Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2023/2841

18.12.2023.

EIROPAS PARLAMENTA UN PADOMES REGULA (ES, Euratom) 2023/2841

(2023. gada 13. decembris),

kas paredz pasākumus nolūkā panākt vienādu augstu kiberdrošības līmeni 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 ([1]),

tā kā:

(1) Digitālajā laikmetā informācijas un komunikācijas tehnoloģijas ir atvērtas, efektīvas un neatkarīgas Eiropas administrācijas stūrakmens. Tehnoloģiju attīstība un pieaugusī digitālo sistēmu sarežģītība un starpsavienotība palielina kiberdrošības riskus, padarot Savienības vienības neaizsargātākas pret kiberdraudiem un incidentiem, un tas apdraud vienību darbības nepārtrauktību un spēju droši glabāt savus datus. Pieaugusī mākoņpakalpojumu izmantošana, informācijas un komunikācijas tehnoloģiju (IKT) izmantošana visās dzīves jomās, augstā digitalizācijas pakāpe, attālinātais darbs un tehnoloģiju un savienotības attīstība ir visu Savienības vienību darbību pamatiezīmes, tomēr digitālā noturība šajās darbībās vēl nav pietiekami integrēta.

(2) Kiberdraudi, ar ko saskaras Savienības vienības, pastāvīgi attīstās. Apdraudētāju izmantotā taktika, paņēmieni un procedūras pastāvīgi attīstās, bet šādu uzbrukumu galvenie motīvi ir gandrīz nemainīgi – nozagt vērtīgu, neizpaustu informāciju, iegūt naudu, manipulēt ar sabiedrisko domu vai apdraudēt digitālo infrastruktūru. Apdraudētāju kiberuzbrukumu biežums palielinās, un to kampaņas kļūst aizvien sarežģītākas un automatizētākas, vēršas pret atklātiem uzbrukuma punktiem, kas arvien paplašinās, un ātri izmanto ievainojamības.

(3) Savienības vienību IKT vidēm ir raksturīga savstarpēja atkarība un tajās ir integrētas datu plūsmas, un to lietotāji cieši sadarbojas. Minētā starpsavienotība nozīmē, ka jebkurš traucējums – pat tad, ja tas sākotnēji rodas tikai vienā Savienības vienībā, – var kļūt plašāks, iespējams, radot tālejošas un ilgas negatīvas sekas citām Savienības vienībām. Turklāt noteiktu Savienības vienību IKT vides ir savienotas ar dalībvalstu IKT vidēm, attiecīgi, ja vienā Savienības vienībā notiek incidents, tas rada kiberdrošības risku dalībvalstu IKT vižu kiberdrošībai, kā arī otrādi. Dalīšanās informācijā par incidentu var palīdzēt atklāt līdzīgus kiberdraudus vai incidentus, kas skar dalībvalstis.

(4) Savienības vienības ir pievilcīgs mērķis ļoti prasmīgiem apdraudētājiem, kuriem ir daudz resursu, kā arī citiem apdraudējumiem. Vienlaikus minētajām vienībām ir ļoti atšķirīga līmeņa un gatavības pakāpes kibernoturība un spēja atklāt ļaunprātīgas kiberdarbības un reaģēt uz tām. Tāpēc Savienības vienību darbībai ir nepieciešams vienāds augsts kiberdrošības līmenis, kas jāsasniedz, īstenojot kiberdrošības pasākumus, kuri ir samērīgi ar identificētajiem kiberdrošības riskiem, kā arī izmantojot informācijas apmaiņu un sadarbību.

([1]) Eiropas Parlamenta 2023. gada 21. novembra nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2023. gada 8. decembra lēmums.

(5) Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2555 ([2]) mērķis ir vēl vairāk uzlabot publisko un privāto vienību, kompetento iestāžu un struktūru un Savienības kopējo kibernoturību un spēju reaģēt uz incidentiem. Tāpēc ir jānodrošina, ka Savienības vienības seko šim piemēram, paredzot noteikumus, kas atbilst Direktīvai (ES) 2022/2555 un tās vērienīguma līmenim.

(6) Lai panāktu vienādu augstu kiberdrošības līmeni, katrai Savienības vienībai jāizveido iekšējs kiberdrošības riska pārvaldības, pārvaldes un kontroles satvars ("satvars"), kas nodrošinātu iedarbīgu un piesardzīgu visu kiberdrošības risku pārvaldību, kā arī ņemtu vērā darbības nepārtrauktību un krīzes pārvaldību. Satvaram būtu jānosaka kiberdrošības rīcībpolitikas, tostarp mērķi un prioritātes, tīklu un informācijas sistēmu drošībai, aptverot visu neklasificēto IKT vidi. Satvara pamatā vajadzētu būt visu apdraudējumu pieejai, kuras mērķis ir aizsargāt tīklu un informācijas sistēmas un šo sistēmu fizisko vidi pret tādiem notikumiem kā zādzība, ugunsgrēks, plūdi, telesakaru vai elektroenerģijas padeves traucējumi vai neatļauta fiziska piekļuve un kaitējums Savienības vienības informācijas un informācijas apstrādes iekārtām un iejaukšanās tajās, kas varētu apdraudēt tādu datu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus glabā, pārsūta, apstrādā vai kuriem var piekļūt, izmantojot tīklu un informācijas sistēmas.

(7) Lai pārvaldītu satvarā identificētos kiberdrošības riskus, katrai Savienības vienībai būtu jāveic piemēroti un samērīgi tehniskie, operacionālie un organizatoriskie pasākumi. Minētajiem pasākumiem būtu jāpievēršas jomām un kiberdrošības riska pārvaldības pasākumiem, ko paredz šī regula, lai stiprinātu katras Savienības vienības kiberdrošību.

(8) Satvarā identificētie aktīvi un kiberdrošības riski, kā arī secinājumi, kuri izriet no regulāriem kiberdrošības gatavības novērtējumiem, būtu jāatspoguļo kiberdrošības plānā, kas būtu jāizstrādā katrai Savienības vienībai. Kiberdrošības plānā būtu jāiekļauj pieņemtie kiberdrošības riska pārvaldības pasākumi.

(9) Tā kā kiberdrošības nodrošināšana ir nepārtraukts process, saskaņā ar šo regulu pieņemto pasākumu piemērotība un iedarbīgums būtu regulāri jāizskata, ņemot vērā Savienības vienību mainīgos kiberdrošības riskus, aktīvus un kiberdrošības gatavību. Satvars būtu jāpārskata regulāri un vismaz ik četrus gadus, savukārt kiberdrošības plāns būtu jāpārskata ik divus gadus vai biežāk, ja nepieciešams, pēc kiberdrošības gatavības novērtējuma vai jebkādas būtiskas satvara pārskatīšanas.

(10) Savienības vienību ieviestajos kiberdrošības riska pārvaldības pasākumos būtu jāiekļauj rīcībpolitikas, kuru mērķis ir, ja iespējams, padarīt pārredzamu pirmkodu, ņemot vērā aizsardzības pasākumus trešo pušu vai Savienības vienību tiesībām. Minētajām rīcībpolitikām vajadzētu būt samērīgām ar kiberdrošības risku, un to mērķis ir atvieglot kiberdraudu analīzi, vienlaikus neradot pienākumu izpaust informāciju vai tiesības piekļūt trešās puses kodam, kas sniegtos pāri piemērojamo līguma noteikumu robežām.

(11) Atvērtā pirmkoda kiberdrošības rīki un lietotnes var veicināt lielāku atvērtību. Atvērtie standarti veicina drošības rīku sadarbspēju, tādējādi labvēlīgi ietekmējot ieinteresēto personu drošību. Atvērtā pirmkoda kiberdrošības rīki un lietotnes var mobilizēt izstrādātāju kopienu kopumā, darot iespējamu piegādātāju dažādošanu. Atvērtā pirmkoda izmantošana var pavērt ceļu pārredzamākai ar kiberdrošību saistītu rīku verifikācijai un kopienas virzītai ievainojamības atklāšanai. Tādēļ Savienības vienībām būtu jāspēj veicināt atvērtā pirmkoda programmatūras un atvērto standartu izmantošanu, īstenojot rīcībpolitikas attiecībā uz atvērto datu un atvērtā pirmkoda izmantošanu kā daļu no drošības, ko panāk ar pārredzamību.

([2]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

(12) Tā kā Savienības vienību vidū pastāv atšķirības, ir vajadzīga šīs regulas elastīga īstenošana. Šajā regulā paredzētajiem vienāda augsta kiberdrošības līmeņa panākšanas pasākumiem nebūtu jāietver pienākumi, kas tieši traucētu Savienības vienību misijas īstenošanai vai mazinātu to institucionālo autonomiju. Tāpēc minētajām vienībām būtu jāizveido pašām savi satvari un jāpieņem savi kiberdrošības risku pārvaldības pasākumi un kiberdrošības plāni. Īstenojot šādus pasākumus, būtu pienācīgi jāņem vērā starp Savienības vienībām pastāvošās sinerģijas, lai nodrošinātu pareizu resursu pārvaldību un izmaksu optimizāciju. Būtu arī pienācīgi jāraugās, lai pasākumi negatīvi neietekmētu efektīvu informācijas apmaiņu un sadarbību starp Savienības vienībām un partneriem dalībvalstīs.

(13) Lai optimizētu resursu izmantošanu, šai regulai būtu jāparedz iespēja divām vai vairākām Savienības vienībām ar līdzīgu struktūru sadarboties savu attiecīgo vienību kiberdrošības gatavības novērtēšanā.

(14) Lai izvairītos no nesamērīga finansiāla un administratīva sloga radīšanas Savienības vienībām, kiberdrošības riska pārvaldības prasībām vajadzētu būt samērīgām ar kiberdrošības risku, kas radīts attiecīgajām tīklu un informācijas sistēmām, ņemot vērā jaunākos sasniegumus šādu pasākumu jomā. Ikvienai Savienības vienībai vajadzētu tiekties piešķirt pienācīgu sava IKT budžeta daļu kiberdrošības līmeņa uzlabošanai. Ilgtermiņā būtu jācenšas sasniegt vismaz indikatīvu 10 % mērķrādītāju. Kiberdrošības gatavības novērtējumā būtu jāizvērtē, vai Savienības vienības kiberdrošības izdevumi ir samērīgi ar kiberdrošības riskiem, ar kuriem tā saskaras. Neskarot Līgumos paredzētos noteikumus par Savienības gada budžetu, Komisijai, novērtējot Savienības vienību budžeta un personāla vajadzības, kas izriet no to izdevumu tāmēm, savā priekšlikumā par pirmo gada budžetu, kurš jāpieņem pēc šīs regulas stāšanās spēkā, būtu jāņem vērā pienākumi, kas izriet no šīs regulas.

(15) Lai panāktu vienādu augstu kiberdrošības līmeni, šī joma jāpārrauga ikvienas Savienības vienības visaugstākā līmeņa vadībai. Savienības vienības visaugstākā līmeņa vadībai vajadzētu būt atbildīgai par šīs regulas īstenošanu, tostarp par satvara izveidi, kiberdrošības risku pārvaldības pasākumu veikšanu un kiberdrošības plāna apstiprināšanu. Kiberdrošības kultūras jautājums, proti, kiberdrošības ikdienas prakse, ir neatņemama satvara un attiecīgo kiberdrošības riska pārvaldības pasākumu daļa visās Savienības vienībās.

(16) Būtiski svarīga ir to tīklu un informācijas sistēmu drošība, kuras rīkojas ar ES klasificēto informāciju (ESKI). Savienības vienībām, kas rīkojas ar ESKI, ir jāpiemēro visaptverošais tiesiskais regulējums, kas ir ieviests, lai šādu informāciju aizsargātu, tostarp īpašu pārvaldību, rīcībpolitikas un riska pārvaldības procedūras. Tīklu un informācijas sistēmām, kuras rīkojas ar ESKI, ir jāatbilst stingrākiem drošības standartiem nekā neklasificētām tīklu un informācijas sistēmām. Tāpēc tīklu un informācijas sistēmas, kas rīkojas ar ESKI, ir noturīgākas pret kiberdraudiem un incidentiem. Līdz ar to, atzīstot, ka šajā sakarā ir vajadzīgs vienots satvars, šī regula nebūtu jāpiemēro tīklu un informācijas sistēmām, kuras rīkojas ar ESKI. Tomēr, ja Savienības vienība to skaidri pieprasa, ES iestāžu, struktūru un aģentūru datorapdraudējumu reaģēšanas vienībai (*CERT-EU*) vajadzētu būt iespējai minētajai Savienības vienībai sniegt palīdzību, kas saistīta ar incidentiem klasificētās IKT vidēs.

(17) Savienības vienībām būtu jānovērtē kiberdrošības riski, kas skar attiecības ar piegādātājiem un pakalpojumu sniedzējiem, tostarp datu glabāšanas un apstrādes pakalpojumu vai pārvaldītu drošības pakalpojumu sniedzējiem, un būtu jāpieņem pienācīgi pasākumi to novēršanai. Kiberdrošības pasākumi būtu sīkāk jāprecizē *CERT-EU* izdotajās vadlīnijās vai ieteikumos. Nosakot pasākumus un vadlīnijas, pienācīgi būtu jāņem vērā jaunākais tehnikas līmenis un attiecīgā gadījumā relevantie Eiropas un starptautiskie standarti, kā arī relevantie Savienības tiesību akti un rīcībpolitikas, tostarp saskaņā ar Direktīvas (ES) 2022/2555 14. pantu izveidotās sadarbības grupas izdotie kiberdrošības riska novērtējumi un ieteikumi, piemēram, ES koordinētais 5G tīklu kiberdrošības riska novērtējums,

kā arī ES 5G kiberdrošības rīkkopa. Turklāt, ņemot vērā kiberdraudu ainu un to, cik svarīgi Savienības vienībām ir palielināt kibernoturību, varētu būt nepieciešama relevanto IKT produktu, pakalpojumu un procesu sertifikācija saskaņā ar konkrētām Eiropas kiberdrošības sertifikācijas shēmām, kas pieņemtas atbilstīgi Eiropas Parlamenta un Padomes Regulas (ES) 2019/881 ([3]) 49. pantam.

(18) 2011. gada maijā Savienības iestāžu un struktūru ģenerālsekretāri nolēma izveidot sākotnējas konfigurācijas grupu *CERT-EU* vajadzībām, ko 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. gada septembrī *CERT-EU* tika izveidota kā Komisijas darba grupa ar starpiestāžu līmeņa pilnvarām. 2017. gada decembrī Savienības iestādes un struktūras noslēdza iestāžu vienošanos par *CERT-EU* organizāciju un darbību ([4]). Šai regulai būtu jānodrošina vispusīga *CERT-EU* organizācijas, funkcionēšanas un darbības noteikumu kopa. Šīs regulas noteikumi prevalē pār 2017. gada decembrī noslēgtās iestāžu vienošanās par *CERT-EU* organizāciju un darbību noteikumiem.

(19) *CERT-EU* būtu jāpārdēvē par Savienības iestāžu, struktūru, biroju un aģentūru kiberdrošības dienestu, taču nosaukuma atpazīstamības dēļ būtu jāsaglabā īsais nosaukums *CERT-EU*.

(20) Papildus lielāka uzdevumu skaita un plašākas lomas piešķiršanai *CERT-EU*, ar šo regulu izveido Iestāžu kiberdrošības padomi (IKP), lai sekmētu vienādu augstu kiberdrošības līmeni Savienības vienībās. IKP vajadzētu būt ekskluzīvai lomai pārraudzīt, kā šo regulu īsteno Savienības vienības, palīdzēt tām to darīt, kā arī uzraudzīt, kā *CERT-EU* īsteno vispārējās prioritātes un mērķus, un sniegt *CERT-EU* stratēģiskās ievirzes. Tādēļ IKP būtu jānodrošina Savienības iestāžu pārstāvība, kā arī Savienības struktūru, biroju un aģentūru pārstāvju dalība, izmantojot ES aģentūru tīklu (ESAT). IKP organizācija un funkcionēšana būtu sīkāk jāreglamentē ar tās iekšējo reglamentu, kas var ietvert sīkāku precizējumu par regulārām IKP sanāksmēm, tostarp ikgadējām politiskā līmeņa sanāksmēm, kurās, piedaloties katra IKP locekļa augstākā līmeņa vadības pārstāvjiem, IKP varētu rīkot stratēģiskas diskusijas un izstrādāt stratēģiskus norādījumus IKP. Turklāt IKP vajadzētu varēt izveidot izpildkomiteju, kas tai palīdzētu darbā, un deleģēt tai dažus savus uzdevumus un pilnvaras, jo īpaši attiecībā uz uzdevumiem, kuros nepieciešama specifiska tās locekļu lietpratība, piemēram, pakalpojumu kataloga apstiprināšanu un turpmākus tā atjauninājumus, pakalpojumu līmeņa vienošanos kārtību, dokumentu un ziņojumu, ko Savienības vienības iesniedz IKP saskaņā ar šo regulu, novērtēšanu un uzdevumus, kuri saistīti ar IKP izdotu lēmumu sagatavošanu par atbilstības nodrošināšanas pasākumiem un to izpildes pārraudzību. IKP būtu jānosaka izpildkomitejas reglaments, tostarp tās uzdevumus un pilnvaras.

(21) IKP mērķis ir palīdzēt Savienības vienībām uzlabot savas attiecīgās kiberdrošības pozīcijas, kas darāms, īstenojot šo regulu. Lai atbalstītu Savienības vienības, IKP būtu jādod norādes *CERT-EU* vadītājam, jāpieņem daudzgadu stratēģija kiberdrošības līmeņa paaugstināšanai Savienības vienībās, jānosaka brīvprātīgas salīdzinošās izvērtēšanas metodika un citi tās aspekti un jāatvieglina neformālas vietējo kiberdrošības amatpersonu grupas izveide, ko atbalstītu Eiropas Savienības Kiberdrošības aģentūra (*ENISA*), ar mērķi apmainīties ar paraugpraksēm un informāciju šīs regulas īstenošanas sakarā.

([3]) 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.).

([4]) Vienošanās starp Eiropas Parlamentu, Eiropadomi, Eiropas Savienības Padomi, Eiropas Komisiju, Eiropas Savienības Tiesu, Eiropas Centrālo banku, Eiropas Revīzijas palātu, Eiropas Ārējās darbības dienestu, Eiropas Ekonomikas un sociālo lietu komiteju, Eiropas Reģionu komiteju un Eiropas Investīciju banku par Savienības iestāžu, struktūru un aģentūru datorapdraudējumu reaģēšanas vienības (*CERT-EU*) organizāciju un darbību (OV C 12, 13.1.2018., 1. lpp.).

(22) Lai visās Savienības vienībās panāktu augstu kiberdrošības līmeni, to Savienības struktūru, biroju un aģentūru intereses, kurām ir sava IKT vide, vajadzētu būt pārstāvētām IKP ar trim ESAT ieceltiem pārstāvjiem. Personas datu apstrādes drošība un līdz ar to arī tās kiberdrošība ir viens no datu aizsardzības stūrakmeņiem. Ņemot vērā sinerģijas starp datu aizsardzību un kiberdrošību, IKP vajadzētu būt pārstāvētam Eiropas Datu aizsardzības uzraudzītājam kā Savienības vienībai, uz kuru attiecas šī regula, ar īpašu lietpratību datu aizsardzības – arī elektronisko sakaru tīklu drošības – jomā. Ņemot vērā inovācijas un konkurētspējas nozīmi kiberdrošības jomā, IKP vajadzētu būt pārstāvētam Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram. IKP vajadzētu būt pārstāvētai *ENISA* un Eiropas Savienības Kosmosa programmas aģentūrai, ņemot vērā *ENISA* kā kiberdrošības lietpratības centra lomu un tās sniegto atbalstu un ņemot vērā Savienības kosmosa infrastruktūras un pakalpojumu kiberdrošības nozīmi. Ņemot vērā lomu, kas ar šo regulu piešķirta *CERT-EU*, IKP priekšsēdētājam uz visām IKP sanāksmēm būtu jāuzaicina *CERT-EU* vadītājs, izņemot gadījumus, kad IKP apspriež jautājumus, kuri tieši saistīti ar *CERT-EU* vadītāju.

(23) IKP būtu jāpārrauga atbilstība šai regulai, kā arī vadlīniju, ieteikumu un aicinājumu rīkoties īstenošana. Tehniskos jautājumos IKP būtu jāsaņem atbalsts no tehniskajām padomdevējām grupām, kas nokomplektētas pēc IKP ieskatiem. Minētajām tehniskajām padomdevējām grupām būtu jāstrādā ciešā sadarbībā ar *CERT-EU*, Savienības vienībām, kā arī, ja nepieciešams, citām ieinteresētajām personām.

(24) Ja IKP konstatē, ka Savienības vienības nav faktiski īstenojušas šo regulu vai saskaņā ar to izdotas vadlīnijas, ieteikumus vai aicinājumus rīkoties, tai, neskarot attiecīgās Savienības vienības iekšējās procedūras, vajadzētu varēt veikt atbilstības nodrošināšanas pasākumus. Atbilstības nodrošināšanas pasākumi IKP būtu jāpiemēro pakāpeniski, citiem vārdiem, IKP vispirms būtu jāpieņem vismazāk stingrais pasākums, proti, pamatots atzinums, un tikai, ja nepieciešams, jāpieņem arvien stingrāki pasākumi, līdz pat visstingrākajam, proti, ieteikums uz laiku apturēt datu plūsmas uz attiecīgo Savienības vienību. Šāds ieteikums būtu jāpiemēro tikai ārkārtējos gadījumos, kad attiecīgā Savienības vienība ilgi, tīši, atkārtoti vai nopietni pārkāpj šo regulu.

(25) Pamatotais atzinums ir vismazāk stingrais atbilstības nodrošināšanas pasākums, kas vēršas pret konstatētām šīs regulas īstenošanas nepilnībām. IKP vajadzētu būt iespējai pēc pamatota atzinuma sniegt norādījumus, lai palīdzētu Savienības vienībai nodrošināt, ka tās satvars, kiberdrošības riska pārvaldības pasākumi, kiberdrošības plāns un ziņošana atbilst šai regulai, un pēc tam brīdinājumu, ka noteiktā laikā jānovērš konstatētie Savienības vienības trūkumi. Ja brīdinājumā norādītie trūkumi nav pietiekami novērsti, IKP vajadzētu būt iespējai izdot pamatotu paziņojumu.

(26) IKP vajadzētu būt iespējai ieteikt veikt Savienības vienības revīziju. Savienības vienībai vajadzētu varēt šajā nolūkā izmantot savu iekšējās revīzijas funkciju. IKP vajadzētu arī varēt pieprasīt, lai revīziju veic revīzijas dienests, kas ir trešā puse, tostarp privātā sektora pakalpojumu sniedzējs, par kuru abas puses vienojušās.

(27) Tādēļ ārkārtējos gadījumos, kad Savienības vienība ilgi, tīši, atkārtoti vai nopietni pārkāpj šo regulu, IKP būtu jāvar kā galēju pasākumu visām dalībvalstīm un Savienības vienībām, kamēr attiecīgā Savienības vienība pārkāpumu nav atrisinājusi līdz galam, ieteikt uz laiku apturēt datu plūsmas uz attiecīgo Savienības vienību. Šāds ieteikums būtu jāpaziņo, izmantojot piemērotus un drošus saziņas kanālus.

(28) Lai nodrošinātu pareizu šīs regulas īstenošanu, IKP, ja tā uzskata, ka Savienības vienības izdarītu pastāvīgu šīs regulas pārkāpumu ir tieši izraisījusi tās darbinieka darbība vai bezdarbība, tostarp augstākajā vadības līmenī, būtu jāpieprasa attiecīgajai Savienības vienībai veikt pienācīgus pasākumus, tostarp apsvērt disciplināra rakstura pasākumu veikšanu saskaņā ar noteikumiem un procedūrām, ko paredz Padomes Regulā (EEK, Euratom, EOTK) Nr. 259/68 ([5]) ("Civildienesta noteikumi") paredzētie Eiropas Savienības Civildienesta noteikumi un Savienības pārējo darbinieku nodarbināšanas kārtība, un citiem piemērojamiem noteikumiem un procedūrām.

(29) *CERT-EU* būtu jāveicina visu Savienības vienību IKT vides drošība. Apsverot, vai pēc kādas Savienības vienības pieprasījuma sniegt tehniskus padomus vai ieguldījumu relevantos rīcībpolitiskos jautājumos, *CERT-EU* būtu jānodrošina, ka tas nav šķērslis citu tai ar šo regulu piešķirto uzdevumu izpildei. Attiecībā pret Savienības vienībām *CERT-EU* būtu jādarbojas ekvivalenti koordinatoram, kas izraudzīts koordinētas ievainojamības izpaušanas nolūkā saskaņā ar Direktīvas (ES) 2022/2555 12. panta 1. punktu.

(30) *CERT-EU* būtu jāatbalsta pasākumu īstenošana vienāda augsta kiberdrošības līmeņa panākšanai, iesniedzot vadlīniju un ieteikumu priekšlikumus IKP vai izdodot aicinājumus rīkoties. Šādas vadlīnijas un ieteikumi būtu jāapstiprina IKP. Vajadzības gadījumā *CERT-EU* būtu jāizdod aicinājumi rīkoties, kuros aprakstīti neatliekami drošības pasākumi, ko Savienības vienības tiek mudinātas veikt noteiktā laikā. IKP būtu jāuzdod *CERT-EU* izdot, atsaukt vai mainīt vadlīniju vai ieteikuma priekšlikumu vai aicinājumu rīkoties.

(31) *CERT-EU* būtu arī jāpilda loma, kas Direktīvā (ES) 2022/2555 tai paredzēta attiecībā uz sadarbību un informācijas apmaiņu ar datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu, kurš izveidots saskaņā ar minētās direktīvas 15. pantu. Turklāt saskaņā ar Komisijas Ieteikumu (ES) 2017/1584 ([6]) *CERT-EU* būtu jāsadarbojas un jākoordinē reakcija ar relevantajām ieinteresētajām personām. Lai palīdzētu sasniegt augstu kiberdrošības līmeni visā Savienībā, *CERT-EU* būtu jādalās incidentu raksturojošā informācijā ar partneriem dalībvalstīs. *CERT-EU* būtu arī jāsadarbojas ar citiem publiskiem un privātiem partneriem, tostarp Ziemeļatlantijas līguma organizāciju, ja saņemta iepriekšēja IKP atļauja.

(32) Atbalstot operatīvo kiberdrošību, *CERT-EU* būtu jāizmanto pieejamā *ENISA* lietpratība, izmantojot strukturētu sadarbību, kā paredzēts Regulā (ES) 2019/881. 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 *ENISA* kiberdraudu analīzes aspektā un savs ziņojums par drošības apdraudējuma ainu regulāri jākopīgo ar to.

(33) *CERT-EU* vajadzētu varēt sadarboties un apmainīties ar informāciju ar relevantām kiberdrošības kopienām Savienībā un tās dalībvalstīs, lai sekmētu operacionālo sadarbību un pastāvošie tīkli varētu realizēt visu savu potenciālu Savienības aizsardzībā.

(34) Tā kā *CERT-EU* pakalpojumi un uzdevumi ir Savienības vienību interesēs, katrai Savienības vienībai, kam ir tēriņi IKT jomā, būtu jādod taisnīgs ieguldījums minēto pakalpojumu un uzdevumu izpildē. Minētais ieguldījums neskar Savienības vienību budžeta autonomiju.

([5]) Padomes Regula (EEK, Euratom, EOTK) Nr. 259/68 (1968. gada 29. februāris), ar ko nosaka Eiropas Kopienu Civildienesta noteikumus un Pārējo darbinieku nodarbināšanas kārtību, kā arī paredz īpašus Komisijas ierēdņiem uz laiku piemērojamus pasākumus (OV L 56, 4.3.1968., 1. lpp.).

([6]) 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.).

(35) Daudzi kiberuzbrukumi ir daļa no plašākām kampaņām, kas vērstas pret Savienības vienībām vai interešu kopienām, kuras ietver Savienības vienības. Lai darītu iespējamu preventīvu atklāšanu, reaģēšanu uz incidentiem vai mitigācijas pasākumus, kā arī atgūšanos no incidentiem, Savienības vienībām vajadzētu varēt paziņot *CERT-EU* par incidentiem, kiberdraudiem, ievainojamībām un gandrīz notikušiem notikumiem un jānorāda attiecīgas tehniskas detaļas, kas dod iespēju atklāt vai mitigēt līdzīgus incidentus, kiberdraudus, ievainojamības un gandrīz notikušus notikumus citās Savienības vienībās, kā arī reaģēt uz tiem. Ievērojot tādu pašu pieeju, kāda paredzēta Direktīvā (ES) 2022/2555, Savienības vienībām 24 stundu laikā pēc tam, kad tās uzzinājušas par būtisku incidentu, būtu jāiesniedz agrīns brīdinājums *CERT-EU*. Šādai informācijas apmaiņai būtu jādod iespēja *CERT-EU* izplatīt informāciju citām Savienības vienībām, kā arī attiecīgajiem partneriem, lai palīdzētu aizsargāt Savienības vienību IKT vides un Savienības vienību partneru IKT vides pret līdzīgiem incidentiem.

(36) Šī regula nosaka vairākposmu pieeju būtisku incidentu paziņošanai, lai panāktu pareizo līdzsvaru starp ātru ziņošanu, kas palīdz mazināt būtisko incidentu potenciālo izplatīšanos un dod Savienības vienībām iespēju lūgt atbalstu, no vienas puses, un padziļinātu ziņošanu, kurā izdara vērtīgus secinājumus no individuāliem incidentiem, kura laika gaitā uzlabo Savienības vienību individuālo kibernoturību un kura palīdz uzlabot to kopējo kiberdrošības stāvokli, no otras puses. Šajā sakarā regulā būtu jāiekļauj ziņošana par incidentiem, kuri, spriežot pēc attiecīgās Savienības vienības veikta sākotnēja novērtējuma, varētu izraisīt smagus attiecīgās Savienības vienības funkcionēšanas traucējumus vai radīt tai finansiālus zaudējumus, vai ietekmēt citas fiziskas vai juridiskas personas, radot būtisku materiālu vai nemateriālu kaitējumu. Šādā sākotnējā novērtējumā cita starpā būtu jāņem vērā skartās tīklu un informācijas sistēmas, sevišķi to nozīmīgums Savienības vienības funkcionēšanā, kiberdrauda smagums un tehniskais raksturojums un visas pamatā esošās ievainojamības, kas tiek izmantotas, kā arī Savienības vienības pieredze ar līdzīgiem incidentiem. Nosakot, vai darbības traucējumi ir smagi, svarīgi varētu būt tādi rādītāji kā apmērs, kādā tiek ietekmēta Savienības vienības funkcionēšana, incidenta ilgums un skarto fizisko un juridisko personu skaits.

(37) Tā kā relevantās Savienības vienības un tās dalībvalsts, kurā minētā Savienības vienība atrodas, infrastruktūra un tīklu un informācijas sistēmas ir savstarpēji savienotas, ir izšķirīgi svarīgi, lai minētā dalībvalsts bez liekas kavēšanās tiktu informēta par būtisku incidentu minētajā Savienības vienībā. Šajā nolūkā skartajai Savienības vienībai par tāda būtiska incidenta gadījumu, par kuru tā ziņo *CERT-EU*, būtu jāinformē ikviens saskaņā ar Direktīvas (ES) 2022/2555 8. un 10. pantu iecelts vai izveidots relevants partneris dalībvalstī. Kad *CERT-EU* uzzina par būtisku incidentu, kas notiek dalībvalstī, tai būtu jāpaziņo visiem relevantajiem partneriem minētajā dalībvalstī.

(38) Būtu jāīsteno mehānisms, kas nodrošinātu Savienības vienību reālu informācijas apmaiņu, koordināciju un sadarbību lielu incidentu gadījumā un kam būtu skaidri noteiktas iesaistīto Savienības vienību lomas un pienākumi. Komisijas pārstāvim IKP, ievērojot kiberkrīžu pārvaldības plānu, vajadzētu būt kontaktpunktam, kas palīdzētu IKP dalīties relevantā informācijā par lieliem incidentiem ar Eiropas Kiberkrīžu sadarbības organizāciju tīklu (*EU-CyCLONe*), tādējādi uzlabojot kopīgo situācijas apzināšanos. Kontaktpunkta lomai, ko Komisijas pārstāvis pilda IKP, nevajadzētu skart Komisijas atsevišķo un atšķirīgo lomu *EU-CyCLONe* saskaņā ar Direktīvas (ES) 2022/2555 16. panta 2. punktu.

(39) Personas datu apstrādei, kas veikta, ievērojot šo regulu, piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 ([7]). Personas datu apstrāde varētu notikt saistībā ar pasākumiem, kas pieņemti sakarā ar kiberdrošības riska pārvaldību, ievainojamību un incidentu risināšanu, informācijas kopīgošanu par incidentiem, kiberdraudiem un ievainojamībām un reaģēšanas uz incidentiem koordināciju un sadarbību. Šādiem pasākumiem varētu būt nepieciešams apstrādāt konkrētu kategoriju personas datus, piemēram, IP adreses, vienotos resursu vietrāžus (*URL*), domēnu nosaukumus, e-pasta adreses, datu subjekta organizatoriskās lomas, laika zīmogus, e-pasta virsrakstus vai datņu nosaukumus. Visiem pasākumiem, kas veikti saskaņā ar šo regulu, būtu jāatbilst datu

([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.).

aizsardzības un privātuma regulējumam, un Savienības vienībām, *CERT-EU* un attiecīgā gadījumā IKP būtu jāveic visi relevantie tehniskie un organizatoriskie aizsardzības pasākumi, lai šādu atbilstību atbildīgi nodrošinātu.

(40) Šī regula izveido juridisko pamatu personas datu apstrādei, ko Savienības vienības, *CERT-EU* un attiecīgā gadījumā IKP veic nolūkā pildīt uzdevumus un pienākumus, kurus tām šī regula paredz, saskaņā ar Regulas (ES) 2018/1725 5. panta 1. punkta b) apakšpunktu. *CERT-EU* var darboties kā apstrādātājs vai pārzinis atkarībā no uzdevuma, ko tas veic, saskaņā ar Regulu (ES) 2018/1725.

(41) Dažos gadījumos nolūkā izpildīt šajā regulā noteiktos pienākumus nodrošināt augstu kiberdrošības līmeni un jo īpaši ievainojamību un incidentu risināšanas kontekstā Savienības vienībām un *CERT-EU* var būt nepieciešams apstrādāt īpašu kategoriju personas datus, kas minēti Regulas (ES) 2018/1725 10. panta 1. punktā. Šī regula izveido juridisko pamatu īpašu kategoriju personas datu apstrādei, ko veic Savienības vienības un *CERT-EU* saskaņā ar Regulas (ES) 2018/1725 10. panta 2. punkta g) apakšpunktu. Īpašu kategoriju personas datu apstrādei, ko veic saskaņā ar šo regulu, vajadzētu būt stingri samērīgai ar sasniedzamo mērķi. Ievērojot minētās regulas 10. panta 2. punkta g) apakšpunktā izklāstītos nosacījumus, Savienības vienībām un *CERT-EU* vajadzētu varēt šādus datus apstrādāt tikai tiktāl, ciktāl tas ir nepieciešams, un ja tas ir skaidri paredzēts šajā regulā. Apstrādājot īpašu kategoriju personas datus, Savienības vienībām un *CERT-EU* būtu jāievēro tiesību uz datu aizsardzību būtība un jānodrošina piemēroti un konkrēti pasākumi, kas sargā datu subjektu pamattiesības un intereses.

(42) Saskaņā ar Regulas (ES) 2018/1725 33. pantu Savienības vienībām un *CERT-EU*, ņemot vērā jaunāko tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, tvērumu, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma riskus fizisku personu tiesībām un brīvībām, būtu jāīsteno pienācīgi tehniski un organizatoriski pasākumi, kas nodrošinātu pienācīgu personas datu drošības līmeni, piemēram, ierobežotu piekļuves tiesību nodrošināšana pēc principa "nepieciešamība zināt", revīzijas izsekojamības principu piemērošana, pārraudzības ķēdes pieņemšana, datu glabāšana miera stāvoklī kontrolētā un revidējamā vidē, standartizētas darbības procedūras un privātuma aizsardzības pasākumi, piemēram, pseidonimizācija vai šifrēšana. Minētie pasākumi nebūtu jāīsteno tā, ka tiktu ietekmēta incidentu risināšana un pierādījumu integritāte. Ja Savienības vienība vai *CERT-EU* nosūta ar incidentu saistītus personas datus, tostarp īpašu kategoriju personas datus, partnerim šīs regulas nolūkos, šādai nosūtīšanai būtu jāatbilst Regulai (ES) 2018/1725. Ja īpašu kategoriju personas dati tiek nosūtīti trešai pusei, Savienības vienībām un *CERT-EU* būtu jānodrošina, ka trešā puse piemēro pasākumus attiecībā uz personas datu aizsardzību tādā līmenī, kas ir līdzvērtīgs Regulas (ES) 2018/1725 nodrošinātajam līmenim.

(43) Šīs regulas nolūkos apstrādātie personas dati būtu jāglabā tikai tik ilgi, cik nepieciešams, saskaņā ar Regulu (ES) 2018/1725. Savienības vienībām un attiecīgā gadījumā *CERT-EU*, kas darbojas kā pārzinis, būtu jānosaka glabāšanas laikposmi, kuriem aprobežojas ar to, kas ir nepieciešams norādīto mērķu sasniegšanai. Jo īpaši attiecībā uz personas datiem, kas savākti incidentu risināšanai, Savienības vienībām un *CERT-EU* būtu jānošķir personas dati, kuri tiek vākti kiberdraudu atklāšanai to IKT vidēs, lai novērstu incidentu, un personas dati, kas tiek vākti, lai mitigētu incidentu, reaģētu uz to un atgūtos no tā. Lai atklātu kiberdraudus, ir svarīgi ņemt vērā laiku, ko apdraudētājs sistēmā var pavadīt neatklāts. Lai mitigētu incidentu, reaģētu uz to un atgūtos no tā, ir svarīgi izsvērt, vai personas dati ir vajadzīgi, lai izsekotu un risinātu atkārtotu incidentu vai līdzīga rakstura incidentu, attiecībā uz kuru varētu pierādīt korelāciju.

(44) Savienības vienībām un *CERT-EU* ar informāciju būtu jārīkojas atbilstoši piemērojamajiem noteikumiem par informācijas drošību. Arī cilvēkresursu drošības iekļaušanai kiberdrošības riska pārvaldības pasākumā būtu jāatbilst piemērojamajiem noteikumiem.

(45) Informācijas kopīgošanas nolūkā tiek izmantoti redzami iezīmējumi, lai norādītu, ka informācijas saņēmējiem jāpiemēro kopīgošanas robežas, kuru pamatā jo īpaši ir vienošanās par informācijas neizpaušanu vai neformāla vienošanās par informācijas neizpaušanu, piemēram, gaismas signālu protokols vai citas skaidras avota norādes. Gaismas signālu protokols ir jāsaprot kā līdzeklis, ar ko sniegt informāciju par jebkādiem ierobežojumiem attiecībā uz tālāku informācijas izplatīšanu. To izmanto gandrīz visās *CSIRT* un dažos informācijas analīzes un kopīgošanas centros.

(46) Šī regula būtu regulāri jāizvērtē, ņemot vērā turpmākās sarunas par daudzgadu finanšu shēmām, kas dotu iespēju pieņemt turpmākus lēmumus par *CERT-EU* darbību un institucionālo lomu, tostarp iespējamo *CERT-EU* izveidi Savienības biroja formā.

(47) 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. Minētajā ziņojumā ar IKP palīdzību būtu jāizvērtē, vai ir lietderīgi šīs regulas darbības jomā iekļaut tīklu un informācijas sistēmas, kuras rīkojas ar ESKI, īpaši apstākļos, kad nav Savienības vienībām kopīgu informācijas drošības noteikumu.

(48) Lai sasniegtu pamatmērķi panākt vienādu augstu kiberdrošības līmeni Savienības vienībās, saskaņā ar proporcionalitātes principu ir nepieciešams un lietderīgi paredzēt noteikumus par Savienības vienību kiberdrošību. Saskaņā ar Līguma par Eiropas Savienību 5. panta 4. punktu šī regula paredz vienīgi tādus pasākumus, kas ir vajadzīgi, lai sasniegtu izvirzīto mērķi.

(49) Šī regula atspoguļo to, ka Savienības vienību lielums un spējas atšķiras, arī finanšu resursu un cilvēkresursu ziņā.

(50) Saskaņā ar Regulas (ES) 2018/1725 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2022. gada 17. maijā sniedza atzinumu ([8]),

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets

Šī regula nosaka pasākumus, kuru mērķis ir panākt vienādu augstu kiberdrošības līmeni Savienības vienībās, attiecībā uz:

a) iekšēja kiberdrošības riska pārvaldības, pārvaldes un kontroles satvara izveidi katrā Savienības vienībā saskaņā ar 6. pantu;

b) kiberdrošības riska pārvaldību, ziņošanu un informācijas kopīgošanu;

c) saskaņā ar 10. pantu izveidotās Iestāžu kiberdrošības padomes organizāciju, funkcionēšanu un darbību, kā arī Savienības iestāžu, struktūru, biroju un aģentūru kiberdrošības dienesta (*CERT-EU*) organizāciju, funkcionēšanu un darbību;

d) šīs regulas īstenošanas uzraudzību.

([8]) OV C 258, 5.7.2022., 10. lpp.

2. pants

Darbības joma

1. Šo regulu piemēro Savienības vienībām, Iestāžu kiberdrošības padomei, kas izveidota saskaņā ar 10. pantu, un *CERT-EU*.

2. Šo regulu piemēro, neskarot iestāžu autonomiju saskaņā ar Līgumiem.

3. Izņemot 13. panta 8. punktu, šo regulu nepiemēro tīklu un informācijas sistēmām, kuras rīkojas ar ES klasificēto informāciju (ESKI).

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

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

2) "tīklu un informācijas sistēma" ir tīklu un informācijas sistēma, kā definēts Direktīvas (ES) 2022/2555 6. panta 1) punktā;

3) "tīklu un informācijas sistēmu drošība" ir tīklu un informācijas sistēmu drošība, kā definēts Direktīvas (ES) 2022/2555 6. panta 2) punktā;

4) "kiberdrošība" ir kiberdrošība, kā definēts Regulas (ES) 2019/881 2. panta 1) punktā;

5) "visaugstākā līmeņa vadība" ir visaugstākā administratīvā līmeņa vadītājs, vadības struktūra vai koordinācijas un uzraudzības struktūra, kas atbild par Savienības vienības funkcionēšanu un kam ir pilnvaras pieņemt vai atļaut lēmumus atbilstoši minētās Savienības vienības augsta līmeņa pārvaldības kārtībai, neskarot citu vadības līmeņu oficiālos pienākumus attiecībā uz atbilstību un kiberdrošības riska pārvaldību attiecīgajās atbildības jomās;

6) "gandrīz noticis notikums" ir gandrīz noticis notikums, kā definēts Direktīvas (ES) 2022/2555 6. panta 5) punktā;

7) "incidents" ir incidents, kā definēts Direktīvas (ES) 2022/2555 6. panta 6) punktā;

8) "liels incidents" ir incidents, kura radītais traucējumu līmenis pārsniedz Savienības vienības un *CERT-EU* spēju uz to reaģēt vai kurš būtiski ietekmē vismaz divas Savienības vienības;

9) "plašapmēra kiberdrošības incidents" ir plašapmēra kiberdrošības incidents, kā definēts Direktīvas (ES) 2022/2555 6. panta 7) punktā;

10) "incidenta risināšana" ir incidenta risināšana, kā definēts Direktīvas (ES) 2022/2555 6. panta 8) punktā;

11) "kiberdraudi" ir kiberdraudi, kā definēts Regulas (ES) 2019/881 2. panta 8) punktā;

12) "būtiski kiberdraudi" ir būtiski kiberdraudi, kā definēts Direktīvas (ES) 2022/2555 6. panta 11) punktā;

13) "ievainojamība" ir ievainojamība, kā definēts Direktīvas (ES) 2022/2555 6. panta 15) punktā;

14) "kiberdrošības risks" ir risks, kā definēts Direktīvas (ES) 2022/2555 6. panta 9) punktā;

15) "mākoņdatošanas pakalpojums" ir mākoņdatošanas pakalpojums, kā definēts Direktīvas (ES) 2022/2555 6. panta 30) punktā.

4. pants

Personas datu apstrāde

1. Personas datu apstrādi, kas paredzēta šajā regulā, *CERT-EU*, Iestāžu kiberdrošības padome, kura izveidota saskaņā ar 10. pantu, un Savienības vienības veic saskaņā ar Regulu (ES) 2018/1725.

2. Ja *CERT-EU*, Iestāžu kiberdrošības padome, kura izveidota saskaņā ar 10. pantu, un Savienības vienības pilda šajā regulā paredzētus uzdevumus vai pienākumus, tās personas datus apstrādā un ar tiem apmainās tikai tādā apmērā, cik nepieciešams, un vienīgi nolūkā pildīt minētos uzdevumus vai pienākumus.

3. Regulas (ES) 2018/1725 10. panta 1. punktā minēto īpašu kategoriju personas datu apstrādi uzskata par nepieciešamu būtisku sabiedrības interešu dēļ saskaņā ar minētās regulas 10. panta 2. punkta g) apakšpunktu. Šādus datus var apstrādāt tikai tiktāl, ciktāl tas nepieciešams šīs regulas 6. un 8. pantā minēto kiberdrošības riska pārvaldības pasākumu īstenošanai, *CERT-EU* pakalpojumu sniegšanai saskaņā ar 13. pantu, incidentu raksturojošas informācijas kopīgošanai saskaņā ar 17. panta 3. punktu un 18. panta 3. punktu, informācijas kopīgošanai saskaņā ar 20. pantu, ziņošanas pienākumiem saskaņā ar 21. pantu, reaģēšanas uz incidentiem koordinācijai un sadarbībai saskaņā ar 22. pantu un lielu incidentu pārvaldībai saskaņā ar 23. pantu. Savienības vienības un *CERT-EU*, rīkojoties kā datu pārziņi, piemēro tehniskus pasākumus, lai nepieļautu īpašu kategoriju personas datu apstrādi citiem nolūkiem, un paredz piemērotus un konkrētus pasākumus, kas aizsargā datu subjektu pamattiesības un intereses.

II NODAĻA

VIENĀDA AUGSTA KIBERDROŠĪBAS LĪMEŅA PANĀKŠANAS PASĀKUMI

5. pants

Pasākumu īstenošana

1. Līdz 2024. gada 8. septembrim saskaņā ar 10. pantu izveidotā Iestāžu kiberdrošības padome pēc apspriešanās ar Eiropas Savienības Kiberdrošības aģentūru (*ENISA*) un pēc *CERT-EU* norādījumu saņemšanas izdod vadlīnijas Savienības vienībām nolūkā veikt sākotnējo kiberdrošības pārskatīšanu un izveidot iekšēju kiberdrošības riska pārvaldības, pārvaldes un kontroles satvaru saskaņā ar 6. pantu, veikt kiberdrošības gatavības novērtējumus saskaņā ar 7. pantu, veikt kiberdrošības riska pārvaldības pasākumus saskaņā ar 8. pantu un pieņemt kiberdrošības plānu saskaņā ar 9. pantu.

2. Īstenojot 6. līdz 9. pantu, Savienības vienības ņem vērā šā panta 1. punktā minētās vadlīnijas, kā arī relevantās vadlīnijas un ieteikumus, kas pieņemti saskaņā ar 11. un 14. pantu.

6. pants

Kiberdrošības riska pārvaldības, pārvaldes un kontroles satvars

1. Līdz 2025. gada 8. aprīlim katra Savienības vienība pēc sākotnējās kiberdrošības pārskatīšanas, piemēram, revīzijas, izveido iekšēju kiberdrošības riska pārvaldības, pārvaldes un kontroles satvaru (“satvars”). Satvara izveidi pārrauga un par to atbild Savienības vienības visaugstākā līmeņa vadība.

2. Satvars aptver visu attiecīgās Savienības vienības neklasificēto IKT vidi, tostarp jebkādu IKT vidi organizācijas telpās, darbības tehnoloģiju tīklu organizācijas telpās, ārpakalpojumu aktīvus un pakalpojumus mākoņdatošanas vidē vai trešās personas mitinātus aktīvus vai pakalpojumus, mobilās ierīces, korporatīvos tīklus, darbības tīklus, kas nav pievienoti internetam, un jebkādas minētajām vidēm (“IKT vide”) pievienotas ierīces. Satvara pamatā ir visu apdraudējumu pieeja.

3. Satvars nodrošina augstu kiberdrošības līmeni. Satvars nosaka iekšējās kiberdrošības rīcībpolitikas, tostarp mērķus un prioritātes, tīklu un informācijas sistēmu drošībai, kā arī to Savienības vienības darbinieku uzdevumus un pienākumus, kuriem uzticēts nodrošināt rezultatīvu šīs regulas īstenošanu. Satvarā iekļauj arī mehānismus īstenošanas rezultativitātes mērīšanai.

4. Mainīgo kiberdrošības risku kontekstā satvaru regulāri un vismaz ik četrus gadus pārskata. Attiecīgā gadījumā un pēc saskaņā ar 10. pantu izveidotās Iestāžu kiberdrošības padomes pieprasījuma Savienības vienība satvaru var atjaunināt, pamatojoties uz *CERT-EU* norādījumiem par konstatētajiem incidentiem vai iespējamiem trūkumiem, kas novēroti šīs regulas īstenošanā.

5. Katras Savienības vienības visaugstākā līmeņa vadība ir atbildīga par šīs regulas īstenošanu un pārrauga, kā tās organizācija pilda ar satvaru saistītos pienākumus.

6. Attiecīgā gadījumā un neskarot vienības atbildību par šīs regulas īstenošanu, katras Savienības vienības visaugstākā līmeņa vadība var šajā regulā noteiktos īpašos pienākumus deleģēt augstākā līmeņa ierēdņiem Civildienesta noteikumu 29. panta 2. punkta izpratnē vai citiem līdzvērtīga līmeņa ierēdņiem attiecīgajā Savienības vienībā. Neatkarīgi no šādas deleģēšanas visaugstākā līmeņa vadību var saukt pie atbildības par šīs regulas pārkāpumiem, ko attiecīgā Savienības vienība izdarījusi.

7. Katra Savienības vienība ievieš iedarbīgus mehānismus, kuru mērķis ir nodrošināt, ka pienācīga to IKT budžeta procentuālā daļa tiek tērēta kiberdrošības vajadzībām. Nosakot minēto procentuālo daļu, pienācīgi ņem vērā satvaru.

8. Katra Savienības vienība ieceļ vietējo kiberdrošības speciālistu vai līdzvērtīgu darbinieku, kas rīkojas kā tās vienotais kontaktpunkts visos kiberdrošības aspektos. Vietējais kiberdrošības speciālists veicina šīs regulas īstenošanu un regulāri tieši ziņo visaugstākā līmeņa vadībai par īstenošanas stāvokli. Neskarot to, ka vietējais kiberdrošības speciālists ir vienotais kontaktpunkts katrā Savienības vienībā, Savienības vienība konkrētus vietējā kiberdrošības speciālista uzdevumus attiecībā uz šīs regulas īstenošanu var deleģēt *CERT-EU*, pamatojoties uz pakalpojumu līmeņa vienošanos, kas noslēgta starp minēto Savienības vienību un *CERT-EU*, vai minētos uzdevumus var sadalīt pa vairākām Savienības vienībām. Ja minētos uzdevumus deleģē *CERT-EU*, saskaņā ar 10. pantu izveidotā Iestāžu kiberdrošības padome pieņem lēmumu, vai minētā pakalpojuma sniegšana ir daļa no *CERT-EU* pamatpakalpojumiem, ņemot vērā attiecīgās Savienības vienības cilvēkresursus un finanšu resursus. Katra Savienības vienība bez liekas kavēšanās paziņo *CERT-EU* par ieceltajiem vietējiem kiberdrošības speciālistiem un jebkādām turpmākām to maiņām.

CERT-EU izveido un atjaunina iecelto vietējo kiberdrošības speciālistu sarakstu.

9. Katras Savienības vienības augstākie ierēdņi Civildienesta noteikumu 29. panta 2. punkta izpratnē vai citi līdzvērtīga līmeņa ierēdņi, kā arī visi relevantie darbinieki, kuriem uzdots īstenot kiberdrošības riska pārvaldības pasākumus un pildīt pienākumus, ko paredz šī regula, regulāri piedalās īpašās apmācībās, lai gūtu zināšanas un prasmes, kas ir pietiekamas, lai izprastu un novērtētu kiberdrošības riska un pārvaldības prakses, kā arī to ietekmi uz Savienības vienības darbību.

7. pants

Kiberdrošības gatavības novērtējumi

1. Līdz 2025. gada 8. jūlijam un pēc tam vismaz ik divus gadus katra Savienības vienība veic kiberdrošības gatavības novērtējumu, kas aptver visus tās IKT vides elementus.

2. Kiberdrošības gatavības novērtējumus attiecīgā gadījumā veic ar specializētas trešās puses palīdzību.

3. Savienības vienības ar līdzīgu struktūru var sadarboties savu attiecīgo vienību kiberdrošības gatavības novērtēšanā.

4. Pēc saskaņā ar 10. pantu izveidotās Iestāžu kiberdrošības padomes pieprasījuma un ar skaidru attiecīgās Savienības vienības piekrišanu kiberdrošības gatavības novērtējuma rezultātus var apspriest minētajā padomē vai neformālajā vietējo kiberdrošības speciālistu grupā, lai mācītos no pieredzes un dalītos paraugpraksēs.

8. pants

Kiberdrošības riska pārvaldības pasākumi

1. Bez liekas kavēšanās un katrā ziņā līdz 2025. gada 8. septembrim katra Savienības vienība savas visaugstākā līmeņa vadības uzraudzībā veic piemērotus un samērīgus tehniskos, operacionālos un organizatoriskos pasākumus, lai pārvaldītu kiberdrošības riskus, kas apzināti satvarā, un lai novērstu vai mazinātu incidentu ietekmi. Ņemot vērā jaunāko tehnikas līmeni un attiecīgā gadījumā relevantos Eiropas un starptautiskos standartus, minētie pasākumi nodrošina tīklu un informācijas sistēmu drošības līmeni visā IKT vidē, kas ir samērīgs ar kiberdrošības riskiem, ar kuriem saskaras. Novērtējot minēto pasākumu samērīgumu, pienācīgi ņem vērā to, cik lielā mērā Savienības vienība ir pakļauta kiberdrošības riskiem, tās lielumu un incidentu varbūtību un smagumu, tostarp sociālo, ekonomisko un starpinstitucionālo ietekmi.

2. Savienības vienības kiberdrošības riska pārvaldības pasākumu īstenošanā pievēršas vismaz šādām jomām:

a) kiberdrošības rīcībpolitika, tostarp pasākumi, kas vajadzīgi, lai īstenotu 6. pantā un šā panta 3. punktā minētos mērķus un prioritātes;

b) kiberdrošības riska analīzes un informācijas sistēmu drošības rīcībpolitikas;

c) rīcībpolitiskie mērķi mākoņdatošanas pakalpojumu izmantošanas ziņā;

d) attiecīgā gadījumā kiberdrošības revīzija, kas var ietvert kiberdrošības riska, ievainojamību un kiberdraudu novērtējumu, un ielaušanās testēšana, ko regulāri veic uzticams privāts pakalpojumu sniedzējs;

e) no d) apakšpunktā minētajām kiberdrošības revīzijām izrietošo ieteikumu īstenošana ar kiberdrošības un rīcībpolitikas atjauninājumiem;

f) kiberdrošības organizācija, tostarp lomu un pienākumu noteikšana;

g) aktīvu pārvaldība, tostarp IKT aktīvu inventarizācija un IKT tīkla kartogrāfija;

h) cilvēkresursu drošība un piekļuves kontrole;

i) darbības drošība;

j) komunikāciju drošība;

k) sistēmas iegāde, izstrāde un uzturēšana, tostarp ievainojamības risināšanas un izpaušanas rīcībpolitikas;

l) ja iespējams, pirmkoda pārredzamības rīcībpolitikas;

m) piegādes ķēdes drošība, tostarp ar drošību saistītus aspektus, kas attiecas uz attiecībām starp katru Savienības vienību un tās tiešajiem piegādātājiem vai pakalpojumu sniedzējiem;

n) incidentu risināšana un sadarbība ar *CERT-EU*, piemēram, drošības uzraudzības un reģistrēšanas uzturēšana;

o) darbības nepārtrauktības pārvaldība, piemēram, dublējuma pārvaldība un negadījuma seku novēršana, un krīžu pārvaldība; un

p) kiberdrošības izglītības, prasmju, izpratnes veidošanas, mācību un apmācības programmu veicināšana un izstrāde.

Pirmās daļas m) apakšpunkta nolūkos Savienības vienības ņem vērā ievainojamības, kas raksturīgas katram tiešajam piegādātājam un pakalpojumu sniedzējam, un savu piegādātāju un pakalpojumu sniedzēju produktu un kiberdrošības prakšu vispārējo kvalitāti, tostarp drošas izstrādes procedūras.

3. Savienības vienības veic vismaz šādus īpašus kiberdrošības riska pārvaldības pasākumus:

a) tehniskie pasākumi, kas dara iespējamu un uztur tāldarbu;

b) konkrēti pasākumi virzībā uz nulles uzticēšanās principiem;

c) daudzfaktoru autentifikācijas izmantošana par normu tīklu un informācijas sistēmās;

d) kriptogrāfijas un šifrēšanas, jo īpaši galšifrēšanas, kā arī droša digitālā paraksta izmantošana;

e) attiecīgā gadījumā droši balss, video un teksta sakari un drošas ārkārtas situācijas sakaru sistēmas Savienības vienībā;

f) proaktīvi pasākumi ļaunprogrammatūras un spiegprogrammatūras atklāšanai un izņemšanai;

g) programmatūras piegādes ķēdes drošības izveide uz programmatūras drošas izstrādes un izvērtēšanas kritēriju pamata;

h) tādu kiberdrošības mācību programmu izveide un pieņemšana, kas ir samērīgas ar Savienības vienības visaugstākā līmeņa vadībai un tehniskajiem un operatīvajiem darbiniekiem, kam uzdots nodrošināt rezultatīvu šīs regulas īstenošanu, noteiktajiem uzdevumiem un vēlamajām spējām;

i) regulāra darbinieku apmācība kiberdrošības jomā;

j) attiecīgā gadījumā dalība savstarpējās savienotības riska analīzē Savienības vienību starpā;

k) iepirkuma noteikumu uzlabošana nolūkā veicināt vienādu augstu kiberdrošības līmeni, kas darāms:

   i) likvidējot līgumiskos šķēršļus, kuri ierobežo to, kā IKT pakalpojumu sniedzēji var informēt *CERT-EU* par incidentiem, ievainojamībām un kiberdraudiem;

   ii) ievērojot līgumiskos pienākumus ziņot par incidentiem, ievainojamībām un kiberdraudiem, kā arī ieviest mehānismus pienācīgai reaģēšanai uz incidentiem un to uzraudzībai.

9. pants

Kiberdrošības plāni

1. Pēc saskaņā ar 7. pantu veiktā kiberdrošības gatavības novērtējuma pabeigšanas un ņemot vērā aktīvus un kiberdrošības riskus, kas konstatēti satvarā, kā arī kiberdrošības riska pārvaldības pasākumos, kuri veikti saskaņā ar 8. pantu, katras Savienības vienības visaugstākā līmeņa vadība bez liekas kavēšanās un katrā ziņā līdz 2026. gada 8. janvārim apstiprina kiberdrošības plānu. Kiberdrošības plāna mērķis ir palielināt Savienības vienības vispārējo kiberdrošību, un tādējādi tas sekmē vienāda augsta kiberdrošības līmeņa uzlabošanu Savienības vienībās. Kiberdrošības plānā iekļauj vismaz kiberdrošības riska pārvaldības pasākumus, kas veikti saskaņā ar 8. pantu. Kiberdrošības plānu pārskata ik divus gadus vai vajadzības gadījumā biežāk pēc kiberdrošības gatavības novērtējumiem, ko veic saskaņā ar 7. pantu, vai katras būtiskas satvara pārskatīšanas.

2. Kiberdrošības plānā iekļauj Savienības vienības kiberkrīžu pārvaldības plānu lieliem incidentiem.

3. Savienības vienība savu pabeigto kiberdrošības plānu iesniedz saskaņā ar 10. pantu izveidotajai Iestāžu kiberdrošības padomei.

III NODAĻA

IESTĀŽU KIBERDROŠĪBAS PADOME

10. pants

Iestāžu kiberdrošības padome

1. Ar šo tiek izveidota Iestāžu kiberdrošības padome (IKP).

2. IKP ziņā ir:

a) uzraudzīt un atbalstīt šīs regulas īstenošanu Savienības vienībās;

b) uzraudzīt *CERT-EU* vispārējo prioritāšu un mērķu īstenošanu un noteikt *CERT-EU* stratēģisko virzienu.

3. IKP sastāvā ir:

a) viens pārstāvis, ko ieceļ katrs no turpmāk minētajiem:

   i) Eiropas Parlaments;

   ii) Eiropadome;

   iii) Eiropas Savienības Padome;

   iv) Komisija;

   v) Eiropas Savienības Tiesa;

   vi) Eiropas Centrālā banka;

   vii) Revīzijas palāta;

   viii) Eiropas Ārējās darbības dienests;

   ix) Eiropas Ekonomikas un sociālo lietu komiteja;

   x) Eiropas Reģionu komiteja;

   xi) Eiropas Investīciju banka;

   xii) Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs;

   xiii) *ENISA*;

   xiv) Eiropas Datu aizsardzības uzraudzītājs (EDAU);

   xv) Eiropas Savienības Kosmosa programmas aģentūra;

b) trīs pārstāvji, ko pēc IKT Padomdevējas komitejas ierosinājuma ieceļ ES aģentūru tīkls (ESAT), lai pārstāvētu tādu Savienības struktūru, biroju un aģentūru intereses, kas uztur savu IKT vidi un kas nav minētas a) apakšpunktā.

IKP pārstāvētās Savienības vienības tiecas iecelto pārstāvju vidū nodrošināt dzimumu līdzsvaru.

4. IKP locekļiem var palīdzēt aizvietotājs. Citus 3. punktā minēto Savienības vienību vai citu Savienības vienību pārstāvjus priekšsēdētājs var uzaicināt piedalīties IKP sanāksmēs bez balsošanas tiesībām.

5. *CERT-EU* vadītājs un saskaņā ar attiecīgi Direktīvas (ES) 2022/2555 14., 15. un 16. pantu izveidotās sadarbības grupas, *CSIRT* tīkla un *EU-CyCLONe* priekšsēdētāji vai to aizstājēji var piedalīties IKP sanāksmēs kā novērotāji. Ārkārtas gadījumos IKP saskaņā ar savu iekšējo reglamentu var nolemt citādi.

6. IKP pieņem iekšējo reglamentu.

7. Saskaņā ar iekšējo reglamentu IKP no visu locekļu vidus uz trim gadiem ieceļ priekšsēdētāju. Priekšsēdētāja aizvietotājs kļūst par pilntiesīgu IKP locekli uz tādu pašu laika periodu.

8. IKP tiekas vismaz trīs reizes gadā pēc tās priekšsēdētāja iniciatīvas, pēc *CERT-EU* pieprasījuma vai pēc kāda tās locekļa lūguma.

9. Katram IKP loceklim ir viena balss. IKP lēmumus pieņem ar vienkāršu balsu vairākumu, izņemot gadījumos, kad šajā regulā paredzēts citādi. IKP priekšsēdētājs nebalso, ja vien nav vienāds balsu sadalījums – tādā gadījumā priekšsēdētāja balss ir izšķirošā.

10. IKP var izmantot vienkāršotu rakstisku procedūru, ko sāk saskaņā ar tās iekšējo reglamentu. Minētajā procedūrā relevantais lēmums tiek uzskatīts par apstiprinātu priekšsēdētāja noteiktajā periodā, ja vien kāds loceklis nav iebildis.

11. IKP sekretariātu nodrošina Komisija, un tas atskaitās IKP priekšsēdētājam.

12. ESAT izvirzītie pārstāvji par IKP lēmumiem informē ESAT locekļus. Ikvienam ESAT loceklim ir tiesības informēt minētos pārstāvjus vai IKP priekšsēdētāju par jebkuru jautājumu, ko tas uzskata par tādu, kas būtu jādara zināms IKP.

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

14. Līdz 2025. gada 8. janvārim un pēc tam ik gadu IKP iesniedz Eiropas Parlamentam un Padomei ziņojumu, kurā sīki izklāstīts progress, kas panākts šīs regulas īstenošanā, un jo īpaši norādīts, cik lielā mērā *CERT-EU* sadarbojas ar saviem partneriem katrā dalībvalstī. Minētais ziņojums ir ieguldījums divgadu ziņojumā par kiberdrošības stāvokli Savienībā, ko pieņem saskaņā ar Direktīvas (ES) 2022/2555 18. pantu.

11. pants

IKP uzdevumi

Pildot savus pienākumus, IKP jo īpaši:

a) sniedz norādes *CERT-EU* vadītājam;

b) rezultatīvi uzrauga un pārrauga šīs regulas īstenošanu un atbalsta Savienības vienības to kiberdrošības stiprināšanā, attiecīgā gadījumā arī pieprasot Savienības vienībām un *CERT-EU ad hoc* ziņojumus;

c) pēc stratēģiskām diskusijām pieņem daudzgadu stratēģiju kiberdrošības līmeņa paaugstināšanai Savienības vienībās un regulāri un vismaz ik piecus gadus novērtē to un vajadzības gadījumā to groza;

d) nosaka metodiku un organizatoriskos aspektus brīvprātīgai salīdzinošajai izvērtēšanai, ko veic Savienības vienības, lai mācītos no kopīgas pieredzes, stiprinātu savstarpējo uzticēšanos, panāktu vienādu augstu kiberdrošības līmeni, kā arī uzlabotu Savienības vienību kiberdrošības spējas, nodrošinot, ka šādu salīdzinošo izvērtēšanu veic kiberdrošības eksperti, kurus iecēlusi Savienības vienība, kas nav vērtējamā Savienības vienība, un ka metodika ir balstīta uz Direktīvas (ES) 2022/2555 19. pantu un attiecīgā gadījumā ir pielāgota Savienības vienībām;

e) uz *CERT-EU* vadītāja priekšlikuma pamata apstiprina *CERT-EU* gada darba programmu un uzrauga tās īstenošanu;

f) uz *CERT-EU* vadītāja priekšlikuma pamata apstiprina *CERT-EU* pakalpojumu katalogu un visus tā turpmākos atjauninājumus;

g) uz *CERT-EU* vadītāja priekšlikuma pamata apstiprina *CERT-EU* darbību ieņēmumu un izdevumu gada finanšu plānu, kas ietver arī personāla sastāvu;

h) uz *CERT-EU* vadītāja priekšlikuma pamata apstiprina pakalpojumu līmeņa vienošanos nosacījumus;

i) izskata un apstiprina *CERT-EU* vadītāja sagatavoto gada pārskatu par *CERT-EU* darbībām un līdzekļu pārvaldību;

j) apstiprina un uzrauga *CERT-EU* galvenos snieguma rādītājus (KPI), kas noteikti uz *CERT-EU* vadītāja priekšlikuma pamata;

k) apstiprina sadarbības kārtību, pakalpojumu līmeņa vienošanās vai līgumus starp *CERT-EU* un citām vienībām atbilstoši 18. pantam;

l) pieņem vadlīnijas un ieteikumus, balstoties uz *CERT-EU* priekšlikumu saskaņā ar 14. pantu, un uzdod *CERT-EU* izdot, atsaukt vai grozīt vadlīniju vai ieteikumu priekšlikumu vai aicinājumu rīkoties;

m) veido tehniskās padomdevējas grupas ar konkrētiem uzdevumiem palīdzēt veikt IKP darbu, apstiprina to darba uzdevumus un ieceļ to attiecīgos priekšsēdētājus;

n) saņem un novērtē dokumentus un ziņojumus, ko Savienības vienības iesniegušas saskaņā ar šo regulu, piemēram, kiberdrošības gatavības novērtējumus;

o) veicina neformālas grupas izveidi, kurā ietilpst vienību vietējie kiberdrošības speciālisti, kuru atbalsta *ENISA* un kuras mērķis ir apmainīties ar paraugpraksēm un informāciju, kas saistīta ar šīs regulas īstenošanu;

p) ņemot vērā *CERT-EU* sniegto informāciju par identificētajiem kiberdrošības riskiem un gūto pieredzi, uzrauga Savienības vienību IKT vižu savienotības pasākumu pietiekamību un konsultē par iespējamiem uzlabojumiem;

q) izstrādā kiberkrīžu pārvaldības plānu, lai operacionālā līmenī atbalstītu tādu lielu incidentu koordinētu pārvaldību, kas ietekmē Savienības vienības, un veicinātu regulāru apmaiņu ar relevantu informāciju, jo īpaši par lielu incidentu ietekmi un smagumu un iespējamiem veidiem, kā mazināt to sekas;

r) koordinē 9. panta 2. punktā minēto individuālo Savienības vienību kiberkrīžu pārvaldības plānu pieņemšanu;

s) ņemot vērā rezultātus, ko devuši Direktīvas (ES) 2022/2555 22. pantā minētie Savienības līmeņa koordinētie kritisko piegādes ķēžu riska novērtējumi, pieņem ieteikumus par 8. panta 2. punkta pirmās daļas m) apakšpunktā minēto piegādes ķēdes drošību, lai palīdzētu Savienības vienībām pieņemt rezultatīvus un samērīgus kiberdrošības riska pārvaldības pasākumus.

12. pants

Atbilstība

1. IKP saskaņā ar 10. panta 2. punktu un 11. pantu rezultatīvi uzrauga šīs regulas un pieņemto vadlīniju, ieteikumu un aicinājumu rīkoties īstenošanu Savienības vienībās. IKP var pieprasīt no Savienības vienībām šim nolūkam nepieciešamo informāciju vai dokumentāciju. Kas attiecas uz atbilstības nodrošināšanas pasākumu pieņemšanu saskaņā ar šo pantu, ja attiecīgā Savienības vienība ir tieši pārstāvēta IKP, minētajai Savienības vienībai nav balsstiesību.

2. Ja IKP konstatē, ka Savienības vienība nav rezultatīvi īstenojusi šo regulu vai vadlīnijas, ieteikumus vai aicinājumus rīkoties, kas izdoti saskaņā ar šo regulu, tā, neskarot attiecīgās Savienības vienības iekšējās procedūras un pēc tam, kad ir devusi iespēju attiecīgajai vienībai izteikt komentārus, var:

a) sniegt attiecīgajai Savienības vienībai pamatotu atzinumu, kur norādītas konstatētās šīs regulas īstenošanas nepilnības;

b) pēc apspriešanās ar *CERT-EU* izdot vadlīnijas attiecīgajai Savienības vienībai, kā noteiktā laikā nodrošināt, ka tās satvars, kiberdrošības riska pārvaldības pasākumi, kiberdrošības plāns un ziņošana atbilst šai regulai;

c) izdot brīdinājumu noteiktā laikā risināt identificētos trūkumus, tostarp ieteikumus grozīt pasākumus, ko attiecīgā Savienības vienība pieņēmusi saskaņā ar šo regulu;

d) sniegt attiecīgajai Savienības vienībai pamatotu paziņojumu, ja saskaņā ar c) apakšpunktu izdotajā brīdinājumā identificētie trūkumi noteiktajā laikā nav pietiekami novērsti;

e) izdot:

i) ieteikumu veikt revīziju; vai

ii) pieprasījumu par to, lai revīziju veiktu trešās puses revīzijas dienests;

f) attiecīgā gadījumā par iespējamo neatbilstību informēt Revīzijas palātu tās pilnvaru ietvaros;

g) izdot ieteikumu visām dalībvalstīm un Savienības vienībām uz laiku apturēt datu plūsmas uz attiecīgo Savienības vienību.

Pirmās daļas c) apakšpunkta nolūkos brīdinājuma saņēmēju loku pienācīgi ierobežo, ja tas nepieciešams kiberdrošības riska dēļ.

Saskaņā ar pirmo daļu izdotus brīdinājumus un ieteikumus adresē attiecīgās Savienības vienības visaugstākā līmeņa vadībai.

3. Ja IKP ir pieņēmusi pasākumus saskaņā ar 2. punkta pirmās daļas a)–g) apakšpunktu, attiecīgā Savienības vienība sniedz detalizētu pārskatu par pasākumiem un darbībām, kas veiktas, lai novērstu iespējamos trūkumus, kurus identificējusi IKP. Savienības vienība šo detalizēto pārskatu iesniedz saprātīgā termiņā, par ko vienojas ar IKP.

4. Ja IKP uzskata, ka Savienības vienība izdara pastāvīgu šīs regulas pārkāpumu, kas tieši izriet no Savienības ierēdņa vai cita darbinieka, tostarp augstākajā vadības līmenī, darbības vai bezdarbības, IKP pieprasa attiecīgajai Savienības vienībai veikt pienācīgus pasākumus, tostarp apsvērt disciplināra rakstura pasākumu veikšanu, saskaņā ar noteikumiem un procedūrām, ko paredz Civildienesta noteikumi un citi piemērojamie noteikumi un procedūras. Šajā nolūkā IKP nodod attiecīgajai Savienības vienībai vajadzīgo informāciju.

5. Ja Savienības vienības ziņo, ka tās nespēj ievērot 6. panta 1. punktā un 8. panta 1. punktā minētos termiņus, pienācīgi pamatotos gadījumos, ņemot vērā Savienības vienības lielumu, IKP var atļaut tos pagarināt.

IV NODAĻA

CERT-EU

13. pants

***CERT-EU* misija un uzdevumi**

1. *CERT-EU* misija ir dot ieguldījumu Savienības vienību neklasificētās IKT vides drošībā, sniedzot tām padomus par kiberdrošību, palīdzot novērst, atklāt, risināt, mitigēt incidentus, reaģēt uz tiem un atgūties no tiem, kā arī rīkojoties kā to kiberdrošības informācijas apmaiņas un reaģēšanas uz incidentiem koordinēšanas centram.

2. *CERT-EU* vāc, pārvalda, analizē un ar Savienības vienībām kopīgo informāciju par kiberdraudiem, ievainojamībām un incidentiem neklasificētā IKT infrastruktūrā. *CERT-EU* koordinē reaģēšanu uz incidentiem starpiestāžu un Savienības vienību līmenī, citstarp nodrošinot specializētu operacionālo palīdzību vai koordinējot tās nodrošināšanu.

3. Lai palīdzētu Savienības vienībām, *CERT-EU* veic šādus uzdevumus:

a) sniedz tām atbalstu šīs regulas īstenošanā un palīdz koordinēt tās īstenošanu, izmantojot 14. panta 1. punktā uzskaitītos pasākumus vai IKP pieprasītus *ad hoc* ziņojumus;

b) piedāvā *CSIRT* standarta pakalpojumus Savienības vienībām ar tā pakalpojumu katalogā aprakstīto kiberdrošības pakalpojumu pakotni (pamatpakalpojumi);

c) uztur partneru un kolēģu tīklu, lai sekmētu pakalpojumu sniegšanu, kā norādīts 17. un 18. pantā;

d) vērš IKP uzmanību uz visām problēmām, kas saistītas ar šīs regulas īstenošanu un vadlīniju, ieteikumu un aicinājumu rīkoties īstenošanu;

e) izmantojot 2. punktā minēto informāciju, ciešā sadarbībā ar *ENISA* sekmē Savienības kibersituācijas apzināšanos;

f) koordinē lielu incidentu pārvaldību;

g) attiecībā pret Savienības vienībām darbojas ekvivalenti koordinatoram, kas izraudzīts koordinētas ievainojamības izpaušanas nolūkā saskaņā ar Direktīvas (ES) 2022/2555 12. panta 1. punktu;

h) pēc Savienības vienības pieprasījuma nodrošina minētās Savienības vienības publiski piekļūstamu tīklu un informācijas sistēmu proaktīvu neintruzīvu skenēšanu.

Šā punkta pirmās daļas e) apakšpunktā minēto informāciju attiecīgos un piemērotos gadījumos un ievērojot pienācīgus konfidencialitātes nosacījumus, kopīgo ar IKP, *CSIRT* tīklu un Eiropas Savienības Izlūkošanas un situāciju centru (*EU INTCEN*).

4. *CERT-EU* var saskaņā ar attiecīgi 17. vai 18. pantu sadarboties ar relevantajām kiberdrošības kopienām Savienībā un tās dalībvalstīs, arī šādās jomās:

a) gatavība, incidentu risināšanas koordinēšana, informācijas apmaiņa un reaģēšana uz krīzi tehniskā līmenī ar Savienības vienībām saistītos gadījumos;

b) operacionālā sadarbība *CSIRT* tīkla aspektā, arī attiecībā uz savstarpējo palīdzību;

c) kiberdraudu izlūkdati, arī situācijas apzināšanās;

d) jebkurš gadījums, kad vajadzīga *CERT-EU* tehniskā kiberdrošības lietpratība.

5. *CERT-EU* savu kompetenču robežās iesaistās strukturētā sadarbībā ar *ENISA* attiecībā uz spēju veidošanu, operacionālo sadarbību un kiberdraudu ilgtermiņa stratēģisko analīzi saskaņā ar Regulu (ES) 2019/881. *CERT-EU* var sadarboties un apmainīties ar informāciju ar Eiropola Eiropas Kibernoziedzības apkarošanas centru.

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

a) pakalpojumi, kas sekmē Savienības vienību IKT vides kiberdrošību un nav minēti 3. punktā, pamatojoties uz pakalpojumu līmeņa vienošanos un atkarībā no pieejamajiem resursiem, jo īpaši plaša spektra tīkla uzraudzība, tostarp nepārtrauktu uzraudzību zemākajā līmenī attiecībā uz īpaši bīstamiem kiberdraudiem;

b) pakalpojumi, kas sekmē Savienības vienību kiberdrošības darbības vai projektus, izņemot pakalpojumus to IKT vides aizsardzībai, pamatojoties uz rakstiskiem līgumiem un ar iepriekšēju IKP apstiprinājumu;

c) pēc pieprasījuma proaktīva attiecīgās Savienības vienības tīklu un informācijas sistēmu skenēšana nolūkā atklāt ievainojamības, kam var būt būtiska ietekme;

d) pakalpojumi, kas sekmē IKT vides drošību organizācijās, kuras nav Savienības vienības, bet cieši sadarbojas ar Savienības vienībām, piemēram, pilda ar Savienības tiesību aktiem uzticētus uzdevumus vai pienākumus, pamatojoties uz rakstiskiem līgumiem un ar iepriekšēju IKP apstiprinājumu.

Attiecībā uz pirmās daļas d) apakšpunktu *CERT-EU* var izņēmuma kārtā slēgt pakalpojumu līmeņa vienošanās ar vienībām, kas nav Savienības vienības, ja IKP tam iepriekš piekritusi.

7. *CERT-EU* organizē kiberdrošības mācības, var piedalīties tajās vai ieteikt piedalīties esošās mācībās attiecīgā gadījumā ciešā sadarbībā ar *ENISA*, lai pārbaudītu Savienības vienību kiberdrošības līmeni.

8. *CERT-EU* var sniegt palīdzību Savienības vienībām attiecībā uz incidentiem tīklu un informācijas sistēmās, kas rīkojas ar ESKI, ja to nepārprotami pieprasa attiecīgās Savienības vienības saskaņā ar savām attiecīgajām procedūrām. *CERT-EU* palīdzības sniegšana saskaņā ar šo punktu neskar piemērojamos noteikumus par klasificētas informācijas aizsardzību.

9. *CERT-EU* informē Savienības vienības par savām incidentu risināšanas procedūrām un procesiem.

10. *CERT-EU*, ievērojot augstu konfidencialitātes un uzticamības līmeni un izmantojot pienācīgos sadarbības mehānismus un ziņošanas kārtību, sniedz relevantu un anonimizētu informāciju par lieliem incidentiem un to, kā tie risināti. Minēto informāciju iekļauj 10. panta 14. punktā minētajā ziņojumā.

11. *CERT-EU* sadarbībā ar EDAU atbalsta attiecīgās Savienības vienības, kad tās risina incidentus, kuru rezultātā notiek personas datu aizsardzības pārkāpumi, neskarot kompetenci un uzdevumus, kas EDAU ir kā uzraudzības iestādei saskaņā ar Regulu (ES) 2018/1725.

12. Ja Savienības vienību rīcībpolitikas nodaļas to skaidri lūdz, *CERT-EU* var sniegt tehniskus padomus vai tehnisku ieguldījumu relevantos rīcībpolitiskos jautājumos.

14. pants

Vadlīnijas, ieteikumi un aicinājumi rīkoties

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

a) aicinājumus rīkoties, kuros apraksta neatliekamus drošības pasākumus, ko Savienības vienības tiek mudinātas veikt noteiktā laikā;

b) IKP adresētus priekšlikumus vadlīnijām, kas paredzētas visām Savienības vienībām vai kādai to grupai;

c) IKP adresētus priekšlikumus ieteikumiem, kas paredzēti atsevišķām Savienības vienībām.

Attiecībā uz pirmās daļas a) apakšpunktu attiecīgā Savienības vienība bez liekas kavēšanās pēc uzaicinājuma rīkoties saņemšanas informē *CERT-EU* par to, kā neatliekamie drošības pasākumi piemēroti.

2. Vadlīnijas un ieteikumi var ietvert:

a) kopīgas metodikas un modeli Savienības vienību kiberdrošības gatavības novērtēšanai, tostarp attiecīgās skalas vai KPI, kas kalpo par atsauces punktu pastāvīgai kiberdrošības uzlabošanai Savienības vienībās un atvieglo prioritāšu noteikšanu kiberdrošības jomām un pasākumiem, ņemot vērā vienību kiberdrošības pozīciju;

b) kiberdrošības riska pārvaldības un kiberdrošības riska pārvaldības pasākumu kārtību vai uzlabojumus;

c) kiberdrošības gatavības novērtējumu un kiberdrošības plānu kārtību;

d) attiecīgā gadījumā plaši lietotu tehnoloģiju, arhitektūras, atvērtā pirmkoda un saistītu paraugprakšu izmantošanu ar mērķi panākt sadarbspēju un kopējus standartus, tostarp koordinētu pieeju piegādes ķēdes drošībai;

e) attiecīgā gadījumā informāciju, kas atvieglo kopīgā iepirkuma instrumentu izmantošanu relevanto kiberdrošības pakalpojumu un produktu iegādei no piegādātājiem trešām pusēm;

f) informācijas kopīgošanas kārtību saskaņā ar 20. pantu.

15. pants

CERT-EU vadītājs

1. Komisija pēc divu trešdaļu IKP locekļu vairākuma apstiprinājuma saņemšanas ieceļ *CERT-EU* vadītāju. Visos iecelšanas procedūras posmos apspriežas ar IKP, jo īpaši attiecībā uz paziņojuma par vakanci sagatavošanu, pieteikumu izskatīšanu un atlases komitejas iecelšanu šai amata vietai. Atlases procedūra, tostarp galīgo to kandidātu saraksts, no kuru vidus jāieceļ *CERT-EU* vadītājs, nodrošina taisnīgu katra dzimuma pārstāvību, ņemot vērā iesniegtos pieteikumus.

2. *CERT-EU* vadītājs ir atbildīgs par pareizu *CERT-EU* darbību un IKP vadībā darbojas savas kompetences ietvaros. *CERT-EU* vadītājs regulāri ziņo IKP priekšsēdētājam un pēc IKP pieprasījuma iesniedz tai *ad hoc* ziņojumus.

3. *CERT-EU* vadītājs palīdz atbildīgajam deleģētajam kredītrīkotājam sagatavot gada darbības pārskatu, kas satur finanšu un vadības informāciju, tostarp kontroļu rezultātus, un ko izstrādā saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES, Euratom) 2018/1046 ([9]) 74. panta 9. punktu, un regulāri ziņo deleģētajam kredītrīkotājam par to pasākumu īstenošanu, attiecībā uz kuriem *CERT-EU* vadītājam pastarpināti deleģētas pilnvaras.

4. *CERT-EU* vadītājs ik gadu sagatavo savu darbību administratīvo ieņēmumu un izdevumu finanšu plānu, gada darba programmas priekšlikumu, *CERT-EU* pakalpojumu kataloga priekšlikumu un pārskatīto pakalpojumu kataloga redakciju priekšlikumus, priekšlikumus par pakalpojumu līmeņa vienošanos kārtību un priekšlikumus par *CERT-EU* KPI, kas IKP jāapstiprina saskaņā ar 11. pantu. Pārskatot *CERT-EU* pakalpojumu katalogā iekļauto pakalpojumu sarakstu, *CERT-EU* vadītājs ņem vērā *CERT-EU* piešķirtos resursus.

5. *CERT-EU* vadītājs vismaz ik gadu iesniedz IKP un IKP priekšsēdētājam ziņojumus par *CERT-EU* darbībām un sniegumu pārskata periodā, tostarp par budžeta izpildi, pakalpojumu līmeņa vienošanos un noslēgtajiem rakstiskajiem nolīgumiem, sadarbību ar partneriem un darbinieku komandējumiem, tostarp 11. pantā minētos ziņojumus. Minētajos ziņojumos iekļauj nākamā perioda darba programmu, ieņēmumu un izdevumu finanšu plānojumu, tostarp personāla sastāvu, *CERT-EU* pakalpojumu kataloga plānoto atjaunināšanu un novērtējumu par šādu atjauninājumu paredzamo ietekmi uz finanšu resursiem un cilvēkresursiem.

16. pants

Finanšu un personāla jautājumi

1. *CERT-EU* integrē Komisijas ģenerāldirektorāta administratīvajā struktūrā, lai gūtu labumu no Komisijas administratīvās, finanšu pārvaldības un grāmatvedības atbalsta struktūrām, vienlaikus *CERT-EU* joprojām paliekot autonomam starpiestāžu pakalpojumu sniedzējam visām Savienības vienībām. Komisija informē IKP par *CERT-EU* administratīvo izvietojumu un par jebkādām tā izmaiņām. Komisija regulāri un katrā ziņā pirms ikvienas daudzgadu finanšu shēmas izveides saskaņā ar LESD 312. pantu pārskata ar *CERT-EU* saistītos administratīvos pasākumus, lai varētu attiecīgi rīkoties. Pārskatīšanā izskata iespēju pārveidot *CERT-EU* par Savienības biroju.

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

([9]) 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.).

3. *CERT-EU* uzdevumus un darbības, tostarp pakalpojumus, ko *CERT-EU* atbilstoši 13. panta 3., 4., 5. un 7. punktam un 14. panta 1. punktam sniedz Savienības vienībām, kuras finansē no daudzgadu finanšu shēmas izdevumu kategorijas, kas paredzēta Eiropas publiskajai pārvaldei, finansē no īpašas Komisijas budžeta pozīcijas. *CERT-EU* paredzētās amata vietas norāda Komisijas štatu saraksta zemsvītras piezīmē.

4. Savienības vienības, kas nav minētas šā panta 3. punktā, veic ikgadēju finansiālu iemaksu *CERT-EU*, lai apmaksātu atbilstoši minētajam punktam sniegtos *CERT-EU* pakalpojumus. Iemaksas balstās uz IKP orientējošo informāciju, un *CERT-EU* par tām vienojas ar katru Savienības vienību, izmantojot pakalpojumu līmeņa vienošanos. Iemaksas ir taisnīga un samērīga daļa no kopējām sniegto pakalpojumu izmaksām. Tās saņem šā panta 3. punktā minētā atsevišķā budžeta pozīcija kā iekšējus piešķirtos ieņēmumus, kā paredzēts Eiropas Parlamenta un Padomes Regulas (ES, Euratom) 2018/1046 21. panta 3. punkta c) apakšpunktā.

5. Regulas 13. panta 6. punktā paredzēto pakalpojumu izmaksas atgūst no Savienības vienībām, kas saņem *CERT-EU* pakalpojumus. Ieņēmumus novirza uz budžeta izmaksu pozīcijām.

17. pants

CERT-EU sadarbība ar partneriem dalībvalstīs

1. *CERT-EU* bez liekas kavēšanās sadarbojas un apmainās ar informāciju ar partneriem dalībvalstīs, jo īpaši *CSIRT*, kas ieceltas vai izveidotas saskaņā ar Direktīvas (ES) 2022/2555 10. pantu, vai attiecīgā gadījumā kompetentajām iestādēm un vienotajiem kontaktpunktiem, kas iecelti vai izveidoti saskaņā ar minētās direktīvas 8. pantu, attiecībā uz incidentiem, kiberdraudiem, ievainojamībām, gandrīz notikušiem notikumiem, iespējamajiem pretpasākumiem, kā arī paraugpraksēm un attiecībā uz visiem jautājumiem, kas ir relevanti Savienības vienību IKT vižu aizsardzībai, arī izmantojot Direktīvas (ES) 2022/2555 15. pantā minēto *CSIRT* tīklu. *CERT-EU* atbalsta Komisiju saskaņā ar Direktīvas (ES) 2022/2555 16. pantu izveidotajā *EU-CyCLONe* koordinētas lielu kiberdrošības incidentu un krīžu pārvaldības jomā.

2. Kad *CERT-EU* uzzina par būtisku incidentu, kas noticis kādas dalībvalsts teritorijā, tā bez kavēšanās saskaņā ar 1. punktu ziņo visiem relevantajiem partneriem minētajā dalībvalstī.

3. Ar noteikumu, ka personas dati tiek aizsargāti saskaņā ar piemērojamajiem Savienības datu aizsardzības tiesību aktiem, *CERT-EU* bez nepamatotas kavēšanās bez skartās Savienības vienības atļaujas apmainās ar attiecīgo incidentu raksturojošu informāciju ar partneriem dalībvalstīs, kas ir relevanta nolūkā atvieglot līdzīgu kiberdraudu vai incidentu atklāšanu vai veicināt incidenta analīzi. *CERT-EU* apmainās ar incidentu raksturojošu informāciju, kas atklāj incidenta mērķa identitāti, tikai kādā no šādiem gadījumiem:

a) skartā Savienības vienība tam piekrīt;

b) skartā Savienības vienība nesniedz a) apakšpunktā paredzēto piekrišanu, bet skartās Savienības vienības identitātes izpaušana palielinātu varbūtību, ka tiks novērsti vai mitigēti incidenti citviet;

c) skartā Savienības vienība jau ir publiski izpaudusi, ka tā ir skarta.

Lēmumus apmainīties ar incidentu raksturojošu informāciju, kas izpauž incidenta mērķa identitāti saskaņā ar pirmās daļas b) apakšpunktu, apstiprina *CERT-EU* vadītājs. Pirms šāda lēmuma izdošanas *CERT-EU* rakstiski sazinās ar skarto Savienības vienību, skaidri paskaidrojot, kā tās identitātes izpaušana palīdzētu novērst vai mitigēt incidentus citviet. *CERT-EU* vadītājs sniedz paskaidrojumu un skaidri lūdz Savienības vienībai noteiktā laikā norādīt, vai tā piekrīt. *CERT-EU* vadītājs informē Savienības vienību arī par to, ka, ņemot vērā sniegto paskaidrojumu, viņš patur tiesības informāciju izpaust pat bez piekrišanas. Pirms informācijas izpaušanas informē skarto Savienības vienību.

18. pants

CERT-EU sadarbība ar citiem partneriem

1. Attiecībā uz rīkiem un metodēm, piemēram, paņēmieniem, taktiku, procedūrām un paraugpraksēm, kā arī kiberdraudiem un ievainojamībām *CERT-EU* var sadarboties ar partneriem Savienībā, kas nav 17. pantā minētie partneri un uz ko attiecas Savienības kiberdrošības prasības, tostarp nozarspecifiskiem industrijas partneriem. Lai sadarbotos ar šādiem partneriem, *CERT-EU* katrā atsevišķā gadījumā iepriekš saņem IKP apstiprinājumu. Ja *CERT-EU* iedibina sadarbību ar šādiem partneriem, tā informē visus relevantos 17. panta 1. punktā minētos partnerus tajā dalībvalstī, kurā partneris atrodas. Attiecīgā un piemērotā gadījumā šādu sadarbību un tās nosacījumus, arī attiecībā uz kiberdrošību, datu aizsardzību un informācijas apstrādi, nosaka ar īpašiem konfidencialitātes pasākumiem, piemēram, līgumu vai administratīvu vienošanos. Konfidencialitātes pasākumi IKP nav iepriekš jāapstiprina, tomēr IKP priekšsēdētāju par tiem informē. Ja ir steidzama un neatliekama vajadzība apmainīties ar kiberdrošības informāciju Savienības vienību vai citas puses interesēs, *CERT-EU* var to darīt ar vienību, kuras konkrētā kompetence, spējas un lietpratība ir pamatoti nepieciešamas, lai palīdzētu risināt šādu steidzamu un neatliekamu vajadzību, pat ja *CERT-EU* ar minēto vienību nav vienojusies par konfidencialitāti. Šādos gadījumos *CERT-EU* nekavējoties informē IKP priekšsēdētāju un ziņo IKP, izmantojot regulārus ziņojumus vai sanāksmes.

2. *CERT-EU* var sadarboties ar partneriem, piemēram, komercuzņēmumiem, tostarp nozarspecifiskām industrijas vienībām, starptautiskām organizācijām, trešo valstu nacionālām vienībām un atsevišķiem ekspertiem, lai vāktu informāciju par vispārējiem un konkrētiem kiberdraudiem, gandrīz notikušiem notikumiem, ievainojamībām un iespējamiem pretpasākumiem. Lai plašāk sadarbotos ar šādiem partneriem, *CERT-EU* katrā atsevišķā gadījumā iepriekš saņem IKP apstiprinājumu.

3. Ar incidenta skartās Savienības vienības piekrišanu un ar noteikumu, ka ir noslēgta informācijas neizpaušanas vienošanās vai līgums ar relevanto partneri, *CERT-EU* var sniegt incidentu raksturojošu informāciju partneriem, kas minēti 1. un 2. punktā, vienīgi nolūkā no tiem saņemt palīdzību tās analīzē.

V NODAĻA

SADARBĪBA UN ZIŅOŠANAS PIENĀKUMI

19. pants

Rīkošanās ar informāciju

1. Savienības vienības un *CERT-EU* ievēro dienesta noslēpuma glabāšanas pienākumu saskaņā ar LESD 339. pantu vai līdzvērtīgu piemērojamu regulējumu.

2. Pieprasījumiem par publisku piekļuvi *CERT-EU* turējumā esošiem dokumentiem piemēro Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1049/2001 ([10]), tostarp minētajā regulā noteikto pienākumu apspriesties ar citām Savienības vienībām vai attiecīgā gadījumā dalībvalstīm, ja pieprasījums attiecas uz to dokumentiem.

3. Savienības vienības un *CERT-EU* ar informāciju rīkojas atbilstoši piemērojamajiem noteikumiem par informācijas drošību.

([10]) 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.).

20. pants

Kiberdrošības informācijas kopīgošanas kārtība

1. Savienības vienības var brīvprātīgi ziņot un sniegt informāciju *CERT-EU* par incidentiem, kiberdraudiem, gandrīz notikušiem notikumiem un ievainojamībām, kas tās skar. *CERT-EU* nodrošina, ka nolūkā atvieglot informācijas kopīgošanu ar Savienības vienībām ir pieejami efektīvi saziņas līdzekļi, kam raksturīga augsta līmeņa izsekojamība, konfidencialitāte un uzticamība. Paziņojumu apstrādē *CERT-EU* var noteikt obligātajiem paziņojumiem prioritāti pār brīvprātīgajiem paziņojumiem. Neskarot 12. pantu, brīvprātīgā paziņošana ziņotājai Savienības vienībai neuzliek nekādus papildu pienākumus, kas uz to neattiektos, ja tā nebūtu iesniegusi paziņojumu.

2. Lai pildītu savu misiju un uzdevumus, kas piešķirti ar 13. pantu, *CERT-EU* var pieprasīt Savienības vienībām sniegt tai informāciju no to attiecīgajām IKT sistēmām, tostarp informāciju par kiberdraudiem, gandrīz notikušiem notikumiem, ievainojamībām, aizskāruma rādītājiem, kiberdrošības brīdinājumiem un ieteikumiem par incidentu atklāšanas kiberdrošības rīku konfigurāciju. Pieprasījuma saņēmēja Savienības vienība prasīto informāciju un tās atjauninājumus nosūta bez liekas kavēšanās.

3. *CERT-EU* var apmainīties ar Savienības vienībām ar incidentu raksturojošu informāciju, kas izpauž incidentā skartās Savienības vienības identitāti, ar noteikumu, kas skartā Savienības vienība tam piekrīt. Ja Savienības vienība piekrišanu nedod, tā sniedz *CERT-EU* šāda lēmuma pamatojumu.

4. Savienības vienības pēc pieprasījuma ar Eiropas Parlamentu un Padomi kopīgo informāciju par kiberdrošības plānu pabeigšanu.

5. Attiecīgā gadījumā IKP vai *CERT-EU* pēc pieprasījuma ar Eiropas Parlamentu un Padomi kopīgo informāciju par vadlīnijām, ieteikumiem un aicinājumiem rīkoties.

6. Šajā pantā noteiktie kopīgošanas pienākumi neattiecas uz:

a) ESKI;

b) informāciju, kuras tālāka izplatīšana ir izslēgta ar redzamu marķējumu, ja vien tās kopīgošana ar *CERT-EU* nav skaidri atļauta.

21. pants

Ziņošanas pienākumi

1. Incidentu uzskata par būtisku, ja:

a) tas ir izraisījis vai spēj izraisīt smagus attiecīgās Savienības vienības funkcionēšanas traucējumus vai finansiālus zaudējumus;

b) tas ir ietekmējis vai spēj ietekmēt citas fiziskas vai juridiskas personas, radot būtisku materiālu vai nemateriālu kaitējumu.

2. Savienības vienības iesniedz *CERT-EU*:

a) bez liekas kavēšanās un katrā ziņā 24 stundu laikā no brīža, kad uzzinājušas par būtisko incidentu, – agrīnu brīdinājumu, kurā attiecīgā gadījumā norāda, ka būtisko incidentu ir izraisījusi, domājams, nelikumīga vai ļaunprātīga rīcība un vai tam varētu būt pārvienību vai pārrobežu ietekme;

b) bez liekas kavēšanās un jebkurā gadījumā 72 stundu laikā pēc tam, kad uzzinājušas par būtisko incidentu, – paziņojumu par incidentu, kurā attiecīgā gadījumā atjaunina a) apakšpunktā minēto informāciju un norāda būtiskā incidenta sākotnējo novērtējumu, tostarp tā smagumu un ietekmi, kā arī, ja pieejami, aizskāruma rādītājus;

c) pēc *CERT-EU* pieprasījuma – starpposma ziņojumu par relevantajiem statusa atjauninājumiem;

d) galīgu ziņojumu ne vēlāk kā mēnesi pēc b) apakšpunktā minētā paziņojuma par incidentu iesniegšanas, un tajā iekļauj:

i) detalizētu incidenta aprakstu, arī par tā smagumu un ietekmi;

ii) draudu veidu vai pamatcēloni, kas, ticamākais, izraisījis incidentu;

iii) piemērotos un notiekošos mitigācijas pasākumus;

iv) attiecīgā gadījumā incidenta pārrobežu vai pārvienību ietekmi;

e) ja šā punkta d) apakšpunktā minētā galīgā ziņojuma iesniegšanas laikā incidents vēl notiek – progresa ziņojumu tajā laikā, savukārt viena mēneša laikā pēc rīkošanās incidenta sakarā — galīgo ziņojumu.

3. Savienības vienība bez liekas kavēšanās un katrā ziņā 24 stundu laikā pēc tam, kad uzzinājusi par būtisku incidentu, informē visus relevantos 17. panta 1. punktā minētos partnerus dalībvalstī, kurā tā atrodas, par to, ka ir noticis būtisks incidents.

4. Savienības vienības cita starpā ziņo jebkādu informāciju, kas *CERT-EU* dod iespēju noteikt jebkādu būtiska incidenta pārvienību ietekmi, ietekmi uz uzņēmēju dalībvalsti vai pārrobežu ietekmi. Neskarot 12. pantu, paziņošana pati par sevi neuzliek Savienības vienībai lielāku atbildību.

5. Attiecīgā gadījumā Savienības vienības skarto tīklu un informācijas sistēmu vai citu IKT vides komponentu lietotājiem, kurus potenciāli var skart būtisks incidents vai būtisks kiberdrauds un kuriem attiecīga gadījumā jāveic mitigācijas pasākumi, bez liekas kavēšanās paziņo par jebkādiem pasākumiem vai korektīvajām darbībām, ko var veikt, reaģējot uz minēto incidentu vai draudu. Attiecīgā gadījumā Savienības vienības informē minētos lietotājus par pašu būtisko kiberdraudu.

6. Ja būtisks incidents vai būtisks kiberdrauds skar Savienības vienības tādas IKT vides tīklu un informācijas sistēmu vai komponentu, kas ir ar nolūku savienota ar citas Savienības vienības IKT vidi, *CERT-EU* izdod relevantu kiberdrošības brīdinājumu.

7. Savienības vienības pēc *CERT-EU* pieprasījuma un bez liekas kavēšanās sniedz tai digitālo informāciju, kas radusies attiecīgajos incidentos iesaistīto elektronisko ierīču izmantošanā. *CERT-EU* var sīkāk precizēt, kuri šādas informācijas veidi tai ir vajadzīgi situācijas apzināšanai un reaģēšanai uz incidentiem.

8. *CERT-EU* ik trīs mēnešus iesniedz IKP, *ENISA*, ES INTCEN un *CSIRT* tīklam kopsavilkuma ziņojumu, kas ietver anonimizētus un apkopotus datus par būtiskiem incidentiem, incidentiem, kiberdraudiem, gandrīz notikušiem notikumiem un ievainojamībām saskaņā ar 20. pantu un būtiskiem incidentiem, kas paziņoti saskaņā ar šā panta 2. punktu. Kopsavilkuma ziņojums ir ieguldījums divgadu ziņojumā par kiberdrošības stāvokli Savienībā, ko pieņem saskaņā ar Direktīvas (ES) 2022/2555 18. pantu.

9. Līdz 2024. gada 8. jūlijam IKP izdod vadlīnijas vai ieteikumus, kur sīkāk precizēta šajā pantā paredzētās ziņošanas kārtība, formāts un saturs. Sagatavojot šādas vadlīnijas vai ieteikumus, IKP ņem vērā visus īstenošanas aktus, kas pieņemti saskaņā ar Direktīvas (ES) 2022/2555 23. panta 11. punktu un nosaka informācijas veidu, formātu un paziņošanas procedūru. *CERT-EU* izplata attiecīgo tehnisko informāciju, lai Savienības vienības varētu preventīvi atklāt incidentus, reaģēt uz tiem vai veikt mitigācijas pasākumus.

10. Šajā pantā noteiktie ziņošanas pienākumi neattiecas uz:

a) ESKI;

b) informāciju, kuras tālāka izplatīšana ir izslēgta ar redzamu marķējumu, ja vien tās kopīgošana ar *CERT-EU* nav skaidri atļauta.

22. pants

Reaģēšanas uz incidentu koordinēšana un sadarbība

1. Rīkojoties kā kiberdrošības informācijas apmaiņas un reaģēšanas uz incidentiem koordinēšanas centrs, *CERT-EU* atvieglo informācijas apmaiņu par incidentiem, kiberdraudiem, ievainojamībām un gandrīz notikušiem notikumiem:

a) Savienības vienību vidū;

b) regulas 17. un 18. pantā minēto partneru vidū.

2. *CERT-EU* attiecīgā gadījumā ciešā sadarbībā ar *ENISA* veicina koordināciju starp Savienības vienībām attiecībā uz reaģēšanu uz incidentiem, tostarp:

a) ieguldījumu konsekventā ārējā komunikācijā;

b) savstarpējo atbalstu, piemēram, Savienības vienībām relevantas informācijas kopīgošanu vai palīdzības sniegšanu, attiecīgā gadījumā tieši uz vietas;

c) optimālu operacionālo resursu izmantošanu;

d) koordinēšanu ar citiem krīzes reaģēšanas mehānismiem Savienības līmenī.

3. *CERT-EU* ciešā sadarbībā ar *ENISA* atbalsta Savienības vienības attiecībā uz situācijas apzināšanos tādos aspektos kā incidenti, kiberdraudi, ievainojamības un gandrīz notikuši notikumi, kā arī relevanto kiberdrošības jomas jaunumu kopīgošanu.

4. Līdz 2025. gada 8. janvārim IKP uz *CERT-EU* priekšlikuma pamata pieņem vadlīnijas vai ieteikumus par reaģēšanas uz incidentiem koordinēšanu un sadarbību būtisku incidentu gadījumā. Ja ir aizdomas par incidenta noziedzīgo raksturu, *CERT-EU* bez liekas kavēšanās sniedz padomus, kā par šo incidentu ziņot tiesībaizsardzības iestādēm.

5. Pēc īpaša dalībvalsts pieprasījuma un ar attiecīgo Savienības vienību piekrišanu *CERT-EU* var aicināt ekspertus no 23. panta 4. punktā minētā saraksta palīdzēt reaģēt uz lielu incidentu, kam ir ietekme minētajā dalībvalstī, vai plašapmēra kiberdrošības incidentu saskaņā ar Direktīvas (ES) 2022/2555 15. panta 3. punkta g) apakšpunktu. Konkrētus noteikumus par piekļuvi Savienības vienību tehniskajiem ekspertiem un viņu izmantošanu uz *CERT-EU* priekšlikuma pamata apstiprina IKP.

23. pants

Lielu incidentu pārvaldība

1. Lai operacionālā līmenī atbalstītu tādu lielu incidentu koordinētu pārvaldību, kas ietekmē Savienības vienības, un veicinātu regulāru relevantās informācijas apmaiņu starp Savienības vienībām un ar dalībvalstīm, IKP ciešā sadarbībā ar *CERT-EU* un *ENISA* saskaņā ar 11. panta q) punktu izstrādā kiberkrīžu pārvaldības plānu, balstoties uz 22. panta 2. punktā minētajām darbībām. Kiberkrīžu pārvaldības plānā iekļauj vismaz šādus elementus:

a) koordinācijas un informācijas plūsmas kārtība starp Savienības vienībām lielu incidentu pārvaldībai operacionālā līmenī;

b) kopējas standarta operāciju procedūras (SOP);

c) lielu incidentu smaguma un krīzes izraisītāju tipiskā taksonomija;

d) regulāras mācības;

e) izmantojamie drošas saziņas kanāli.

2. Komisijas pārstāvis IKP, ievērojot kiberkrīžu pārvaldības plānu, kas izveidots saskaņā ar šā panta 1. punktu, un neskarot Direktīvas (ES) 2022/2555 16. panta 2. punkta pirmo daļu, ir kontaktpunkts relevantās informācijas kopīgošanai ar *EU-CyCLONe* lielu incidentu sakarā.

3. *CERT-EU* koordinē to, kā Savienības vienības pārvalda lielus incidentus. Tā uztur tādu pieejamās tehniskās lietpratības portfeli, kas būtu vajadzīga reaģēšanai uz incidentiem lielu incidentu gadījumā, un palīdz IKP koordinēt 9. panta 2. punktā minētos Savienības vienību kiberkrīžu pārvaldības plānus lielu incidentu gadījumiem.

4. Savienības vienības palīdz veidot tehniskās lietpratības portfeli, iesniedzot un katru gadu atjauninot to attiecīgajās organizācijās pieejamo ekspertu sarakstu, kurā norāda viņu konkrētās tehniskās prasmes.

VI NODAĻA

NOBEIGUMA NOTEIKUMI

24. pants

Sākotnējā budžeta pārdale

Lai nodrošinātu pienācīgu un stabilu *CERT-EU* darbību, Komisija var ierosināt personāla un finanšu resursu pārdali uz Komisijas budžetu izmantošanai *CERT-EU* operācijās. Pārdale stājas spēkā vienlaikus ar pirmo Savienības gada budžetu, kas pieņemts pēc šīs regulas stāšanās spēkā.

25. pants

Pārskatīšana

1. Līdz 2025. gada 8. janvārim un pēc tam ik gadu IKP ar *CERT-EU* palīdzību ziņo Komisijai par šīs regulas īstenošanu. IKP var arī sniegt Komisijai ieteikumus pārskatīt šo regulu.

2. Līdz 2027. gada 8. janvārim un pēc tam ik divus gadus Komisija novērtē šīs regulas īstenošanu un stratēģiskajā un operacionālajā līmenī gūto pieredzi un ziņo par to Eiropas Parlamentam un Padomei.

Šī punkta pirmajā daļā minētajā ziņojumā ietver 16. panta 1. punktā minēto pārskatīšanu par iespēju *CERT-EU* izveidot kā Savienības biroju.

3. Līdz 2029. gada 8. janvārim Komisija izvērtē šīs regulas darbību un iesniedz ziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai. Komisija arī izvērtē, vai ir lietderīgi šīs regulas darbības jomā iekļaut tīklu un informācijas sistēmas, kuras rīkojas ar ESKI, ņemot vērā citus Savienības tiesību aktus, kas minētajām sistēmām piemērojami. Ziņojumam vajadzības gadījumā pievieno leģislatīva akta priekšlikumu.

26. 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.

Strasbūrā, 2023. gada 13. decembrī

Eiropas Parlamenta vārdā –
priekšsēdētāja
R. METSOLA

Padomes vārdā –
priekšsēdētājs
P. NAVARRO RÍOS