Grozījums Nr. 2
Cristian-Silviu Buşoi
Rūpniecības, pētniecības un enerģētikas komitejas vārdā

Ziņojums **A9-0307/2023**
Josianne Cutajar
Pārvaldīti drošības pakalpojumi
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Regulas priekšlikums
–

EIROPAS PARLAMENTA GROZĪJUMI*

Komisijas priekšlikumā

EIROPAS PARLAMENTA UN PADOMES
REGULA (ES) 2024/...

(… gada …),

ar ko attiecībā uz pārvaldītiem drošības pakalpojumiem groza Regulu (ES) 2019/881

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

* Grozījumi: jaunais vai grozītais teksts ir norādīts treknā slīprakstā; svītrojumi ir apzīmēti ar simbolu ▌.

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[1],

pēc apspriešanās ar Reģionu komiteju,

saskaņā ar parasto likumdošanas procedūru[2],

[1] ***OV C 349, 29.9.2023., 167. lpp.***

[2] ***Eiropas Parlamenta ... nostāja [(OV ...) /(Oficiālajā Vēstnesī vēl nav publicēta)] un Padomes ... lēmums.***

tā kā:

(1) Ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/881[3] ir noteikts satvars, kurā jāizveido Eiropas kiberdrošības sertifikācijas shēmas, lai Savienībā ***informācijas un komunikācijas tehnoloģiju (IKT)*** produktiem, IKT pakalpojumiem un IKT procesiem nodrošinātu pietiekami augstu kiberdrošības līmeni, kā arī nolūkā izvairīties no iekšējā tirgus sadrumstalotības attiecībā uz kiberdrošības sertifikācijas shēmām Savienībā.

(2) Lai nodrošinātu Savienības noturību pret kiberuzbrukumiem un novērstu jebkādu ievainojamību Savienības tirgū, ar šo regulu ir paredzēts papildināt horizontālo tiesisko regulējumu, ar ko ievieš visaptverošas kiberdrošības prasības visiem produktiem ar digitāliem elementiem saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES).../...[4] (2022/0272(COD)), nosakot pamatprasības pārvaldītiem kiberdrošības pakalpojumiem un to sniegšanai un uzticamībai.

---

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 ***Eiropas Parlamenta un Padomes Regula (ES) .../... (… gada …) par ... (OV L ..., ..., ELI: ...).***

(3) Pārvaldīti drošības pakalpojumi ***ir pakalpojumi, ko sniedz pārvaldītu drošības pakalpojumu sniedzēji, kā noteikts Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2555[5] 6. panta 40. punktā. Tādēļ pārvaldītu drošības pakalpojumu definīcijai šajā regulā būtu jāatbilst pārvaldītu drošības pakalpojumu sniedzēju definīcijai Direktīvā (ES) 2022/2555. Šie*** pakalpojumi ***ietver*** tādu darbību veikšanu vai atbalstīšanu, kuras saistītas ar klientu kiberdrošības riska pārvaldību, ***un*** tie kļūst arvien nozīmīgāki kiberincidentu novēršanā un to seku mazināšanā. Līdz ar to saskaņā ar ▌ Direktīvu (ES) 2022/2555 minēto pakalpojumu sniedzēji tiek uzskatīti par būtiskām vai svarīgām vienībām, kas ir piederīgas sevišķi kritiskai nozarei. Saskaņā ar minētās direktīvas 86. apsvērumu pārvaldītu drošības pakalpojumu sniedzējiem ir īpaši svarīga loma tādās jomās kā reaģēšana uz incidentiem, ielaušanās testēšana, drošības revīzijas un konsultācijas, palīdzot vienībām to centienos novērst un atklāt incidentus, reaģēt uz tiem vai atkopties no tiem. Tomēr arī pārvaldītu pakalpojumu sniedzēji ir bijuši kiberuzbrukumu mērķis un rada īpašu risku, jo ir cieši iesaistīti savu klientu darbībās. Tāpēc būtiskām un svarīgām vienībām Direktīvas (ES) 2022/2555 nozīmē, izvēloties pārvaldīta drošības pakalpojuma sniedzēju, būtu jāievēro īpaša piesardzība.

---

5 Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību 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.).

(4) Pārvaldītu drošības pakalpojumu definīcija šīs regulas nozīmē ietver neizsmeļošu tādu pārvaldītu drošības pakalpojumu sarakstu, kuri var tikt iekļauti sertifikācijas shēmās un kuru vidū ir, piemēram, incidentu novēršana, ielaušanās testēšana, drošības revīzijas un konsultācijas saistībā ar tehnisko atbalstu. Pārvaldīti drošības pakalpojumi varētu ietvert kiberdrošības pakalpojumus, kas atbalsta sagatavotību kiberdrošības incidentiem, to novēršanu, atklāšanu, analīzi, seku mazināšanu, reaģēšanu uz tiem un atkopšanos no tiem. Par pārvaldītiem drošības pakalpojumiem varētu uzskatīt arī kiberdraudu izlūkdatu sniegšanu un riska novērtējumu, kas saistīts ar tehnisko atbalstu. Dažādiem pārvaldītiem drošības pakalpojumiem var būt atsevišķas Eiropas kiberdrošības sertifikācijas shēmas. Eiropas kiberdrošības sertifikātiem, kas izdoti saskaņā ar šādām shēmām, būtu jāattiecas uz konkrētiem pārvaldītiem drošības pakalpojumiem, kurus sniedz konkrēts šo pakalpojumu sniedzējs.

(5) Pārvaldītu drošības pakalpojumu sniedzējiem ***var būt*** svarīga loma arī ***saistībā ar*** Savienības darbībām, ar kurām ***atbalsta*** reaģēšanu un tūlītēju atkopšanos ievērojamu un plaša mēroga kiberdrošības incidentu gadījumā***, paļaujoties uz uzticamu privāto pakalpojumu sniedzēju pakalpojumiem un uz kritisko vienību testēšanu attiecībā uz iespējamām ievainojamībām, kuras pamatā ir ES riska novērtējumi***. ***Pārvaldītu drošības pakalpojumu sertifikācijai var būt nozīme*** uzticamu pakalpojumu sniedzēju ***atlasē*** ▌.

(6) Pārvaldītu drošības pakalpojumu sertifikācijai ir ne tikai būtiska nozīme ES kiberdrošības rezervju atlases procesā, bet tā ir arī īpaši svarīgs kvalitātes rādītājs privātām un publiskām struktūrām, kas plāno iegādāties šādus pakalpojumus. Ņemot vērā pārvaldīto drošības pakalpojumu kritiskumu un to sniegšanas gaitā apstrādāto datu sensitivitāti, sertifikācija varētu potenciālajiem klientiem nodrošināt svarīgas norādes un pārliecību par šo pakalpojumu uzticamību. Pārvaldītiem drošības pakalpojumiem paredzētas Eiropas sertifikācijas shēmas palīdz nepieļaut vienotā tirgus sadrumstalotību. Tādēļ šīs regulas mērķis ir uzlabot iekšējā tirgus darbību.

(7) Pārvaldītiem drošības pakalpojumiem paredzētām Eiropas sertifikācijas shēmām būtu jāveicina minēto pakalpojumu ieviešana un lielāka konkurence starp pārvaldītu drošības pakalpojumu sniedzējiem. Neskarot mērķi nodrošināt, ka šādu pakalpojumu sniedzējiem ir pietiekams un atbilstīgs attiecīgo tehnisko zināšanu līmenis un profesionālā integritāte, sertifikācijas shēmām līdz ar to būtu jāveicina pārvaldītu drošības pakalpojumu ienākšana tirgū un piedāvājums, cik vien iespējams vienkāršojot iespējamo regulatīvo, administratīvo un finansiālo slogu, ar ko pakalpojumu sniedzēji, jo īpaši mikrouzņēmumi vai mazie un vidējie uzņēmumi (MVU), varētu saskarties, piedāvājot pārvaldītus drošības pakalpojumus. Turklāt, lai veicinātu pārvaldītu drošības pakalpojumu ieviešanu un pieprasījumu pēc tiem, šīm shēmām būtu jāsekmē to pieejamība, jo īpaši mazākiem dalībniekiem, piemēram, mikrouzņēmumiem un MVU, kā arī vietējām un reģionālajām pašvaldībām, kam ir ierobežotas spējas un resursi un kas ir neaizsargātākas pret kiberdrošības pārkāpumiem, kuriem ir finansiālas un juridiskas sekas un kuri ietekmē reputāciju un darbību.

(8) Ir svarīgi sniegt atbalstu mikrouzņēmumiem un mazajiem un vidējiem uzņēmumiem (MVU) šīs regulas īstenošanā un tādu darbinieku pieņemšanā darbā, kuriem ir specializētas kiberdrošības prasmes un zināšanas, kas vajadzīgas, lai sniegtu pārvaldītus drošības pakalpojumus atbilstīgi šajā regulā noteiktajām prasībām. Programma "Digitālā Eiropa" un citas attiecīgās Savienības programmas paredz, ka Komisijai būtu jānodrošina finansiāls un tehnisks atbalsts, kas ļautu šiem uzņēmumiem veicināt Eiropas ekonomikas izaugsmi un uzlabot kiberdrošības līmeni ES kopumā, tostarp racionalizējot finansiālo atbalstu no programmas "Digitālā Eiropa" un citām attiecīgām Savienības programmām un atbalstot mikrouzņēmumus un MVU.

(9) Pārvaldītiem drošības pakalpojumiem paredzētai Savienības sertifikācijas shēmai būtu jāveicina tādu drošu un kvalitatīvu pakalpojumu pieejamība, kuri garantē drošu digitālo pārkārtošanos un palīdz sasniegt Digitālās desmitgades politikas programmā noteiktos mērķrādītājus, jo īpaši mērķi panākt, ka 75 % Savienības uzņēmumu sāk izmantot mākoņdatošanu, mākslīgo intelektu vai lielos datus, ka vairāk nekā 90 % mikrouzņēmumu un MVU sasniedz vismaz digitālās intensitātes pamatlīmeni un ka būtiskākie sabiedriskie pakalpojumi tiek piedāvāti tiešsaistē.

(10) Papildus IKT produktu, IKT pakalpojumu vai IKT procesu ieviešanai pārvaldītie drošības pakalpojumi bieži vien nodrošina pakalpojumu papildu elementus, kas balstās uz personāla kompetenci, specializētām zināšanām un pieredzi. Lai nodrošinātu pārvaldīto drošības pakalpojumu īpaši augstu kvalitāti, daļai no drošības mērķiem vajadzētu būt īpaši augstam šo kompetenču, specializēto zināšanu un pieredzes līmenim, kā arī atbilstīgām iekšējām procedūrām. Tādēļ, lai nodrošinātu, ka ***īpašas*** sertifikācijas ***shēmas*** var aptvert visus ***pārvaldītu*** drošības ***pakalpojumu*** aspektus, ir jāgroza Regula (ES) 2019/881. ***Būtu jāņem vērā*** Regulā (ES) 2019/881 ***paredzētās izvērtēšanas un pārskatīšanas rezultāti un tajās sniegtie ieteikumi.***

(11) Lai veicinātu uzticama Savienības tirgus izaugsmi un vienlaikus arī veidotu partnerības ar līdzīgi domājošām trešām valstīm, sertifikācijas process, kas paredzēts saskaņā ar šo regulu izveidotajā satvarā, būtu jāracionalizē ar mērķi atvieglot starptautisku atzīšanu un saskaņošanu ar starptautiskajiem standartiem.

(12) Savienība saskaras ar talantu trūkumu, ko raksturo kvalificētu speciālistu trūkums, un strauji mainīgu apdraudējumu ainu, kā atzīts Komisijas 2023. gada 18. aprīļa paziņojumā par Kiberdrošības prasmju akadēmiju. Izglītības resursi un formālās apmācības veidi atšķiras, un zināšanas var iegūt dažādi — gan formālā veidā, piemēram, augstskolā vai kursos, gan neformālā veidā, piemēram, saņemot apmācību darbavietā vai iegūstot darba pieredzi attiecīgajā jomā. Tāpēc, lai veicinātu kvalitatīvu un nozīmīgu pārvaldītu drošības pakalpojumu rašanos un lai gūtu labāku priekšstatu par Savienības kiberdrošības darbaspēka sastāvu, ir svarīgi stiprināt sadarbību starp dalībvalstīm, Komisiju, ENISA un ieinteresētajām personām, tostarp privāto sektoru un akadēmiskajām aprindām, attīstot publiskā un privātā sektora partnerības, atbalstot pētniecības un inovācijas iniciatīvas un izstrādājot un savstarpēji atzīstot kopīgus standartus un kiberdrošības prasmju sertifikāciju, cita starpā ar Eiropas kiberdrošības prasmju satvara starpniecību. Šāda sadarbība tāpat veicinātu kiberdrošības speciālistu mobilitāti Savienībā, kā arī zināšanu un apmācības kiberdrošības jomā iekļaušanu izglītības programmās, vienlaikus nodrošinot māceklības un stažēšanās iespējas jauniešiem, tostarp personām, kas dzīvo mazāk attīstītos reģionos, piemēram, salās un mazapdzīvotos, lauku un attālos apvidos. Ir svarīgi, lai minēto pasākumu mērķis būtu piesaistīt šajā nozarē vairāk sieviešu un meiteņu un palīdzēt novērst dzimumu nelīdztiesību zinātnes, tehnoloģiju, inženierzinātņu un matemātikas jomā un lai privātā sektora mērķis būtu nodrošināt apmācību darbavietā, pievēršoties vispieprasītākajām prasmēm ar valsts pārvaldes un jaunuzņēmumu, kā arī mikrouzņēmumu un MVU līdzdalību. Ir arī svarīgi, lai šie pakalpojumu sniedzēji un dalībvalstis sadarbotos un sniegtu ieguldījumu datu vākšanā par kiberdrošības darba tirgus situāciju un attīstību.

(13) ENISA ir svarīga loma Eiropas sertifikācijas kandidātshēmu sagatavošanā. Sagatavojot Savienības vispārējā budžeta projektu, Komisijai būtu jāizvērtē ENISA štatu sarakstam nepieciešamie budžeta resursi saskaņā ar Regulas (ES) 2019/881 29. pantā noteikto procedūru.

(14) Šī regula paredz mērķtiecīgus grozījumus Regulā (ES) 2019/881 nolūkā pievienot iespēju izveidot pārvaldītu drošības pakalpojumu sniedzējiem paredzētas kiberdrošības sertifikācijas shēmas. Šajā sakarā tajā arī ir paredzēti un precizēti konkrēti noteikumi par visu Eiropas kiberdrošības sertifikācijas shēmu sagatavošanu un darbību ar mērķi nodrošināt to pārredzamību un atvērtību. Pēdējiem minētajiem grozījumiem, kas attiecas vienīgi uz noteikumu paredzēšanu vai precizēšanu Regulā (ES) 2019/881, jo īpaši grozījumiem 49. un 49.a pantā, nekādā veidā nebūtu jāskar minētās regulas plašāka novērtēšana un pārskatīšana, kas prasīta tās 67. pantā, tostarp konkrēti minētās regulas sadaļas par kiberdrošības sertifikācijas shēmām ietekmes, efektivitātes un lietderības novērtēšana. Minētās sadaļas par kiberdrošības sertifikācijas shēmām novērtēšana un pārskatīšana būtu jābalsta uz plašu apspriešanos ar ieinteresētajām personām un iesaistīto procedūru pilnīgu un rūpīgu analīzi.

(15) Tā kā šīs regulas mērķi, proti, dot iespēju pieņemt pārvaldītiem drošības pakalpojumiem paredzētas Eiropas kiberdrošības sertifikācijas shēmas, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet mēroga un ietekmes dēļ to var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tādus pasākumus, kas ir vajadzīgi šā mērķa sasniegšanai.

(16) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 2018/1725*[6] *42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2024. gada 10. janvārī sniedza atzinumu*[7].**

IR PIEŅĒMUSI ŠO REGULU.

---

6 ***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.).***

7 ***OV C.../....***

1. pants

Grozījumi Regulā (ES) 2019/881

Regulu (ES) 2019/881 groza šādi:

(1) regulas 1. panta 1. punkta pirmās daļas b) apakšpunktu aizstāj ar šādu:

“b) satvars, kurā jāizveido Eiropas kiberdrošības sertifikācijas shēmas, lai Savienībā IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem nodrošinātu pietiekamu kiberdrošības līmeni, kā arī lai nepieļautu iekšējā tirgus sadrumstalotību attiecībā uz kiberdrošības sertifikācijas shēmām Savienībā.”;

(2) regulas 2. pantu groza šādi:

(a) panta 9., 10. un 11. punktu aizstāj ar šādiem:

“9) “Eiropas kiberdrošības sertifikācijas shēma” ir visaptverošs noteikumu, tehnisko prasību, standartu un procedūru kopums, kas noteikts Savienības līmenī un kas attiecas uz konkrētu IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu sertifikāciju vai atbilstības novērtēšanu;

10) “valsts kiberdrošības sertifikācijas shēma” ir visaptverošs noteikumu, tehnisko prasību, standartu un procedūru kopums, ko izstrādājusi un pieņēmusi valsts publiskā iestāde un kas attiecas uz to IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu sertifikāciju vai atbilstības novērtēšanu, kuri ietilpst konkrētās shēmas tvērumā;

11) “Eiropas kiberdrošības sertifikāts” ir dokuments, ko izdevusi atbilstīga struktūra un kas apliecina, ka ir izvērtēta attiecīgā IKT produkta, IKT pakalpojuma, IKT procesa vai pārvaldīta drošības pakalpojuma atbilstība konkrētajām Eiropas kiberdrošības sertifikācijas shēmā noteiktajām drošības prasībām;”;

(b) iekļauj šādu punktu:

“14a) “pārvaldīts drošības pakalpojums” ir pakalpojums, ***kas sniegts trešai pusei un*** kas ietver ar kiberdrošības riska pārvaldību saistītu darbību veikšanu vai atbalstīšanu, piemēram, incidentu ***novēršanu***, ielaušanās testēšanu, drošības revīzijas un ***konsultācijas, tostarp ekspertu sniegtas konsultācijas, kas saistītas ar tehnisko atbalstu;***”;

(c) panta 20., 21. un 22. punktu aizstāj ar šādiem:

"20) "tehniskās specifikācijas" ir dokuments, kurā noteiktas tehniskās prasības, kam IKT produktam, IKT pakalpojumam, IKT procesam vai pārvaldītam drošības pakalpojumam ir jāatbilst, vai atbilstības novērtēšanas procedūras, kas uz tiem attiecas;

21) "apliecinājuma līmenis" ir pamats paļauties, ka IKT produkts, IKT pakalpojums, IKT process vai pārvaldīts drošības pakalpojums atbilst konkrētas Eiropas kiberdrošības sertifikācijas shēmas prasībām; "apliecinājuma līmenis" norāda to, kādā līmenī IKT produkts, IKT pakalpojums, IKT process vai pārvaldīts drošības pakalpojums ir izvērtēts, bet pats par sevi nemēra attiecīgā IKT produkta, IKT pakalpojuma, IKT procesa vai pārvaldīta drošības pakalpojuma drošību;

22) “atbilstības pašnovērtējums” ir darbība, ko veic IKT produktu, IKT pakalpojumu vai IKT procesu, vai pārvaldītu drošības pakalpojumu ražotājs vai sniedzējs, kurš izvērtē, vai minētie IKT produkti, IKT pakalpojumi, IKT procesi vai pārvaldītie drošības pakalpojumi atbilst konkrētas Eiropas kiberdrošības sertifikācijas shēmas prasībām.”;

(3) regulas 4. panta 6. punktu aizstāj ar šādu:

“6. *ENISA* veicina Eiropas kiberdrošības sertifikācijas izmantošanu nolūkā nepieļaut iekšējā tirgus sadrumstalotību. *ENISA* palīdz izveidot un uzturēt Eiropas kiberdrošības sertifikācijas satvaru saskaņā ar šīs regulas III sadaļu, lai uzlabotu IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu kiberdrošības pārredzamību, tādējādi stiprinot uzticēšanos digitālajam iekšējam tirgum un tā konkurētspēju.”;

(4) regulas 8. pantu groza šādi:

(a) panta 1. punktu aizstāj ar šādu:

"1. *ENISA* atbalsta un veicina Savienības politikas IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu kiberdrošības sertifikācijas jomā izstrādi un īstenošanu, kā noteikts šīs regulas III sadaļā, proti:

a) pastāvīgi pārrauga norises saistītajās standartizācijas jomās un iesaka atbilstīgas tehniskās specifikācijas, kas būtu izmantojamas Eiropas kiberdrošības sertifikācijas shēmu izstrādē saskaņā ar 54. panta 1. punkta c) apakšpunktu gadījumos, kad standarti nav pieejami;

b) sagatavo IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem paredzētas Eiropas kiberdrošības sertifikācijas kandidātshēmas (“kandidātshēmas”) saskaņā ar 49. pantu;

c) izvērtē pieņemtās Eiropas kiberdrošības sertifikācijas shēmas saskaņā ar 49. panta 8. punktu;

d) piedalās salīdzinošā izvērtēšanā, ievērojot 59. panta 4. punktu;

e) palīdz Komisijai nodrošināt *ECCG* sekretariāta darbību saskaņā ar 62. panta 5. punktu.”;

(b) panta 3. punktu aizstāj ar šādu:

“3. *ENISA* sadarbībā ar valstu kiberdrošības sertifikācijas iestādēm un nozares pārstāvjiem oficiālā, strukturētā un pārredzamā veidā apkopo un publicē pamatnostādnes un izstrādā labu praksi attiecībā uz IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu kiberdrošības prasībām.”;

(c) panta 5. punktu aizstāj ar šādu:

"5. *ENISA* palīdz izstrādāt un ieviest Eiropas un starptautiskos riska pārvaldības un IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu drošības standartus.";

(5) regulas 46. panta 1. un 2. punktu aizstāj ar šādiem:

"1. Eiropas kiberdrošības sertifikācijas satvaru izveido, lai uzlabotu iekšējā tirgus darbības nosacījumus, palielinot kiberdrošības līmeni Savienībā un dodot iespēju Savienības līmenī izmantot saskaņotu pieeju attiecībā uz Eiropas kiberdrošības sertifikācijas shēmām nolūkā izveidot IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu digitālu vienoto tirgu.

2. Eiropas kiberdrošības sertifikācijas satvars paredz mehānismu Eiropas kiberdrošības sertifikācijas shēmu izveidei. Tas apliecina, ka IKT produkti, IKT pakalpojumi un IKT procesi, kas ir izvērtēti saskaņā ar šādām shēmām, atbilst noteiktajām drošības prasībām nolūkā visā to dzīves ciklā aizsargāt tādu glabāto, pārsūtīto vai apstrādāto datu vai funkciju, vai pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā vai kuriem piekļūst, izmantojot minētos produktus, pakalpojumus un procesus. Turklāt tas apliecina, ka pārvaldītie drošības pakalpojumi, kas ir izvērtēti saskaņā ar šādām shēmām, atbilst noteiktajām drošības prasībām nolūkā aizsargāt tādu datu pieejamību, autentiskumu, integritāti un konfidencialitāti, kuriem piekļūst un kurus apstrādā, glabā vai pārsūta saistībā ar minēto pakalpojumu sniegšanu, un ka minētos pakalpojumus nepārtraukti sniedz darbinieki, kuriem ir vajadzīgā kompetence, kvalifikācija un pieredze un ***pietiekams un pienācīgs*** attiecīgo tehnisko zināšanu un profesionālās integritātes līmenis.***”***;

(6) regulas 47. panta 2. un 3. punktu aizstāj ar šādiem:

“2. Savienības mainīgajā darba programmā jo īpaši iekļauj tādu IKT produktu, IKT pakalpojumu, IKT procesu vai to kategoriju un pārvaldītu drošības pakalpojumu sarakstu, kuri varētu gūt labumu no iekļaušanas Eiropas kiberdrošības sertifikācijas shēmas darbības jomā.

3. Konkrētu IKT produktu, IKT pakalpojumu un IKT procesu vai to kategoriju vai pārvaldītu drošības pakalpojumu iekļaušanu Savienības mainīgajā darba programmā pamato ar vienu vai vairākiem šādiem iemesliem:

a) tādu valsts kiberdrošības sertifikācijas shēmu pieejamību un izstrādi, kuras aptver konkrētu IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu kategoriju, jo īpaši attiecībā uz sadrumstalotības risku;

b) attiecīgu Savienības vai dalībvalsts tiesību aktu vai rīcībpolitiku;

c) pieprasījumu tirgū;

ca) tehnoloģiju attīstību un starptautisko kiberdrošības sertifikācijas shēmu un starptautisko un rūpniecības standartu pieejamību un izstrādi;

d) tendencēm kiberdraudu vidē;

e) *ECCG* pieprasījumu sagatavot konkrētu kandidātshēmu.”;

(7) ▌regulas 49. pantu ***groza šādi***:

(a) panta 1., 2., 3. un 4. punktu aizstāj ar šādiem:

"*1. Pēc Komisijas pieprasījuma saskaņā ar 48. pantu ENISA sagatavo kandidātshēmu, kas atbilst 51., 51.a, 52. un 54. pantā noteiktajām piemērojamajām prasībām.*

2. Pēc ECCG pieprasījuma saskaņā ar 48. panta 2. punktu ENISA var sagatavot kandidātshēmu, kas atbilst 51., 51.a, 52. un 54. pantā noteiktajām piemērojamajām prasībām. Ja ENISA šādu pieprasījumu noraida, tā norāda noraidīšanas iemeslus. Jebkuru lēmumu noraidīt šādu pieprasījumu pieņem Valde.'';

3. Sagatavojot kandidātshēmu, ENISA oficiālā, atklātā, pārredzamā un iekļaujošā apspriešanās procesā savlaicīgi apspriežas ar visām attiecīgajām ieinteresētajām personām. Nosūtot kandidātshēmu Komisijai saskaņā ar 49. panta 6. punktu, ENISA sniedz informāciju par to, kā tā ir izpildījusi šo pienākumu.

4. Attiecībā uz katru kandidātshēmu ENISA saskaņā ar 20. panta 4. punktu izveido ad hoc darba grupu, lai nodrošinātu ENISA specializētas konsultācijas un zināšanas. Šim nolūkam izveidotajās ad hoc darba grupās, ja nepieciešams un neskarot 20. panta 4. punktā noteiktās procedūras un rīcības brīvību, iekļauj ekspertus no dalībvalstu publiskās pārvaldes iestādēm, Savienības iestādēm, struktūrām, birojiem un aģentūrām un privātā sektora.";

(b) panta 7. punktu aizstāj ar šādu:

"7. Pamatojoties uz *ENISA* sagatavoto kandidātshēmu, Komisija var pieņemt īstenošanas aktus, kuros paredzēta Eiropas kiberdrošības sertifikācijas shēma IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem, kas atbilst 51., ***51.a,*** 52. un 54. pantā izklāstītajām prasībām. Minētos īstenošanas aktus pieņem saskaņā ar 66. panta 2. punktā minēto pārbaudes procedūru.'';

(8) iekļauj šādu pantu:

“49.a pants

Informēšana un apspriešanās par Eiropas kiberdrošības sertifikācijas shēmām

1. Komisija informāciju par savu pieprasījumu ENISA sagatavot kandidātshēmu vai pārskatīt esošu Eiropas kiberdrošības sertifikācijas shēmu, kas minēta 48. pantā, dara publiski pieejamu.

2. Kad ENISA sagatavo kandidātshēmu saskaņā ar 49. pantu, Eiropas Parlaments, kā arī Padome var pieprasīt Komisijai kā Eiropas Kiberdrošības sertifikācijas grupas (ECCG) priekšsēdētājai un ENISA reizi ceturksnī iesniegt attiecīgu informāciju par kandidātshēmas projektu. Pēc Eiropas Parlamenta vai Padomes pieprasījuma ENISA, vienojoties ar Komisiju un neskarot 27. pantu, var darīt pieejamas Eiropas Parlamentam un Padomei kandidātshēmas projekta attiecīgās daļas prasītajam konfidencialitātes līmenim atbilstošā veidā un attiecīgā gadījumā ierobežotā veidā.

3. Lai uzlabotu dialogu starp Savienības iestādēm un veicinātu oficiālu, atklātu, pārredzamu un iekļaujošu apspriešanās procesu, Eiropas Parlaments, kā arī Padome var aicināt Komisiju un ENISA apspriest jautājumus, kas skar IKT produktiem, IKT pakalpojumiem, IKT procesiem vai pārvaldītiem drošības pakalpojumiem paredzētu Eiropas kiberdrošības sertifikācijas shēmu darbību.

4. Komisija, izvērtējot šo regulu saskaņā ar 67. pantu, attiecīgā gadījumā ņem vērā elementus, kas izriet no Eiropas Parlamenta un Padomes paustajiem viedokļiem par šā panta 3. punktā minētajiem jautājumiem.";

(9) regulas 51. pantu groza šādi:

(a) virsrakstu aizstāj ar šādu:

"Drošības mērķi: Eiropas kiberdrošības sertifikācijas shēmas IKT produktiem, IKT pakalpojumiem un IKT procesiem"

(b) ievadteikumu aizstāj ar šādu:

"Eiropas kiberdrošības sertifikācijas shēmu IKT produktiem, IKT pakalpojumiem vai IKT procesiem izstrādā tā, lai attiecīgā gadījumā sasniegtu vismaz šādus drošības mērķus:";

(10) iekļauj šādu pantu:

"51.a pants

Drošības mērķi: Eiropas kiberdrošības sertifikācijas shēmas pārvaldītiem drošības pakalpojumiem

Eiropas kiberdrošības sertifikācijas shēmu pārvaldītiem drošības pakalpojumiem izstrādā tā, lai attiecīgā gadījumā sasniegtu vismaz šādus drošības mērķus:

a) ▌ pārvaldītu drošības pakalpojumu sniegšanā tiek nodrošināta vajadzīgā kompetence, zināšanas un pieredze, tostarp par šo pakalpojumu sniegšanu atbildīgajam personālam ir ***pietiekama un pienācīga*** līmeņa tehniskās zināšanas un kompetence konkrētajā jomā, pietiekama un atbilstīga pieredze un augstākais profesionālās integritātes līmenis;

b) ▌ pakalpojumu sniedzējs ir ieviesis pienācīgas iekšējās procedūras, kas nodrošina, ka pārvaldītie drošības pakalpojumi vienmēr tiek sniegti ***pietiekamā un pienācīgā*** kvalitātes līmenī;

c) dati, kuriem piekļūst un kurus glabā, pārsūta vai citādi apstrādā saistībā ar pārvaldītu drošības pakalpojumu sniegšanu, tiek aizsargāti pret nejaušu vai neatļautu piekļuvi, glabāšanu, atklāšanu, iznīcināšanu, citu apstrādi, pazaudēšanu, pārveidošanu vai nepieejamību;

d) ▌ fiziska vai tehniska incidenta gadījumos laikus tiek atjaunota datu, pakalpojumu un funkciju pieejamība un piekļūstamība;

e) ▌ pilnvarotas personas, programmas vai iekārtas var piekļūt vienīgi tādiem datiem, pakalpojumiem vai funkcijām, attiecībā uz ko tām ir piekļuves tiesības;

f) tiek reģistrēts un ir iespējams novērtēt, kuriem datiem, pakalpojumiem vai funkcijām ir piekļūts, kuru datu, pakalpojumu un funkciju izmantošana ir notikusi vai kuri dati ir citādi apstrādāti, kad tas ir noticis un kas to ir darījis;

g) ▌ pārvaldīto drošības pakalpojumu sniegšanā izmantotie IKT produkti, IKT pakalpojumi un IKT procesi ir droši pēc noklusējuma un konstruēti tā, lai būtu droši, ***un attiecīgā gadījumā*** ietver jaunākos drošības atjauninājumus***, taču neietver publiski zināmas ievainojamības***;";

(11) regulas 52. pantu groza šādi:

(a) panta 1. punktu aizstāj ar šādu:

"1. Eiropas kiberdrošības sertifikācijas shēmā var norādīt vienu vai vairākus šādus IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu apliecinājuma līmeņus: "pamata", "būtisks" vai "augsts". Apliecinājuma līmenis incidenta varbūtības un ietekmes ziņā atbilst riska līmenim, kas saistīts ar IKT produkta, IKT pakalpojuma, IKT procesa vai pārvaldīta drošības pakalpojuma paredzamo lietojumu.";

(b) panta 3. punktu aizstāj ar šādu:

"3. Attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā jānorāda katram apliecinājuma līmenim atbilstošās drošības prasības, tostarp atbilstošās drošības funkcijas un IKT produktam, IKT pakalpojumam, IKT procesam vai pārvaldītam drošības pakalpojumam veicamā izvērtējuma atbilstošā stingrības un detalizācijas pakāpe.";

(c) panta 5., 6. un 7. punktu aizstāj ar šādiem:

"5. Ar Eiropas kiberdrošības sertifikātu vai ES atbilstības apliecinājumu, kam ir norāde uz apliecinājuma līmeni "pamata", sniedz apliecinājumu, ka IKT produkti, IKT pakalpojumi, IKT procesi un pārvaldīti drošības pakalpojumi, par kuriem izdots minētais sertifikāts vai minētais ES atbilstības apliecinājums, atbilst attiecīgajām drošības prasībām, tostarp drošības funkciju ziņā, un ka tie ir izvērtēti tādā līmenī, lai līdz minimumam ierobežotu zināmos incidentu un kiberuzbrukumu pamata riskus. Veicamās izvērtēšanas darbības ietver vismaz tehniskās dokumentācijas pārskatīšanu. Ja šāda pārskatīšana nav pienācīga, ir jāveic alternatīvas izvērtēšanas darbības ar līdzvērtīgu ietekmi.

6. Ar Eiropas kiberdrošības sertifikātu, kam ir norāde uz apliecinājuma līmeni “būtisks”, sniedz apliecinājumu, ka IKT produkti, IKT pakalpojumi, IKT procesi un pārvaldīti drošības pakalpojumi, par kuriem izdots minētais sertifikāts, atbilst attiecīgajām drošības prasībām, tostarp drošības funkciju ziņā, un ka tie ir izvērtēti tādā līmenī, lai līdz minimumam ierobežotu zināmos kiberdrošības riskus un tādu incidentu un kiberuzbrukumu risku, ko rada aktori ar ierobežotām prasmēm un resursiem. Veicamās izvērtēšanas darbības ietver vismaz: pārskatīšanu nolūkā apliecināt publiski zināmu ievainojamību neesamību un testēšanu nolūkā apliecināt to, ka ar IKT produktiem, IKT pakalpojumiem, IKT procesiem vai pārvaldītiem drošības pakalpojumiem ir pareizi īstenotas vajadzīgās drošības funkcijas. Ja neviena šāda izvērtēšanas darbība nav pienācīga, veic alternatīvas izvērtēšanas darbības ar līdzvērtīgu ietekmi.

7. Ar Eiropas kiberdrošības sertifikātu, kam ir norāde uz apliecinājuma līmeni “augsts”, sniedz apliecinājumu, ka IKT produkti, IKT pakalpojumi, IKT procesi un pārvadīti drošības pakalpojumi, par kuriem izdots minētais sertifikāts, atbilst attiecīgajām drošības prasībām, tostarp drošības funkciju ziņā, un ka tie ir izvērtēti tādā līmenī, lai līdz minimumam ierobežotu sarežģītu kiberuzbrukumu risku, ko rada aktori ar attīstītām prasmēm un nozīmīgiem resursiem. Veicamās izvērtēšanas darbības ietver vismaz: pārskatīšanu nolūkā apliecināt publiski zināmu ievainojamību neesamību; testēšanu nolūkā apliecināt to, ka ar IKT produktiem, IKT pakalpojumiem, IKT procesiem vai pārvaldītiem drošības pakalpojumiem ir augstākajā līmenī pareizi īstenotas vajadzīgās drošības funkcijas; un ar ielaušanās testēšanu veiktu izvērtējumu par to, ka tie ir noturīgi prasmīgi veiktu uzbrukumu gadījumā. Ja neviena šāda izvērtēšanas darbība nav pienācīga, veic alternatīvas izvērtēšanas darbības ar līdzvērtīgu ietekmi.”;

(12) regulas 53. panta 1., 2. un 3. punktu aizstāj ar šādiem:

"1. Eiropas kiberdrošības sertifikācijas shēmā var atļaut veikt atbilstības pašnovērtējumu, par ko atbildīgs ir tikai pats IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājs vai sniedzējs. Šādu atbilstības pašnovērtējumu atļauj veikt tikai attiecībā uz IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem ar zemu risku, kas atbilst apliecinājuma līmenim "pamata".

2. IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājs vai sniedzējs var izdot ES atbilstības apliecinājumu, kurā ir norādīts, ka atbilstība shēmā izklāstītajām prasībām ir pierādīta. Izdodot šādu apliecinājumu, IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājs vai sniedzējs uzņemas atbildību par IKT produkta, IKT pakalpojuma, IKT procesa vai pārvaldīta drošības pakalpojuma atbilstību minētajā shēmā izklāstītajām prasībām.

3. IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājs vai sniedzējs attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā paredzētajā laikposmā 58. pantā minētajai valsts kiberdrošības sertifikācijas iestādei dara pieejamu ES atbilstības apliecinājumu, tehnisko dokumentāciju un visu pārējo būtisko informāciju, kas saistīta ar IKT produktu, IKT pakalpojumu vai pārvaldītu drošības pakalpojumu atbilstību shēmai. ES atbilstības apliecinājuma kopiju iesniedz valsts kiberdrošības sertifikācijas iestādei un *ENISA*.";

(13) regulas 54. panta 1. punktu groza šādi:

(a) punkta a) apakšpunktu aizstāj ar šādu:

"a) sertifikācijas shēmas priekšmets un tvērums, tostarp shēmas aptverto IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu veidi vai kategorijas;";

(aa) punkta g) apakšpunktu aizstāj ar šādu:

"g) izmantojamie konkrētie izvērtēšanas kritēriji un metodes, tostarp izvērtēšanas veidi, ar ko pierāda, ka 51. un 51.a pantā minētie piemērojamie drošības mērķi ir sasniegti;

(b) punkta j) apakšpunktu aizstāj ar šādu:

"j) noteikumi, kas vajadzīgi, lai pārraudzītu, vai IKT produkti, IKT pakalpojumi, IKT procesi un pārvaldīti drošības pakalpojumi atbilst Eiropas kiberdrošības sertifikātu vai ES atbilstības apliecinājumu prasībām, tostarp mehānismi, kas izmantojami, lai pierādītu noteikto kiberdrošības prasību pastāvīgu ievērošanu;";

(c) punkta l) apakšpunktu aizstāj ar šādu:

"l) noteikumi par sekām attiecībā uz tādiem IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem, kuri ir sertificēti vai par kuriem ir izdots ES atbilstības apliecinājums, bet kuri neatbilst shēmas prasībām;";

(d) punkta o) apakšpunktu aizstāj ar šādu:

“o) to valsts vai starptautisko kiberdrošības sertifikācijas shēmu identifikācija, kuras attiecas uz viena un tā paša veida vai kategorijas IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem, drošības prasībām, izvērtēšanas kritērijiem un metodēm un apliecinājuma līmeņiem;”;

(e) punkta q) apakšpunktu aizstāj ar šādu:

“q) pieejamības laikposms, kurā IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājam vai sniedzējam jādara pieejams ES atbilstības apliecinājums, tehniskā dokumentācija un visa pārējā attiecīgā informācija;”;

(14) regulas 56. pantu groza šādi:

(a) panta 1. punktu aizstāj ar šādu:

“1. IKT produktus, IKT pakalpojumus, IKT procesus un pārvaldītus drošības pakalpojumus, kuri ir sertificēti atbilstīgi Eiropas kiberdrošības sertifikācijas shēmai, kas pieņemta saskaņā ar 49. pantu, uzskata par atbilstīgiem minētās shēmas prasībām.”;

(b) panta 3. punktu groza šādi:

i) pirmo daļu aizstāj ar šādu:

“Komisija regulāri novērtē pieņemto Eiropas kiberdrošības sertifikācijas shēmu efektivitāti un izmantojumu un to, vai konkrēta Eiropas kiberdrošības sertifikācijas shēma ir jānosaka par obligātu ar attiecīgu Savienības tiesību aktu, lai nodrošinātu IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu pienācīgi augstu kiberdrošības līmeni Savienībā un uzlabotu iekšējā tirgus darbību. Pirmais šāds novērtējums jāveic līdz 2023. gada 31. decembrim, un pēc tam turpmākie novērtējumi jāveic vismaz reizi divos gados. Komisija, balstoties uz minēto novērtējumu iznākumu, nosaka tos kādas esošas sertifikācijas shēmas aptvertus IKT produktus, IKT pakalpojumus, IKT procesus un pārvaldītus drošības pakalpojumus, uz kuriem jāattiecina obligāta sertificēšanas shēma.”;

ii) trešo daļu groza šādi:

aa) daļas a) apakšpunktu aizstāj ar šādu:

"a) ņem vērā minēto pasākumu ietekmi izmaksu ziņā uz šādu IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājiem vai sniedzējiem un lietotājiem un to, kādi sociāli vai ekonomiski ieguvumi izriet no paredzētās drošības līmeņa paaugstināšanas konkrētajiem IKT produktiem, IKT pakalpojumiem, IKT procesiem vai pārvaldītiem drošības pakalpojumiem;";

bb) daļas d) apakšpunktu aizstāj ar šādu:

"d) ņem vērā jebkurus īstenošanas termiņus, pārejas pasākumus un laikposmus, jo īpaši attiecībā uz pasākuma iespējamo ietekmi uz IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājiem vai sniedzējiem, tostarp ***mikrouzņēmumu un*** MVU ***specifiskās intereses un vajadzības;***'';

(c) panta 7. un 8. punktu aizstāj ar šādiem:

"7. Fiziska vai juridiska persona, kas iesniedz pieteikumu IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu sertifikācijai, dara pieejamu visu sertifikācijas veikšanai nepieciešamo informāciju 58. pantā minētajai valsts kiberdrošības sertifikācijas iestādei, ja tā ir Eiropas kiberdrošības sertifikāta izdevēja struktūra, vai 60. pantā minētajai atbilstības novērtēšanas struktūrai.

8. Eiropas kiberdrošības sertifikāta turētājs 7. punktā minēto iestādi vai struktūru informē par jebkādām vēlāk atklātām IKT produkta, IKT pakalpojuma, IKT procesa vai pārvaldīta drošības pakalpojuma ievainojamībām vai neatbilstībām, kuras varētu ietekmēt tā atbilstību ar sertifikāciju saistītajām prasībām. Minētā iestāde vai struktūra saņemto informāciju bez liekas kavēšanās pārsūta attiecīgajai valsts kiberdrošības sertifikācijas iestādei.";

(15) regulas 57. panta 1. un 2. punktu aizstāj ar šādiem:

“1. Neskarot šā panta 3. punktu, valsts kiberdrošības sertifikācijas shēmas un saistītās procedūras, kas paredzētas IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem, uz kuriem attiecas Eiropas kiberdrošības sertifikācijas shēma, zaudē spēku no datuma, kas noteikts saskaņā ar 49. panta 7. punktu pieņemtajā īstenošanas aktā. Valsts kiberdrošības sertifikācijas shēmas un saistītās procedūras, kas paredzētas IKT produktiem, IKT pakalpojumiem, IKT procesiem un pārvaldītiem drošības pakalpojumiem, uz kuriem neattiecas Eiropas kiberdrošības sertifikācijas shēma, paliek spēkā arī turpmāk.

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

(16) regulas 58. pantu groza šādi:

(a) panta 7. punktu groza šādi:

i) punkta a) un b) apakšpunktu aizstāj ar šādiem:

“a) sadarbībā ar citām attiecīgām tirgus uzraudzības iestādēm uzrauga noteikumus, kas, ievērojot 54. panta 1. punkta j) apakšpunktu, ietverti Eiropas kiberdrošības sertifikācijas shēmās nolūkā pārraudzīt IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu atbilstību to attiecīgajās teritorijās izdoto Eiropas kiberdrošības sertifikātu prasībām, un nodrošina minēto noteikumu izpildi;

b) pārrauga atbilstību tiem pienākumiem un panāk to pienākumu izpildi, kas piemērojami IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotājiem vai sniedzējiem, kuri ir iedibināti to attiecīgajās teritorijās un kuri veic atbilstības pašnovērtēšanu, un jo īpaši pārrauga šādu ražotāju vai sniedzēju atbilstību tiem pienākumiem un panāk to pienākumu izpildi, kas izklāstīti 53. panta 2. un 3. punktā un attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā;”;

ii) punkta h) apakšpunktu aizstāj ar šādu:

“h) sadarbojas ar citām valsts kiberdrošības sertifikācijas iestādēm vai citām publiskām iestādēm, piemēram, kopīgojot informāciju par IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu iespējamu neatbilstību šīs regulas vai konkrētu Eiropas kiberdrošības sertifikācijas shēmu prasībām; un;’’;

(b) panta 9. punktu aizstāj ar šādu:

“9. Valsts kiberdrošības sertifikācijas iestādes sadarbojas savā starpā un ar Komisiju, jo īpaši apmainoties ar informāciju, pieredzi un labu praksi attiecībā uz kiberdrošības sertifikācijas un tehniskiem jautājumiem, kas skar IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu kiberdrošību.”;

(17) regulas 59. panta 3. punkta b) un c) apakšpunktu aizstāj ar šādiem:

"b) uzraudzības un noteikumu izpildes panākšanas procedūras, ar ko paredz pārraudzīt IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu atbilstību Eiropas kiberdrošības sertifikātiem, ievērojot 58. panta 7. punkta a) apakšpunktu;

c) procedūras, kas paredzētas IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu ražotāju vai sniedzēju pienākumu pārraudzībai un izpildes panākšanai, ievērojot 58. panta 7. punkta b) apakšpunktu;";

(18) regulas 67. panta 2. un 3. punktu aizstāj ar šādiem:

2. Novērtējumā izvērtē arī šīs regulas III sadaļas noteikumu***, tostarp procedūru, kuru rezultātā tiek pieņemtas kiberdrošības sertifikācijas shēmas un to pierādījumu bāzes,*** ietekmi, rezultativitāti un efektivitāti attiecībā uz mērķiem nodrošināt IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu pienācīgu kiberdrošības līmeni Savienībā un uzlabot iekšējā tirgus darbību.

3. Novērtējumā izvērtē, vai ir nepieciešamas kiberdrošības pamatprasības attiecībā uz piekļuvi iekšējam tirgum, lai novērstu kiberdrošības pamatprasībām neatbilstošu IKT produktu, IKT pakalpojumu, IKT procesu un pārvaldītu drošības pakalpojumu ienākšanu Savienības tirgū."

(19) Pielikumu aizstāj ar šīs regulas pielikuma tekstu.

2. pants

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

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

... [vieta], ... [datums]

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

PIELIKUMS

PRASĪBAS, KAS JĀIEVĒRO ATBILSTĪBAS NOVĒRTĒŠANAS STRUKTŪRĀM

Atbilstības novērtēšanas struktūras, kuras vēlas tikt akreditētas, ievēro šādas prasības:

1. *Atbilstības novērtēšanas struktūra ir izveidota saskaņā ar valsts tiesību aktiem un tai ir juridiskas personas statuss.*

2. *Atbilstības novērtēšanas struktūra ir trešās puses struktūra, kas ir neatkarīga no organizācijas vai IKT produktiem, IKT pakalpojumiem, IKT procesiem vai pārvaldītiem drošības pakalpojumiem, ko tā novērtē.*

3. *Struktūra, kas pieder uzņēmumu apvienībai vai profesionālajai federācijai, kura pārstāv uzņēmumus, kas iesaistīti novērtējamo IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu izstrādē, ražošanā, nodrošināšanā, montāžā, lietošanā vai apkalpošanā, var tikt uzskatīta par atbilstības novērtēšanas struktūru, ja ir pierādīta tās neatkarība un interešu konfliktu neesamība.*

4. *Atbilstības novērtēšanas struktūras, to augstākā vadība un personas, kas atbild par atbilstības novērtēšanas uzdevumu veikšanu, nav ne vērtētā IKT produkta, IKT pakalpojuma, IKT procesa vai pārvaldīta drošības pakalpojuma izstrādātāji, ražotāji, piegādātāji, uzstādītāji, pircēji, īpašnieki, lietotāji vai apkalpotāji, ne kādas minētās puses pilnvarotie pārstāvji. Minētais aizliegums neliedz izmantot vērtētos IKT produktus, ja tie ir nepieciešami atbilstības novērtēšanas struktūras darbību veikšanai, vai izmantot šādus IKT produktus personiskām vajadzībām.*

5. *Atbilstības novērtēšanas struktūras, to augstākā vadība un personas, kas atbild par atbilstības novērtēšanas uzdevumiem, nav tieši saistītas ar vērtēto IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu izstrādi, ražošanu vai konstruēšanu, nodrošināšanu, tirdzniecību, uzstādīšanu, lietošanu vai apkalpošanu, kā arī nepārstāv minētajās darbībās iesaistītās puses. Atbilstības novērtēšanas struktūras, to augstākā vadība un personas, kas atbild par atbilstības novērtēšanas uzdevumu veikšanu, neiesaistās darbībās, kas var apdraudēt lēmumu pieņemšanas neatkarību vai godprātību, tām veicot atbilstības novērtēšanas darbības. Minētais aizliegums jo īpaši attiecas uz konsultāciju pakalpojumiem.*

6. Ja atbilstības novērtēšanas struktūra pieder publiskai struktūrai vai iestādei vai to pārvalda publiska struktūra vai iestāde, tiek nodrošināta un dokumentēta neatkarība un interešu konfliktu neesamība starp valsts kiberdrošības sertifikācijas iestādi un atbilstības novērtēšanas struktūru.

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

8. Atbilstības novērtēšanas iestādes un to darbinieki veic atbilstības novērtēšanas darbības ar visaugstāko profesionālo integritāti un vajadzīgo tehnisko kompetenci konkrētajā jomā bez spiediena un pamudinājumiem, kas varētu ietekmēt to pieņemto lēmumu vai atbilstības novērtēšanas darbību rezultātus, tostarp bez finansiāla spiediena un pamudinājumiem, jo īpaši no tādu personu vai personu grupu puses, kuras ir ieinteresētas minēto darbību rezultātos.

9. Atbilstības novērtēšanas iestāde spēj veikt visus tai saskaņā ar šo regulu uzticētos atbilstības novērtēšanas uzdevumus neatkarīgi no tā, vai tā minētos uzdevumus veic pati vai tie tiek veikti šīs iestādes vārdā un atbildībā. Jebkuru apakšlīgumu slēgšanu vai konsultācijas ar ārējiem darbiniekiem pienācīgi dokumentē, tajās neiesaista starpniekus un par tām rakstiski vienojas, cita starpā attiecībā uz konfidencialitāti un interešu konfliktiem. Attiecīgā atbilstības novērtēšanas struktūra uzņemas pilnu atbildību par veiktajiem uzdevumiem.

10. Atbilstības novērtēšanas struktūras rīcībā katrai atbilstības novērtēšanas procedūrai un katram IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu veidam, kategorijai un apakškategorijai vienmēr ir vajadzīgie:

(a) darbinieki, kuriem ir tehniskās zināšanas un atbilstības novērtēšanas uzdevumu veikšanai pietiekama un pienācīga pieredze;

(b) to procedūru apraksti, saskaņā ar kurām veicama atbilstības novērtēšana, lai nodrošinātu minēto procedūru pārredzamību un iespēju tās atkārtot. Tā ir ieviesusi atbilstīgu politiku un procedūras, lai nošķirtu uzdevumus, kurus tā veic saskaņā ar 61. pantu paziņotās struktūras statusā, no citām tās darbībām;

(c) darbību veikšanas procedūras, kurās pienācīgi ņem vērā uzņēmuma lielumu, nozari, kurā tas darbojas, tā struktūru, attiecīgā IKT produkta, IKT pakalpojuma, IKT procesa vai pārvaldīta drošības pakalpojuma tehnoloģisko sarežģītību un to, vai ražošana notiek masveidā vai sērijveidā.

11. Atbilstības novērtēšanas struktūras rīcībā ir nepieciešamie līdzekļi, lai tā varētu pienācīgi veikt tehniskos un administratīvos uzdevumus, kas saistīti ar atbilstības novērtēšanas darbībām, un tai ir piekļuve visam nepieciešamajam aprīkojumam un iekārtām.

12. Personām, kuras atbild par atbilstības novērtēšanas darbību veikšanu, ir:

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

(b) pietiekamas zināšanas par prasībām attiecībā uz to veiktajiem atbilstības novērtējumiem un atbilstošas pilnvaras veikt minētos novērtējumus;

(c) pienācīgas zināšanas un izpratne par piemērojamām prasībām un testēšanas standartiem;

(d) prasme sagatavot sertifikātus, ierakstus un ziņojumus, kas apliecina atbilstības novērtējumu veikšanu.

13. Tiek garantēta atbilstības novērtēšanas struktūru, to augstākās vadības, personu, kuras atbild par atbilstības novērtēšanas darbību veikšanu, un jebkuru apakšuzņēmēju neitralitāte.

14. Atbilstības novērtēšanas struktūras augstākās vadības un personu, kuras atbild par atbilstības novērtēšanas darbību veikšanu, atalgojums nav atkarīgs no veikto atbilstības novērtējumu skaita vai rezultātiem.

15. Atbilstības novērtēšanas struktūras nodrošina civiltiesiskās atbildības apdrošināšanu, ja vien civiltiesisko atbildību nav uzņēmusies dalībvalsts saskaņā ar saviem valsts tiesību aktiem vai dalībvalsts pati nav tieši atbildīga par atbilstības novērtēšanu.

16. Atbilstības novērtēšanas struktūra un tās darbinieki, komitejas, filiāles, apakšuzņēmēji un jebkādas citas ar atbilstības novērtēšanas struktūru saistītās struktūras vai ārēju struktūru darbinieki ievēro konfidencialitāti un glabā dienesta

noslēpumu attiecībā uz jebkādu informāciju, kura iegūta, veicot atbilstības novērtēšanas uzdevumus saskaņā ar šo regulu vai valsts tiesību normām, ar ko īsteno šo regulu, izņemot gadījumus, kad informācija ir jāatklāj saskaņā ar Savienības vai dalībvalstu tiesību aktiem, kuri šīm personām ir jāievēro; tas neattiecas uz to dalībvalstu kompetentajām iestādēm, kurās tās veic savas darbības. Intelektuālā īpašuma tiesības tiek aizsargātas. Attiecībā uz šajā punktā noteiktajām prasībām atbilstības novērtēšanas struktūra paredz dokumentētas procedūras.

17. ***Izņemot attiecībā uz 16. punktu, šajā pielikumā noteiktās prasības neliedz atbilstības novērtēšanas struktūrai un personai, kas iesniedz sertifikācijas pieteikumu vai apsver iespēju to iesniegt, apmainīties ar tehnisko informāciju un regulatīviem norādījumiem.***

18. ***Atbilstības novērtēšanas struktūras darbojas saskaņā ar konsekventiem, taisnīgiem un saprātīgiem noteikumiem, attiecībā uz maksām ņemot vērā MVU intereses.***

19. ***Atbilstības novērtēšanas struktūras atbilst attiecīgā standarta prasībām, kurš ir saskaņots atbilstīgi Regulai (EK) Nr. 765/2008 attiecībā uz to atbilstības novērtēšanas struktūru akreditāciju, kas veic IKT produktu, IKT pakalpojumu, IKT procesu vai pārvaldītu drošības pakalpojumu sertifikāciju.***

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

Or. en