneriem trešās valstīs, tostarp partneriem konkrētās nozarēs. *CERT-EU* iepriekš saņem IKP apstiprinājumu, lai jebkādā veidā sadarbotos ar šādiem partneriem, arī satvarā, kur trešo valstu partneri sadarbojas ar partneriem dalībvalstīs.
2. *CERT-EU* drīkst sadarboties ar citiem partneriem, piemēram, komercuzņēmumiem, starptautiskām organizācijām, valstu iestādēm no trešām valstīm vai atsevišķiem ekspertiem, lai apkopotu informāciju par vispārējiem un konkrētiem kiberdraudiem, ievainojamībām un iespējamiem pretpasākumiem. Lai plašāk sadarbotos ar šādiem partneriem, *CERT-EU* iepriekš saņem IKP apstiprinājumu.
3. Saņemot incidentā skartās organizācijas piekrišanu, *CERT-EU* drīkst ar incidentu saistīto informāciju sniegt partneriem, kuri var palīdzēt to analizēt.

## V nodaļa
## SADARBĪBA UN ZIŅOŠANAS PIENĀKUMI

*18. pants*

***Informācijas apstrāde***

1. *CERT-EU* un Savienības iestādes, struktūras un aģentūras ievēro dienesta noslēpuma glabāšanas pienākumu saskaņā ar Līguma par Eiropas Savienības darbību 339. pantu vai līdzvērtīgu piemērojamu regulējumu.
2. Eiropas Parlamenta un Padomes Regulas (EK) Nr. 1049/2001[9] noteikumus piemēro pieprasījumiem par publisku piekļuvi *CERT-EU* turējumā esošiem dokumentiem, ieskaitot minētajā regulā noteikto pienākumu apspriesties ar citām Savienības iestādēm, struktūrām un aģentūrām, ja pieprasījums attiecas uz to dokumentiem.
3. Uz persondatu apstrādi, ko veic saskaņā ar šo regulu, attiecas Eiropas Parlamenta un Padomes Regula (ES) 2018/1725.
4. *CERT-EU* un Savienības iestādes, struktūras un aģentūras apstrādā informāciju atbilstoši noteikumiem, kas norādīti [ierosinātajā regulā par informācijas drošību].
5. Par visu saziņu ar *CERT-EU*, ko aizsāk vai rosina valsts drošības un izlūkošanas dienesti, bez liekas kavēšanās ziņo Komisijas Drošības direktorātam un IKP priekšsēdētājam.

*19. pants*

***Kopīgošanas pienākumi***

1. Lai *CERT-EU* varētu koordinēt ievainojamību pārvaldību un reaģēšanu uz incidentiem, tā drīkst pieprasīt Savienības iestādēm, struktūrām un aģentūrām sniegt tādu informāciju no to attiecīgajām IT sistēmām, kas ir būtiska *CERT-EU* atbalstam. Pieprasījuma saņēmēja iestāde, struktūra vai aģentūra bez liekas kavēšanās nosūta prasīto informāciju un tās atjauninājumus.

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

2. Savienības iestādes, struktūras un aģentūras pēc *CERT-EU* pieprasījuma un bez liekas kavēšanās tam sniedz digitālo informāciju, kas radusies attiecīgajos incidentos iesaistīto elektronisko ierīču izmantošanas rezultātā. *CERT-EU* drīkst sīkāk precizēt, kuri šādas digitālās informācijas veidi ir vajadzīgi situācijas apzināšanai un reaģēšanai uz incidentiem.

3. *CERT-EU* drīkst apmainīties ar konkrētu informāciju par incidentu, kas atklāj incidentā skartās Savienības iestādes, struktūras vai aģentūras identitāti, tikai ar šīs vienības piekrišanu. *CERT-EU* drīkst apmainīties ar konkrētu informāciju par incidentu, kas atklāj kiberdrošības incidenta mērķa identitāti, tikai ar incidentā skartās vienības piekrišanu.

4. Kopīgošanas pienākumi neattiecas uz ES klasificēto informāciju (ESKI) un uz informāciju, ko Savienības iestāde, struktūra vai aģentūra ir saņēmusi no dalībvalsts drošības vai izlūkošanas dienesta vai tiesībaizsardzības iestādes ar skaidru nosacījumu, ka tā netiks kopīgota ar *CERT-EU*.

*20. pants*
***Paziņošanas pienākumi***

1. Visas Savienības iestādes, struktūras un aģentūras bez liekas kavēšanās, bet ne vēlāk kā 24 stundas pēc tam, kad par to uzzinājušas, sniedz sākotnēju paziņojumu *CERT-EU* par būtiskiem kiberdraudiem, būtiskām ievainojamībām un būtiskiem incidentiem.

   Pienācīgi pamatotos gadījumos un pēc vienošanās ar *CERT-EU* attiecīgā Savienības iestāde, struktūra vai aģentūra var neievērot iepriekšējā daļā norādīto termiņu.

2. Savienības iestādes, struktūras un aģentūras bez liekas kavēšanās *CERT-EU* sniedz papildu paziņojumus par kiberdraudu, ievainojamību un incidentu, ietverot atbilstošu tehnisko informāciju, kas ļauj veikt noteikšanu, reaģēšanu uz incidentiem vai mazināšanas pasākumus. Ja šī informācija ir pieejama, paziņojumā iekļauj:

   (a) attiecīgos aizskāruma rādītājus;

   (b) attiecīgos atklāšanas mehānismus;

   (c) iespējamo ietekmi;

   (d) attiecīgos mazināšanas pasākumus.

3. *CERT-EU* katru mēnesi iesniedz *ENISA* kopsavilkuma ziņojumu, ietverot anonimizētus un apkopotus datus par būtiskiem kiberdraudiem, būtiskām ievainojamībām un būtiskiem incidentiem, kas paziņoti saskaņā ar 1. punktu.

4. IKP drīkst izdot norādījumu dokumentus vai ieteikumus par paziņojuma kārtību un saturu. *CERT-EU* izplata atbilstošo tehnisko informāciju, lai Savienības iestādes, struktūras un aģentūras varētu preventīvi atklāt incidentus, reaģēt uz tiem vai īstenot mazināšanas pasākumus.

5. Paziņošanas pienākumi neattiecas uz ESKI un uz informāciju, ko Savienības iestāde, struktūra vai aģentūra ir saņēmusi no dalībvalsts drošības vai izlūkošanas dienesta vai tiesībaizsardzības iestādes ar skaidru nosacījumu, ka tā netiks kopīgota ar *CERT-EU*.

*21. pants*

***Reaģēšanas uz incidentu koordinēšana un sadarbība būtisku incidentu gadījumā***

1. Rīkojoties kā kiberdrošības informācijas apmaiņas un reaģēšanas uz incidentiem koordinēšanas centrs, *CERT-EU* sekmē informācijas apmaiņu saistībā ar kiberdraudiem, ievainojamībām un incidentiem:

   (a) Savienības iestāžu, struktūru un aģentūru vidū;

   (b) 16. un 17. pantā minēto partneru vidū.

2. *CERT-EU* sekmē Savienības iestāžu, struktūru un aģentūru darba koordinēšanu saistībā ar reaģēšanu uz incidentiem, ietverot:

   (a) ieguldījumu konsekventā ārējā saziņā;

   (b) savstarpējo palīdzību;

   (c) operatīvo resursu optimālu izmantošanu;

   (d) koordinēšanu ar citiem krīzes reaģēšanas mehānismiem Savienības līmenī.

3. *CERT-EU* atbalsta Savienības iestādes, struktūras un aģentūras saistībā ar situācijas apzināšanos attiecībā uz kiberdraudiem, ievainojamībām un incidentiem.

4. IKP sniedz norādījumus par reaģēšanas uz incidentiem koordinēšanu un sadarbību būtisku incidentu gadījumā. Ja ir aizdomas par incidenta noziedzīgo raksturu, *CERT-EU* sniedz padomus, kā par šo incidentu ziņot tiesībaizsardzības iestādēm.

*22. pants*

***Būtiski uzbrukumi***

1. *CERT-EU* koordinē Savienības iestāžu, struktūru un aģentūru reakciju uz būtiskiem uzbrukumiem. Tas uztur tādu tehniskās zinātības portfeli, kas būtu vajadzīga reaģēšanai uz incidentiem šādu uzbrukumu gadījumā.

2. Savienības iestādes, struktūras un aģentūras palīdz veidot tehniskās zinātības portfeli, iesniedzot un katru gadu atjauninot sarakstu ar ekspertiem, kas pieejami to attiecīgajās organizācijās, sīki norādot to konkrētās tehniskās prasmes.

3. Saņemot attiecīgo Savienības iestāžu, struktūru un aģentūru apstiprinājumu, *CERT-EU* drīkst arī aicināt 2. punktā minētajā sarakstā iekļautos ekspertus palīdzēt reaģēt uz būtisku uzbrukumu dalībvalstī atbilstoši Kopējās kibervienības darbības procedūrām.

## VI nodaļa
## NOBEIGUMA NOTEIKUMI

*23. pants*

***Sākotnējā budžeta pārdale***

Komisija rosina darbinieku un finanšu resursu pārdali no attiecīgajām Savienības iestādēm, struktūrām un aģentūrām uz Komisijas budžetu. Pārdale stājas spēkā vienlaikus ar pirmo budžetu, kas pieņemts pēc šīs regulas stāšanās spēkā.

*24. pants*

***Pārskatīšana***

1. IKP ar *CERT-EU* palīdzību periodiski ziņo Komisijai šīs regulas īstenošanu. IKP drīkst arī sniegt Komisijai ieteikumus, kuru mērķis ir rosināt šīs regulas grozījumus.

2. Komisija ne vēlāk kā 48 mēnešus pēc šīs regulas stāšanās spēkā un pēc tam ik pēc trim gadiem ziņo par šīs regulas īstenošanu Eiropas Parlamentam un Padomei.

3. Ne agrāk kā piecus gadus pēc stāšanās spēkā Komisija izvērtē šīs regulas darbību uz ziņo par to Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai.

*25. pants*

***Stāšanās spēkā***

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

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

Briselē,

| | |
|---|---|
| *Eiropas Parlamenta vārdā —* | *Padomes vārdā —* |
| *priekšsēdētāja* | *priekšsēdētājs* |

# TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

## 1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

### 1.1. Priekšlikuma/iniciatīvas nosaukums

### 1.2. Attiecīgā rīcībpolitikas joma

### 1.3. Priekšlikums/iniciatīva attiecas uz:

### 1.4. Mērķi

*1.4.1. Vispārīgie mērķi*

*1.4.2. Konkrētie mērķi*

*1.4.3. Paredzamie rezultāti un ietekme*

*1.4.4. Snieguma rādītāji*

### 1.5. Priekšlikuma/iniciatīvas pamatojums

*1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, tostarp sīki izstrādāts iniciatīvas izvēršanas grafiks*

*1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.*

*1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas*

*1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem*

*1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums*

### 1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

### 1.7. Paredzētie pārvaldības veidi

## 2. PĀRVALDĪBAS PASĀKUMI

### 2.1. Pārraudzības un ziņošanas noteikumi

### 2.2. Pārvaldības un kontroles sistēma

*2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums*

*2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu*

*2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)*

### 2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

## 3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

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

**3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām**

*3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām*

*3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām*

*3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām*

*3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu*

*3.2.5. Trešo personu iemaksas*

**3.3. Aplēstā ietekme uz ieņēmumiem**

# TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

## 1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

### 1.1. Priekšlikuma/iniciatīvas nosaukums

Priekšlikums Eiropas Parlamenta un Padomes regulai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās

### 1.2. Attiecīgā rīcībpolitikas joma

Eiropas publiskā pārvalde

Priekšlikums attiecas uz pasākumiem, kas nodrošina vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās un aģentūrās

### 1.3. Priekšlikums/iniciatīva attiecas uz:

**☑jaunu darbību**

**☐ jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību[10]**

**☐ esošas darbības pagarināšanu**

**☑ vienas vai vairāku darbību apvienošanu vai pārorientēšanu uz citu/jaunu darbību**

### 1.4. Mērķi

*1.4.1. Vispārīgie mērķi*

– Izveidot sistēmu, kas nodrošina vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās un aģentūrās

– Nodrošināt *CERT-EU* jaunu juridisko pamatu, lai pastiprinātu tā pilnvarojumu un palielinātu finansējumu

*1.4.2. Konkrētie mērķi*

(1) Noteikt Savienības iestāžu, struktūru un aģentūru pienākumus izveidot iekšēju kiberdrošības riska pārvaldības, vadības un kontroles sistēmu

(2) Noteikt Savienības iestāžu, struktūru un aģentūru pienākumus ziņot par kiberdrošības riska pārvaldības, vadības un kontroles sistēmu, kā arī par kiberdrošības incidentiem

(3) Noteikt Savienības iestāžu, struktūru un aģentūru kiberdrošības centra (*CERT-EU*) un Iestāžu kiberdrošības padomes (IKP) organizācijas un darbības noteikumus

(4) Atbalstīt Kopējo kibervienību

*1.4.3. Paredzamie rezultāti un ietekme*

*Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz labuma guvējiem / mērķgrupām.*

[10] Kā paredzēts Finanšu regulas 58. panta 2. punkta a) vai b) apakšpunktā.

| |
|---|
| – Iekšējās kiberdrošības riska pārvaldības, vadības un kontroles sistēmas, kiberdrošības pamatparametri, regulāri gatavības novērtējumi un kiberdrošības plāni Savienības iestādēs, struktūrās un aģentūrās<br>– Kiberdrošības noturības un reaģēšanas uz incidentiem spēju uzlabošana Savienības iestādēs, struktūrās un aģentūrās<br>– *CERT-EU* modernizācija<br>– Atbalsts Kopējai kibervienībai |

*1.4.4. Snieguma rādītāji*

*Norādīt, pēc kādiem rādītājiem seko līdzi progresam un sasniegumiem.*

| |
|---|
| – Ieviestas sistēmas un noteikti pamatparametri, regulāri gatavības novērtējumi un kiberdrošības plāni, kas īstenoti Savienības iestādēs, struktūrās un aģentūrās<br>– Labāka rīcība incidentu gadījumos<br>– Labāka izpratne par kiberdrošības riskiem Savienības iestāžu, struktūru un aģentūru augstākās vadības līmenī<br>– Tēriņu par IKT drošību kā noteiktas procentuālās daļas no visiem IKT tēriņiem noteikšana<br>– Spēcīga IKP un *CERT-EU* vadība<br>– Aktīvāka informācijas apmaiņa Savienības iestāžu, struktūru un aģentūru starpā un ar attiecīgajām struktūrām un ieinteresētajām personām ES<br>– Aktīvāka sadarbība kiberdrošības jomā ar attiecīgajām struktūrām un ieinteresētajām personām ES, izmantojot *CERT-EU* un *ENISA* |

## 1.5. Priekšlikuma/iniciatīvas pamatojums

*1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, tostarp sīki izstrādāts iniciatīvas izvēršanas grafiks*

| |
|---|
| Priekšlikuma mērķis ir uzlabot Savienības iestāžu, struktūru un aģentūru kibernoturību, samazināt noturības līmeņa neatbilstības starp šīm vienībās un uzlabot kopīgo situācijas apzināšanās līmeni un kolektīvo spēju sagatavoties un reaģēt.<br>Šis priekšlikums pilnībā atbilst citām saistītām iniciatīvām un ir saskanīgs ar tām, jo īpaši priekšlikumu Direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148 [TID 2 priekšlikums].<br>Priekšlikums ir būtiska daļa no ES Drošības savienības stratēģijas un ES Kiberdrošības stratēģijas digitālajai desmitgadei.<br>Tiek plānots, ka Eiropas Komisija ierosinās šo regulu 2021. gada oktobrī. Gaidāms, ka regulu Eiropas Parlamentā un Padomē pieņems 2022. gadā un ka tās noteikumi būs piemērojami no regulas spēkā stāšanās brīža. Plānots, ka finansiālā ietekme un ietekme uz cilvēkresursiem, kas izklāstīta šajā tiesību akta priekšlikuma finanšu pārskatā, sāksies 2023. gadā. Sagatavošanās periods jau sākās 2021. gadā, bet sagatavošanās darbības 2021. un 2022. gadā nav šā priekšlikuma finanšu ietekmes jomā. |

*1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka*

*rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.*

Eiropas līmeņa rīcības pamatojums (*ex ante*)

Laikā no 2019. līdz 2021. gadam tādu būtisku incidentu skaits, kas skāruši Savienības iestādes, struktūras un aģentūras un ko radījuši paaugstināta pastāvīga apdraudējuma izraisītāji, ir būtiski palielinājies. 2021. gada pirmajā pusē bija tikpat daudz būtisku incidentu kā visā 2020. gadā. To labi atspoguļo kriminālanalīžu (skarto sistēmu vai ierīču satura momentzņēmumi) skaits, ko *CERT-EU* veica 2020. gadā un kas trīskāršojās salīdzinājumā ar 2019. gadu, un kopš 2018. gada būtisko incidentu skaits ir palielinājies par vairāk nekā desmit reizēm.

Dažādās vienībās kiberdrošības gatavības līmenis ievērojami atšķiras[11]. Šī regula nodrošina, ka visas Savienības iestādes, struktūras un aģentūras īsteno drošības pamatpasākumus un sadarbojas savā starpā, lai sasniegtu mērķi nodrošināt atvērtu un efektīvu Savienības administrācijas darbību.

Saglabājamās sistēmas ietilpst Savienības iestāžu, struktūru un aģentūru autonomijā, un tās izmanto Savienības iestādes, struktūras un aģentūras; rosinātās darbības nevarētu izveidot dalībvalstis.

*1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas*

TID direktīva ir pirmais horizontālais iekšējā tirgus instruments, kura mērķis ir uzlabot tīklu un sistēmu noturību Savienībā saistībā ar kiberdrošības riskiem. Kopš tās stāšanās spēkā 2016. gadā direktīva ir palīdzējusi ievērojami uzlabot vispārējo kiberdrošības līmeni dalībvalstīs. TID 2 direktīvas priekšlikuma mērķis ir vēl vairāk uzlabot šos pasākumus.

Regulas mērķis ir noteikt vienādus pasākumus Savienības iestādēm, struktūrām un aģentūrām.

*1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem*

Priekšlikums atbilst daudzgadu finanšu shēmai un ir būtiska daļa no ES Drošības savienības stratēģijas, kā arī ES Kiberdrošības stratēģijas digitālajai desmitgadei.

Ar priekšlikumu paredz piemērot pasākumus, kas nodrošina vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās un aģentūrās. Šis priekšlikums pilnībā atbilst priekšlikumam Direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148 [TID 2 priekšlikums].

*1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums*

Tā kā *CERT-EU* pārvalda uzdevumus, ir vajadzīgas konkrētas zināšanas un pieredze, kā arī papildu darba slodze, ko nevar īstenot bez cilvēkresursu un finanšu resursu palielināšanas.

[11] Atsauce: [*ECA* īpašais ziņojums par kiberdrošību Savienības iestādēs, struktūrās un aģentūrās].

## 1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

☐ **Ierobežots ilgums**

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

– ☐ Finansiālā ietekme uz saistību apropriācijām — no GGGG. līdz GGGG. gadam, uz maksājumu apropriācijām — no GGGG. līdz GGGG. gadam.

☑ **Beztermiņa**

– Finansiālo ietekmi būtu jāsāk just, pieņemot pirmo budžetu pēc regulas stāšanās spēkā. Resursu pārdale no Savienības iestādēm un Komisijas galvenajām struktūrām notiktu pirmajā gadā, ko uzskata par pārejas gadu; šī un citas resursu piešķiršanas (pārdales) notiks ikgadējā budžeta ietvarā. Ja regula tiks pieņemta 2022. gadā, 2023. finanšu gads būs pārejas periods, bet 2024. gadā notiks pilnvērtīga darbība.

## 1.7. Paredzētie pārvaldības veidi[12]

☑ Komisijas un katras Savienības iestādes, struktūras un aģentūras īstenota **tieša pārvaldība**:

– ☑ ko veic tās struktūrvienības, tostarp personāls Savienības delegācijās;

– ☐ ko veic izpildaģentūras.

☐ **Dalīta pārvaldība** kopā ar dalībvalstīm

☐ **Netieša pārvaldība**, kurā budžeta izpildes uzdevumi uzticēti:

– ☐ trešām valstīm vai to izraudzītām struktūrām;

– ☐ starptautiskām organizācijām un to aģentūrām (precizēt);

– ☐ EIB un Eiropas Investīciju fondam;

– ☐ Finanšu regulas 70. un 71. pantā minētajām struktūrām;

– ☐ publisko tiesību subjektiem;

– ☐ privāttiesību subjektiem, kas veic sabiedrisko pakalpojumu sniedzēju uzdevumus, tādā mērā, kādā tiem ir pienācīgas finanšu garantijas;

– ☐ dalībvalstu privāttiesību subjektiem, kuriem ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuri sniedz pienācīgas finanšu garantijas;

– ☐ personām, kurām, ievērojot Līguma par Eiropas Savienību V sadaļu, uzticēts īstenot konkrētas KĀDP darbības un kuras ir noteiktas attiecīgajā pamataktā.

– *Ja norādīti vairāki pārvaldības veidi, sniedziet papildu informāciju iedaļā "Piezīmes".*

Piezīmes

| |
|---|
| Administratīvo un finanšu procedūru piemērošanā *CERT-EU* darbojas Komisijas pakļautībā. |
| Papildu resursi, kas izriet no regulas projekta |
| Regulas projekta 12. un 13. panta īstenošanas rezultātā ir plašāks pakalpojumu katalogs ar papildu pamatpakalpojumiem. Darbojoties ar pilnu jaudu, būs vajadzīgi tālāk norādītie |

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

papildu resursi (līdz DFS beigām 2027. gada beigās): 21 pilnslodzes ekvivalents (*FTE*) un 14,05 miljoni EUR.

Budžetā paredzēto papildu resursu sadalījums dažādiem uzdevumiem ir šāds:

(a) tādu uzdevumu veikšanai Savienības iestāžu, struktūru un aģentūru vajadzībām, kas sīki izklāstīti 12. panta 2. punkta a), b), c) un e) apakšpunktā: 13,75 *FTE* un 11,275 miljoni EUR;

(b) 12. panta 3. punktā sīki izklāstīto uzdevumu veikšanai (atbalsts Kopējai kibervienībai): 2 *FTE* un 381 000 EUR;

(c) 12. panta 4. punktā sīki izklāstīto uzdevumu veikšanai (strukturēta sadarbība ar *ENISA*): 0,25 *FTE* un 236 000 EUR;

(d) 12. panta 6. punktā sīki izklāstīto uzdevumu veikšanai (kiberdrošības mācības): 0,25 *FTE* un 79 000 EUR;

(e) 12. panta 2. punkta d) apakšpunktā un 13. pantā sīki izklāstīto uzdevumu veikšanai (analīze un ziņošana par regulas īstenošanu, norādījumu dokumentu, ieteikumu un aicinājumu rīkoties sagatavošana): 3,75 *FTE* un 2,079 miljoni EUR;

(f) tādu uzdevumu veikšanai, ar ko atbalsta Iestāžu kiberdrošības padomes (IKP) sekretariātu: 1 *FTE*.

Pašreizējo resursu pārskats un pāreja uz darbību ar pilnu jaudu:

2021. gada septembrī *CERT-EU* darbojās, izmantojot šādus resursus:

— pastāvīgie un norīkotie darbinieki: 14 *FTE*,

— līgumdarbinieki, ko finansē saskaņā ar pakalpojumu līmeņa nolīgumiem: 24 *FTE*,

— kopā 38 *FTE*.

2020. gadā *CERT-EU* budžets bija: 250 000 EUR no Komisijas budžeta, 3,5 miljoni EUR piešķirto ieņēmumu no pakalpojumu līmeņa nolīgumiem. Kopā: 3,75 miljoni EUR. Tas bija kopējais *CERT-EU* budžets, kas ietvēra apmācību, aparatūru, programmatūru, misijas, atbalstu, līgumdarbiniekus un konferences.

Kad regula stāsies spēkā, plānots, ka *CERT-EU* resursi būs:

— pastāvīgie darbinieki: 34 *FTE*,

— līgumdarbinieki: 15 *FTE*,

— kopā 49 *FTE*, tādējādi neto palielinājums ir 11 *FTE*.

Izmaiņas pastāvīgo amata vietu un līgumdarbinieku attiecībā novērš būtisku traucēkli, proti, augstāka līmeņa kiberdrošības speciālistu nolīgšanu un paturēšanu darbā saistībā ar to trūkumu darba tirgū.

Turklāt 1 *FTE* līgumdarbinieks būs vajadzīgs Komisijas Informātikas ģenerāldirektorātā, un viņa uzdevums būs atbalstīt IKP (Iestāžu kiberdrošības padomi).

Tādējādi regulas īstenošanai kopā būs vajadzīgs 21 *FTE* (20 *FTE CERT-EU* un 1 *FTE* Komisijas Informātikas ģenerāldirektorātam). To kompensēs paralēls samazinājums par 9 *FTE* līgumdarbiniekiem *CERT-EU*; tos iepriekš finansēja ar piešķirtajiem ieņēmumiem no pakalpojumu līmeņa nolīgumiem.

Pēc pārejas perioda *CERT-EU* 2024. gada budžets, kas neietver cilvēkresursus, aptvers uzdevumus, kas iepriekš norādīti a)–e) apakšpunktā, un to paredzēts finansēt šādi:

— 8,921 miljons EUR gadā no Savienības iestādēm, ko finansē no Savienības budžeta 7. izdevumu kategorijas,

— 2,459 miljoni EUR no Savienības iestādēm, struktūrām un aģentūrām, ko finansē no Savienības budžeta 1.–6. izdevumu kategorijas,

— 2,670 miljoni EUR no pašfinansētām Savienības iestādēm, struktūrām un aģentūrām,

— kopējais *CERT-EU* budžets: 14,05 miljoni EUR.

Regulas 12. panta 5. punktā uzskaitītie uzdevumi nav aprakstīti pakalpojumu katalogā, tie ir maksas pakalpojumi. Tie ir papildpakalpojumi, to summa ir relatīvi zema, tie lielākoties ir pagaidu pakalpojumi, un šo pakalpojumu izmaksas sedz pakalpojumu saņēmēji atbilstoši pakalpojumu līmeņa nolīgumiem vai rakstveida nolīgumiem.

Attiecībā uz maksājumiem *CERT-EU* darbiniekiem: Savienības iestādes un galvenās struktūras sedz taisnīgu daļu, kas atbilst to attiecīgajai organizācijas pastāvīgo *AD* kategorijas darbinieku daļai. Būtu jānoskaidro, vai ECB un EIB arī var sniegt taisnīgu ieguldījuma daļu, norīkojot pastāvīgos darbiniekus.

## 2. PĀRVALDĪBAS PASĀKUMI

### 2.1. Pārraudzības un ziņošanas noteikumi

*Norādīt biežumu un nosacījumus.*

Komisija ar IKP un *CERT-EU* palīdzību periodiski pārskatīs regulas darbību un ziņos Eiropas Parlamentam un Padomei; pirmo reizi tas notiks ne vēlāk kā 48 mēnešus pēc šīs regulas stāšanās spēkā un pēc tam reizi trīs gados.

Pārskatīšanai izmantotie datu avoti galvenokārt būtu no IKP un *CERT-EU*. Turklāt, ja nepieciešams, būtu jāizmanto arī konkrēti datu vākšanas rīki, piemēram, Savienības iestāžu, struktūru un aģentūru, *ENISA* vai *CSIRT* tīkla apsekojumi.

### 2.2. Pārvaldības un kontroles sistēma

*2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums*

No šīs regulas izrietošās darbības pārvaldīs katrā Savienības iestādē, struktūrā un aģentūrā atbilstoši to attiecīgajiem piemērojamajiem noteikumiem.

*CERT-EU* darbību administratīvā un finansiālā pārvaldība ir iekļauta Komisijas vadībā un atbilst tās pārvaldības un īstenošanas mehānismiem, maksājumu kārtībai un kontroles pasākumiem.

Komisijas iekšējam revidentam *CERT-EU* ir tādas pašas pilnvaras kā Komisijas dienestos.

*2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu*

Ļoti mazs risks, jo *CERT-EU* kā Komisijas darba grupa jau ir administratīvi saistīta ar informātikas ģenerāldirektoru, un IKP darbojas līdzīgi kā pašreizējā *CERT-EU* koordinācijas padome. Tāpēc finanšu pārvaldības un iekšējās kontroles ekosistēma jau ir izveidota.

*2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)*

Iepirkumu, finanšu pārvaldības un kontroles procedūras jau ir īstenotas un pienācīgi pārbaudītas. Kontroles izmaksu lietderība un kļūdu rašanās riska līmenis atbilst attiecīgiem rādītājiem katrā Savienības iestādē, struktūrā vai aģentūrā, kā arī Komisijas rādītājiem saistībā ar *CERT-EU* darbībām.

### 2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

*Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.*

*CERT-EU* darbībām piemēro Komisijas finanšu pārvaldības un iekšējās kontroles sistēmas.

Lai apkarotu krāpšanu, korupciju un citas nelikumīgas darbības, Eiropas Parlamenta un Padomes 2013. gada 11. septembra Regulas (ES, Euratom) Nr. 883/2013 par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*), noteikumi piemērojami bez ierobežojuma.

## 3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

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

- Esošās budžeta pozīcijas

*<u>Sarindotas</u> pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām*

| Daudzgadu finanšu shēmas izdevumu kategorija | Budžeta pozīcija | Izdevumu veids | Iemaksas | | | |
|---|---|---|---|---|---|---|
| | Nr. | Dif./nedif. [13] | no EBTA valstīm[14] | no kandidātvalstīm[15] | no trešām valstīm | Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē |
| 1–6 | Budžeta pozīcijas, kas ietver Savienības maksājumus decentralizētām aģentūrām un struktūrām | Dif. | NĒ | NĒ | NĒ | NĒ |
| 7 | Budžeta pozīcijas, kas ietver darbinieku atalgojumu, IT izdevumus un citus administratīvus izdevumus dažādās ES budžeta iedaļās | Nedif. | NĒ | NĒ | NĒ | NĒ |

- Jaunveidojamās budžeta pozīcijas

*<u>Sarindotas</u> pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām*

| Daudzgadu finanšu shēmas izdevumu kategorija | Budžeta pozīcija | Izdevumu veids | Iemaksas | | | |
|---|---|---|---|---|---|---|
| | Nr. | Dif./nedif. | no EBTA valstīm | no kandidātvalstīm | no trešām valstīm | Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē |
| | Nav | | JĀ/NĒ | JĀ/NĒ | JĀ/NĒ | JĀ/NĒ |

[13] Dif. — diferencētās apropriācijas, nedif. — nediferencētās apropriācijas.
[14] EBTA: Eiropas Brīvās tirdzniecības asociācija.
[15] Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

### 3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

*3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām*

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgas darbības apropriācijas

– ☑ Priekšlikumam/iniciatīvai ir vajadzīgas šādas darbības apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

| **Daudzgadu finanšu shēmas izdevumu kategorija** | 1–6 | Izdevumu kategorijas, kas ietver maksājumus decentralizētām aģentūrām un struktūrām |
|---|---|---|

| ĢD: vairāki | | | **2023. gads** | **2024. gads** | **2025. gads** | **2026. gads** | **2027. gads** | **KOPĀ** |
|---|---|---|---|---|---|---|---|---|
| ○ Darbības apropriācijas | | | | | | | | |
| Budžeta pozīcijas, kas ietver Savienības maksājumus decentralizētām aģentūrām (xx 10 xx xx)[16] | Saistības | (1a) | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| | Maksājumi | (2a) | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem[17] | | | | | | | | |
| Budžeta pozīcija | | (3) | | | | | | |
| **KOPĀ apropriācijas ĢD: vairāki** | Saistības | = 1a + 1b + 3 | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| | Maksājumi | = 2a + 2b +3 | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |

[16] Saskaņā ar oficiālo budžeta nomenklatūru.

[17] Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās *BA* pozīcijas), netiešā pētniecība, tiešā pētniecība.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ○ KOPĀ darbības apropriācijas | Saistības | (4) | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| | Maksājumi | (5) | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| ○ KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem | | (6) | | | | | | |
| **KOPĀ** daudzgadu finanšu shēmas **1.–6. IZDEVUMU KATEGORIJAS apropriācijas** | Saistības | = 4 + 6 | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| | Maksājumi | = 5 + 6 | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |

**<u>Ja priekšlikums/iniciatīva ietekmē vairāk nekā vienu darbības izdevumu kategoriju, atkārtot iepriekš minēto iedaļu:</u>**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ○ KOPĀ darbības apropriācijas (visas darbības izdevumu kategorijas) | Saistības | (4) | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| | Maksājumi | (5) | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem (visas darbības izdevumu kategorijas) | | (6) | | | | | | |
| **KOPĀ** daudzgadu finanšu shēmas **1.–6. IZDEVUMU KATEGORIJAS apropriācijas** (atsauces summa) | Saistības | = 4 + 6 | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |
| | Maksājumi | = 5 + 6 | 2,459 | 2,459 | 2,459 | 2,459 | 2,459 | 12,293 |

| | | |
|---|---|---|
| **Daudzgadu finanšu shēmas izdevumu kategorija** | **7** | "Administratīvie izdevumi" |

Šī iedaļa būtu jāaizpilda, izmantojot administratīva rakstura budžeta datu izklājlapu, kas vispirms jānoformē tiesību akta finanšu pārskata pielikumā (iekšējo noteikumu V pielikums), kurš starpdienestu konsultāciju vajadzībām tiek augšupielādēts sistēmā *DECIDE*.

miljonos EUR (trīs zīmes aiz komata)

| | | **2023. gads** | **2024. gads** | **2025. gads** | **2026. gads** | **2027. gads** | **KOPĀ** |
|---|---|---|---|---|---|---|---|
| ĢD: *DIGIT* (*CERT-EU*) | | | | | | | |
| ○ Cilvēkresursi | | 1,184 | 2,126 | 2,754 | 3,225 | 3,225 | 12,514 |
| ○ Citi administratīvie izdevumi | | 7,938 | 8,921 | 8,921 | 8,921 | 8,921 | 43,622 |
| **KOPĀ *DIGIT* ĢD(*CERT-EU*)** | Apropriācijas | 9,122 | 11,047 | 11,675 | 12,146 | 12,146 | 56,136 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **KOPĀ** daudzgadu finanšu shēmas **7. IZDEVUMU KATEGORIJAS apropriācijas** | (Saistību summa = maksājumu summa) | 9,122 | 11,047 | 11,675 | 12,146 | 12,146 | **56,136** |

miljonos EUR (trīs zīmes aiz komata)

| | | 2023. gads | 2024. gads | 2025. gads | 2026. gads | 2027. gads | **KOPĀ** |
|---|---|---|---|---|---|---|---|
| **KOPĀ** daudzgadu finanšu shēmas **1.–7. IZDEVUMU KATEGORIJAS apropriācijas** (*) | Saistības | 11,581 | 13,506 | 14,134 | 14,605 | 14,605 | 68,429 |
| | Maksājumi | 11,581 | 13,506 | 14,134 | 14,605 | 14,605 | 68,429 |

(*) Lēstās iemaksas no pašfinansētajām Savienības iestādēm, struktūrām un aģentūrām ir 2,670 miljoni EUR gadā (par pieciem gadiem kopā 13,350 miljoni EUR). Šīs iemaksas tiks uzskatītas par *CERT-EU* piešķirtajiem ieņēmumiem. Iepriekš norādītajās tabulās ir iekļauta tikai lēstā kopējā ietekme uz Savienības budžetu un nav iekļautas šīs iemaksas.

*3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām*

Saistību apropriācijas miljonos EUR (trīs zīmes aiz komata)

| **Norādīt mērķus un iznākumus** | | | **N gads** | | **N+1 gads** | | **N+2 gads** | | **N+3 gads** | | Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu) | | | | | | **KOPĀ** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **IZNĀKUMI** | | | | | | | | | | | | | | | | | |
| ⇩ | Veids [18] | Vidējais izmaksas | Daudzums | Izmaksas | Daudzums | Izmaksas | Daudzums | Izmaksas | Daudzums | Izmaksas | Daudzums | Izmaksas | Daudzums | Izmaksas | Daudzums | Izmaksas | Kopējais daudzums | Kopējās izmaksas |
| KONKRĒTAIS MĒRĶIS Nr. 1[19]… | | | | | | | | | | | | | | | | | | |
| — Iznākums | | | | | | | | | | | | | | | | | | |
| — Iznākums | | | | | | | | | | | | | | | | | | |
| — Iznākums | | | | | | | | | | | | | | | | | | |
| Starpsumma — konkrētais mērķis Nr. 1 | | | | | | | | | | | | | | | | | | |
| KONKRĒTAIS MĒRĶIS Nr. 2 ... | | | | | | | | | | | | | | | | | | |
| — Iznākums | | | | | | | | | | | | | | | | | | |
| Starpsumma — konkrētais mērķis Nr. 2 | | | | | | | | | | | | | | | | | | |
| **KOPSUMMAS** | | | | | | | | | | | | | | | | | | |

[18] Iznākumi ir attiecīgie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

[19] Konkrētie mērķi, kas norādīti 1.4.2. punktā "Konkrētie mērķi".

*3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām*

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgas administratīvās apropriācijas

– ☑ Priekšlikumam/iniciatīvai ir vajadzīgas šādas administratīvās apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

| | 2023. gads | 2024. gads | 2025. gads | 2026. gads | 2027. gads | **KOPĀ** |
|---|---|---|---|---|---|---|
| **Daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA** | | | | | | |
| Cilvēkresursi | | | | | | |
| Pastāvīgi darbinieki (*AD* kategorija) | 1,099 | 2,041 | 2,669 | 3,14 | 3,14 | 12,089 |
| Līgumdarbinieki | 0,085 | 0,085 | 0,085 | 0,085 | 0,085 | 0,425 |
| Citi administratīvie izdevumi | 7,938 | 8,921 | 8,921 | 8,921 | 8,921 | 43,622 |
| **Starpsumma — daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA** | 9,122 | 11,047 | 11,675 | 12,146 | 12,146 | 56,136 |
| **Ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS[20]** | | | | | | |
| Cilvēkresursi | | | | | | |
| Pārējie administratīvie izdevumi | | | | | | |
| **Starpsumma — ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS** | | | | | | |
| **KOPĀ** | 9,122 | 11,047 | 11,675 | 12,146 | 12,146 | 56,136 |

Vajadzīgās cilvēkresursu un citu administratīvu izdevumu apropriācijas tiks nodrošinātas no ĢD apropriācijām, kas jau ir piešķirtas darbības pārvaldībai un/vai ir pārdalītas attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

[20] Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās *BA* pozīcijas), netiešā pētniecība, tiešā pētniecība.

3.2.3.1. Aplēstās cilvēkresursu vajadzības

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgi cilvēkresursi

– ☑ Priekšlikumam/iniciatīvai ir vajadzīgi šādi cilvēkresursi:

*Aplēse izsakāma ar pilnslodzes ekvivalentu*

| | | 2023. gads | 2024. gads | 2025. gads | 2026. gads | 2027. gads | | |
|---|---|---|---|---|---|---|---|---|
| **O Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)** | | | | | | | | |
| 20 01 02 01 (Galvenā mītne un Komisijas pārstāvniecības) | | 7 | 13 | 17 | 20 | 20 | | |
| 20 01 02 03 (Delegācijas) | | | | | | | | |
| 01 01 01 01 (Netiešā pētniecība) | | | | | | | | |
| 01 01 01 11 (Tiešā pētniecība) | | | | | | | | |
| Citas budžeta pozīcijas (norādīt) | | | | | | | | |
| **OĀrštata darbinieki (izsakot ar pilnslodzes ekvivalentu *FTE*)[21]** | | | | | | | | |
| 20 02 01 (*AC*, *END*, *INT*, ko finansē no vispārīgajām apropriācijām) | | 1 | 1 | 1 | 1 | 1 | | |
| 20 02 03 (*AC*, *AL*, *END*, *INT* un JED delegācijās) | | | | | | | | |
| **XX** 01 xx **yy zz** [22] | — galvenajā mītnē | | | | | | | |
| | — delegācijās | | | | | | | |
| 01 01 01 02 (*AC*, *END*, *INT* — netiešā pētniecība) | | | | | | | | |
| 01 01 01 12 (*AC*, *END*, *INT* — tiešā pētniecība) | | | | | | | | |
| Citas budžeta pozīcijas (norādīt) | | | | | | | | |
| **KOPĀ** | | **8** | **14** | **18** | **21** | **21** | | |

**XX** ir attiecīgā politikas joma vai budžeta sadaļa.

Nepieciešamie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts:

| | |
|---|---|
| Ierēdņi un pagaidu darbinieki | Ierēdņi pilda *CERT-EU* uzdevumus un īsteno darbības atbilstoši regulai, jo īpaši tās IV un V nodaļai. |
| Ārštata darbinieki | Līgumdarbinieki palīdz ar sekretariāta funkciju izpildi Iestāžu kiberdrošības padomē. |

[21] *AC* = līgumdarbinieki, *AL* — vietējie darbinieki, *END* — valstu norīkotie eksperti, *INT* — aģentūru darbinieki, JED — jaunākie eksperti delegācijās.

[22] Ārštata darbiniekiem paredzēto maksimālo summu finansē no darbības apropriācijām (kādreizējām *BA* pozīcijām).

*3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu*

Priekšlikuma/iniciatīvas finansēšanai:

– ☑ pilnībā pietiek ar līdzekļu pārvietošanu daudzgadu finanšu shēmas (DFS) attiecīgajā izdevumu kategorijā

| |
|---|
| Aprakstiet, kas jāpārplāno, norādot attiecīgās budžeta pozīcijas un summas. Lielas pārplānošanas gadījumā sniedziet *Excel* tabulu. |

– ☐ jāizmanto no DFS attiecīgās izdevumu kategorijas nepiešķirtās rezerves un/vai īpašie instrumenti, kas noteikti DFS regulā

| |
|---|
| Paskaidrojiet, kas jādara, norādot attiecīgās izdevumu kategorijas un budžeta pozīcijas, atbilstošās summas un instrumentus, kurus ierosināts izmantot. |

– ☐ jāpārskata DFS.

| |
|---|
| Paskaidrojiet, kas jādara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un atbilstošās summas. |

*3.2.5. Trešo personu iemaksas*

Priekšlikums/iniciatīva:

– ☑ neparedz trešo personu līdzfinansējumu[23]

– ☐ paredz trešo personu sniegtu līdzfinansējumu atbilstoši šādai aplēsei:

Apropriācijas miljonos EUR (trīs zīmes aiz komata)

| | **N** gads[24] | **N+1** gads | **N+2** gads | **N+3** gads | Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu) | | | Kopā |
|---|---|---|---|---|---|---|---|---|
| Norādīt līdzfinansētāju struktūru | | | | | | | | |
| KOPĀ līdzfinansētās apropriācijas | | | | | | | | |

[23] Piešķirtie ieņēmumi, kas izriet no pakalpojumu neregulāras sniegšanas tvērumā neietilpstošām organizācijām un kas paredzēti 12. panta 5. punkta c) apakšpunktā, nav aprēķināti, jo tiem vajadzētu būt niecīgiem.

[24] N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, 2021.). Tas pats attiecas uz turpmākajiem gadiem.

### 3.3. Aplēstā ietekme uz ieņēmumiem

– ☑ Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus.

– ☐ Priekšlikums/iniciatīva finansiāli ietekmē:

– ☐ pašu resursus

– ☐ citus ieņēmumus

– atzīmējiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām ☐

miljonos EUR (trīs zīmes aiz komata)

| Budžeta ieņēmumu pozīcija: | Kārtējā finanšu gadā pieejamās apropriācijas | Priekšlikuma/iniciatīvas ietekme[25] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **N** gads | **N+1** gads | **N+2** gads | **N+3** gads | Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu) | | |
| ……. pants | | | | | | | | |

Attiecībā uz piešķirtajiem ieņēmumiem norādīt attiecīgās budžeta izdevumu pozīcijas.

Citas piezīmes (piemēram, metode/formula, ko izmanto, lai aprēķinātu ietekmi uz ieņēmumiem, vai jebkura cita informācija).

[25] Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.