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)

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

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

ņemot vērā Reģionu komitejas atzinumu ([2]),

saskaņā ar parasto likumdošanas procedūru ([3]),

tā kā:

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

(2) Iedzīvotāji, organizācijas un uzņēmumi plaši izmanto tīklu un informācijas sistēmas visā Savienības teritorijā. Digitalizācija un savienojamība kļūst par galvenajiem elementiem aizvien plašākajā produktu un pakalpojumu klāstā, un, attīstoties lietu internetam, paredzams, ka tuvākajā desmitgadē visā Savienībā izmantos ārkārtīgi augstu skaitu satīkloto digitālo ierīču. Lai gan internetam pieslēgto ierīču kļūst aizvien vairāk, drošība un noturība nav pietiekami integrēta un līdz ar to arī kiberdrošības līmenis nav pietiekami augsts. Minētajos apstākļos, ja sertifikācijas izmantošana ir ierobežota, ne individuālie lietotāji, ne lietotāji organizācijās un uzņēmumos, nav pietiekami informēti par IKT produktu, pakalpojumu un IKT procesu kiberdrošības aspektiem, kas mazina uzticēšanos digitālajiem risinājumiem. Tīklu un informācijas sistēmas spēj atbalstīt visus mūsu dzīves aspektus un virzīt Savienības ekonomikas izaugsmi. Tās ir stūrakmens digitālā vienotā tirgus sasniegšanai.

(3) Aizvien plašākā digitalizācija un satīklojamība palielina kiberdrošības riskus, tādējādi sabiedrību kopumā padarot mazāk aizsargātu pret kiberdraudiem un palielinot briesmas, ar ko saskaras iedzīvotāji, tostarp tādas neaizsargātas personas kā bērni. Lai mazinātu minētos riskus, ir jāveic visi vajadzīgie pasākumi, kuru mērķis ir uzlabot kiberdrošību Savienībā, lai tīklu un informācijas sistēmas, sakaru tīkli, digitālie produkti, pakalpojumi un ierīces, ko izmanto iedzīvotāji, organizācijas un uzņēmumi, sākot no maziem un vidējiem uzņēmumiem (MVU), kā definēts Komisijas Ieteikumā 2003/361/EK ([4]), līdz pat kritiskās infrastruktūras apsaimniekotājiem, būtu labāk aizsargāti pret kiberdraudiem.

([1]) OV C 227, 28.6.2018., 86. lpp.
([2]) OV C 176, 23.5.2018., 29. lpp.
([3]) Eiropas Parlamenta 2019. gada 12. marta nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2019. gada 9. aprīļa lēmums.
([4]) Komisijas Ieteikums (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

(4) Eiropas Savienības Tīklu un informācijas drošības aģentūra (*ENISA*), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 526/2013 ([5]), sabiedrībai darot pieejamu attiecīgu informāciju, sekmē kiberdrošības nozares attīstību Savienībā, jo īpaši MVU un jaunuzņēmumu veidošanos. *ENISA* būtu jātiecas veidot ciešāku sadarbību ar augstākās izglītības iestādēm un pētniecības iestādēm, lai mazinātu atkarību no kiberdrošības produktiem un pakalpojumiem, kuru izcelsme ir ārpus Savienības, un stiprinātu piegādes ķēdes Savienības iekšienē.

(5) Kiberuzbrukumi kļūst aizvien biežāki, tāpēc satiklotai ekonomikai un sabiedrībai, kas ir mazāk aizsargāta pret kiberdraudiem un uzbrukumiem, ir vajadzīga spēcīgāka aizsardzība. Tomēr, lai gan kiberuzbrukumi bieži notiek pāri robežām, kiberdrošības iestāžu un tiesībaizsardzības iestāžu kompetence un politiskā reakcija pārsvarā ir valstu piekritībā. Plašapmēra incidenti var pārtraukt būtisku pakalpojumu sniegšanu visā Savienībā. Tas rada vajadzību pēc efektīvas un koordinētas Savienības līmeņa atbildes un krīžu pārvarēšanas, kuras pamatā izmantota specifiska politika un plašāka mēroga instrumenti Eiropas solidaritātes un savstarpējā atbalsta nodrošināšanai. Turklāt politikas veidotājiem, nozarei un lietotājiem ir svarīgi, lai kiberdrošības un noturības stāvoklis Savienībā tiktu regulāri izvērtēts, pamatojoties uz ticamiem Savienības līmeņa datiem, kā arī lai sistemātiski tiktu prognozēta turpmākā attīstība, izaicinājumi un draudi Savienības un globālā līmenī.

(6) Ņemot vērā pieaugošos kiberdrošības izaicinājumus, ar ko saskaras Savienība, ir jāizveido visaptverošs pasākumu kopums, kas papildinātu agrāko Savienības rīcību un palīdzētu sasniegt savstarpēji pastiprinošus mērķus. Minētie mērķi paredz vairāk uzlabot dalībvalstu un uzņēmumu spējas un sagatavotību, kā arī sekmēt sadarbību, informācijas apmaiņu un koordināciju starp dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām. Turklāt, ņemot vērā kiberdraudu pārrobežu raksturu, ir jāpalielina spējas Savienības līmenī, kas varētu papildināt dalībvalstu rīcību, sevišķi plašapmēra pārrobežu incidentu un krīžu gadījumā, vienlaikus ņemot vērā to, cik svarīgi ir saglabāt un vēl vairāk uzlabot valstu spējas reaģēt uz jebkāda apjoma kiberdraudiem.

(7) Vajadzīgi arī papildu centieni, kas uzlabotu iedzīvotāju, organizāciju un uzņēmumu izpratni kiberdrošības jautājumos. Turklāt, ņemot vērā to, ka incidenti mazina uzticēšanos digitālo pakalpojumu sniedzējiem un pašam digitālajam tirgum, jo īpaši patērētāju vidū, uzticēšanās būtu vēl vairāk jāstiprina, pārredzamā veidā sniedzot informāciju par IKT produktu, IKT pakalpojumu un IKT procesu drošības līmeni, kurā uzsvērts, ka pat augsts kiberdrošības sertifikācijas līmenis nevar garantēt IKT produkta, IKT pakalpojuma vai IKT procesa pilnīgu drošību. Lielāku uzticēšanos var veicināt Savienības mēroga sertifikācija, kuras ietvaros visos valstu tirgos un nozarēs tiktu nodrošinātas vienotas kiberdrošības prasības un izvērtēšanas kritēriji.

(8) Kiberdrošība nav tikai jautājums par tehnoloģiju, vienlīdz svarīga ir arī cilvēku uzvedība. Tāpēc būtu pastiprināti jāveicina "kiberhigiēna", proti, vienkārši ikdienā veicami pasākumi, kurus ieviešot un regulāri veicot iedzīvotāji, organizācijas un uzņēmumi samazina kiberdraudu radītos riskus.

(9) Lai stiprinātu Savienības kiberdrošības struktūras, ir svarīgi uzturēt un attīstīt dalībvalstu spējas visaptveroši reaģēt uz kiberdraudiem, tostarp pārrobežu incidentiem.

(10) Uzņēmumu un patērētāju rīcībā vajadzētu būt precīzai informācijai par to, kāda līmeņa drošības apliecinājumam sertificēti to IKT produkti, IKT pakalpojumi un IKT procesi. Tajā pašā laikā neviens IKT produkts vai IKT pakalpojums nav pilnībā kiberdrošs, un ir jāpopularizē un par prioritāti jāizvirza kiberhigiēnas pamatnoteikumi. Ņemot vērā to, ka arvien pieejamākas kļūst lietu interneta ierīces, ir pieejams plašs tādu brīvprātīgu pasākumu klāsts, kurus privātais sektors var veikt, lai pastiprinātu IKT produktu, IKT pakalpojumu un IKT procesu drošību.

(11) Mūsdienīgos IKT produktos un sistēmās bieži ir integrēta viena vai vairākas trešo personu tehnoloģijas un komponenti, piemēram, programmatūras moduļi, krātuves vai lietojumprogrammu saskarnes, un minētie produkti un sistēmas ir atkarīgi no šīm tehnoloģijām un komponentiem. Šī "atkarība" varētu radīt papildu kiberdrošības riskus, jo trešo personu komponentos atrastās ievainojamības varētu ietekmēt arī IKT produktu, IKT pakalpojumu un IKT procesu drošību. Daudzos gadījumos šādas atkarības identificēšana un dokumentēšana dod iespēju IKT produktu, IKT pakalpojumu un IKT procesu galalietotājiem uzlabot savas kiberdrošības riska pārvaldības darbības, piemēram, uzlabojot lietotāju kiberdrošības ievainojamības pārvaldības un novēršanas procedūras.

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

(12) Organizācijas, ražotāji vai pakalpojumu sniedzēji, kas iesaistīti IKT produktu, IKT pakalpojumu un IKT procesu projektēšanā un attīstībā, būtu jāmudina pēc iespējas agrīnā projektēšanas un attīstības stadijā iespējami visaugstākajā līmenī aizsargāt minēto produktu, procesu un pakalpojumu drošību, paredzot kiberuzbrukumu iespējamību un prognozējot un mazinot to ietekmi (integrētā drošība). Drošība būtu jānodrošina visā IKT produkta, IKT pakalpojuma vai IKT procesa dzīves cikla laikā, izmantojot projektēšanas un izstrādes procesus, kas pastāvīgi attīstās, lai samazinātu ļaunprātīgas izmantošanas kaitējuma risku.

(13) Uzņēmumiem, organizācijām un publiskajam sektoram to projektētie IKT produkti, IKT pakalpojumi vai IKT procesi būtu jākonfigurē tā, ka tiek nodrošināta augstāka līmeņa drošība, kam vajadzētu dot iespēju pirmajam lietotājam saņemt standarta konfigurāciju ar visdrošākajiem iestatījumiem, kādi vien ir iespējami (drošība pēc noklusējuma), tādējādi lietotājiem samazinot slogu, kas rastos, ja viņiem pašiem būtu pienācīgi jākonfigurē IKT produkts, IKT pakalpojums vai IKT process. Drošībai pēc noklusējuma nevajadzētu būt tādai, kurai ir nepieciešama plaša konfigurēšana vai tādai, kuras lietotājam būtu specifiska tehniska izpratne vai arī tam jāveic rīcība, kas nav pašsaprotama, un pēc iestatīšanas tai vajadzētu darboties vienkārši un uzticami. Ja attiecīgā gadījumā riska un lietojamības analīze liek izdarīt secinājumu, ka šādi standarta iestatījumi nav iespējami, lietotāji būtu jāmudina izvēlēties visdrošākos iestatījumus.

(14) Eiropas Parlamenta un Padomes Regula (EK) Nr. 460/2004 ([6]) izveidoja *ENISA*, lai tā sekmētu augsta un efektīva līmeņa tīklu un informācijas drošības mērķu sasniegšanu Savienībā un palīdzētu attīstīt tīklu un informācijas drošības kultūru, kas nāktu par labu iedzīvotājiem, patērētājiem, uzņēmumiem un valsts pārvaldes iestādēm. Ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1007/2008 ([7]) pagarināja *ENISA* pilnvaru termiņu līdz 2012. gada martam. Savukārt ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 580/2011 ([8]) *ENISA* pilnvaru termiņu pagarināja līdz 2013. gada 13. septembrim. Ar Regulu (ES) Nr. 526/2013 *ENISA* pilnvaru termiņu pagarināja līdz 2020. gada 19. jūnijam.

(15) Savienība jau ir veikusi būtiskus pasākumus, lai nodrošinātu kiberdrošību un palielinātu uzticēšanos digitālajām tehnoloģijām. 2013. gadā tika pieņemta Eiropas Savienības kiberdrošības stratēģija ar mērķi dot virzību Savienības politiskajai reakcijai uz kiberdraudiem un kiberriskiem. Cenšoties uzlabot iedzīvotāju aizsardzību tiešsaistē, 2016. gadā tika pieņemts pirmais Savienības tiesību akts kiberdrošības jomā, proti, Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 ([9]). Direktīvā (ES) 2016/1148 ir ieviestas prasības attiecībā uz valstu spējām kiberdrošības jomā, izveidoti pirmie mehānismi dalībvalstu stratēģiskās un operatīvās sadarbības stiprināšanai un noteikti pienākumi attiecībā uz drošības pasākumiem un incidentu paziņošanu ekonomiski un sabiedriski nozīmīgās nozarēs, piemēram, enerģētikā, transporta, dzeramā ūdens piegādes un izplatīšanas, banku, finanšu tirgus infrastruktūru, veselības aprūpes un digitālās infrastruktūras nozarē, kā arī pienākumi galvenajiem digitālo pakalpojumu sniedzējiem (meklētājprogrammas, mākoņdatošanas pakalpojumi un tiešsaistes tirdzniecības vietas).

Lai atbalstītu minētās direktīvas īstenošanu, *ENISA* tika uzticēta būtiska loma. Turklāt efektīva cīņa pret kibernoziegumiem ir noteikta par svarīgu prioritāti Eiropas Drošības programmā, tādējādi palīdzot sasniegt vispārējo mērķi attiecībā uz augstu kiberdrošības līmeni. Augsta līmeņa kiberdrošību digitālajā vienotajā tirgū veicina arī citi tiesību akti, piemēram, Eiropas Parlamenta un Padomes Regula (ES) 2016/679 ([10]) un Eiropas Parlamenta un Padomes Direktīva 2002/58/EK ([11]) un (ES) 2018/1972 ([12]).

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

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

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

([9]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

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

([11]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

([12]) Eiropas Parlamenta un Padomes Direktīva (ES) 2018/1972 (2018. gada 11. decembris) par Eiropas Elektronisko sakaru kodeksa izveidi (OV L 321, 17.12.2018., 36. lpp.).

(16) Kopš Eiropas Savienības kiberdrošības stratēģijas pieņemšanas 2013. gadā un *ENISA* pilnvaru pēdējās pārskatīšanas vispārējais politikas konteksts ir ievērojami mainījies, jo situācija pasaules mērogā ir kļuvusi aizvien neskaidrāka un nedrošāka. Šajā sakarībā un saistībā ar pozitīvo *ENISA* lomas attīstību, kura ir uzziņas punkts padomiem un lietpratībai un darbojas kā sadarbības un spēju veidošanas sekmētāja, kā arī jaunās Savienības kiberdrošības politikas satvarā ir jāpārskata *ENISA* pilnvaras, lai noteiktu tās uzdevumus mainītajā kiberdrošības ekosistēmā un nodrošinātu, ka tā dod efektīvu ieguldījumu Savienības reaģēšanā uz kiberdrošības izaicinājumiem, kas izriet no radikāli pārveidotās kiberdraudu ainas, attiecībā uz kuru, kā atzīts *ENISA* izvērtējumā, tagadējais pilnvaru tvērums nav pietiekami plašs.

(17) Ar šo regulu izveidotajai *ENISA* būtu jāpārņem ar Regulu (ES) Nr. 526/2013 izveidotās *ENISA* darbs. *ENISA* būtu jāpilda pienākumi, kas tai uzticēti ar šo regulu un ar citiem Savienības tiesību aktiem kiberdrošības jomā, cita starpā dodot padomus un daloties lietpratībā, kā arī darbojoties kā Savienības informācijas un zināšanu centram. Tai būtu jāveicina paraugprakses apmaiņa dalībvalstu un privāto ieinteresēto personu starpā, Komisijai un dalībvalstīm jāizvirza politikas ierosinājumi, jādarbojas kā uzziņas punktam attiecībā uz Savienības nozaru politikas iniciatīvām kiberdrošības jautājumos un jāsekmē operatīvā sadarbība gan dalībvalstu starpā, gan dalībvalstu un Savienības iestāžu, struktūru, biroju un aģentūru starpā.

(18) Saskaņā ar Lēmumu 2004/97/EK, Euratom, kas pieņemts, tiekoties dalībvalstu pārstāvjiem valstu un valdību vadītāju līmenī ([13]), dalībvalstu pārstāvji nolēma, ka *ENISA* atrašanās vieta būs kādā no Grieķijas pilsētām, kuru izvēlēsies Grieķijas valdība. *ENISA* mītnes dalībvalstij būtu jānodrošina pēc iespējas labāki apstākļi *ENISA* netraucētai un efektīvai darbībai. Lai tā varētu pienācīgi un efektīvi veikt savus uzdevumus, pieņemt darbā darbiniekus un noturēt tos un lai uzlabotu tīklošanas darbību efektivitāti, *ENISA* noteikti būtu jāatrodas piemērotā vietā, kurā cita starpā būtu nodrošināti pienācīgi transporta savienojumi un infrastruktūra darbinieku laulātajiem un bērniem. Nepieciešamie pasākumi būtu jāparedz *ENISA* un mītnes dalībvalsts nolīgumā, ko noslēgtu pēc *ENISA* Administratīvās padomes apstiprinājuma saņemšanas.

(19) Ņemot vērā pieaugošos kiberdrošības riskus un izaicinājumus, ar ko saskaras Savienība, būtu jāpalielina *ENISA* piešķirtie finansiālie līdzekļi un cilvēkresursi, lai tie atbilstu tās paplašinātajai lomai un uzdevumiem, kā arī īpaši svarīgajai nozīmei, kas tai ir to organizāciju ekosistēmā, kuras aizsargā Savienības digitālo ekosistēmu, dodot *ENISA* iespēju efektīvi veikt tai ar šo regulu uzticētos uzdevumus.

(20) *ENISA* būtu jāattīsta un jāsaglabā augsts lietpratības līmenis un jākļūst par uzziņas punktu, kas ar savu neatkarību, sniegto padomu kvalitāti, izplatītās informācijas kvalitāti, darba procedūru pārredzamību, darbības metožu pārredzamību un neatlaidību uzdevumu izpildē rada uzticēšanos vienotajam tirgum. *ENISA* būtu aktīvi jāatbalsta valstu centieni un būtu proaktīvi jāveicina Savienības centieni, pildot savus uzdevumus pilnīgā sadarbībā ar Savienības iestādēm, struktūrām, birojiem un aģentūrām un dalībvalstīm, izvairoties no darba dublēšanās un sekmējot sinerģiju. Turklāt *ENISA* būtu jāizmanto privātā sektora, kā arī citu attiecīgo ieinteresēto personu piedāvātais atbalsts un sadarbības iespējas. *ENISA* uzdevumu kopumam būtu jānosaka tās mērķu sasniegšanas veidi, vienlaikus ļaujot tai darboties elastīgi.

(21) Lai spētu nodrošināt pietiekamu atbalstu operatīvajai sadarbībai starp dalībvalstīm, *ENISA* būtu vēl vairāk jāstiprina savas tehniskās un cilvēkresursu iespējas un prasmes. *ENISA* būtu jāpaplašina tās zinātība un spējas. *ENISA* un dalībvalstis brīvprātīgi var izstrādāt programmas valsts ekspertu norīkošanai uz *ENISA*, izveidojot ekspertu rezerves sarakstus un personāla apmaiņu.

(22) *ENISA* būtu jāpalīdz Komisijai ar padomiem, atzinumiem un analīzi attiecībā uz visiem Savienības jautājumiem, kas ir saistīti ar politikas un tiesību aktu izstrādi, atjaunināšanu un pārskatīšanu kiberdrošības jomā un ar konkrētu nozaru kiberdrošības aspektiem, nolūkā palielināt Savienības politikas un tiesību aktu ar kiberdrošības dimensiju nozīmīgumu un panākt minētās politikas un tiesību aktu īstenošanas konsekvenci valstu līmenī. Saistībā ar konkrētu nozaru Savienības politikas un tiesību aktu iniciatīvām, kurās ietverti ar kiberdrošību saistīti jautājumi, *ENISA* būtu jādarbojas kā padomu un lietpratības uzziņas punktam. *ENISA* par savu darbību būtu regulāri jāinformē Eiropas Parlaments.

([13]) Lēmums 2004/97/EK, Euratom, kas pieņemts, tiekoties dalībvalstu pārstāvjiem valstu un valdību vadītāju līmenī, (2003. gada 13. decembris) par atsevišķu Eiropas Savienības biroju un aģentūru atrašanās vietu (OV L 29, 3.2.2004., 15. lpp.).

(23) Atklātā interneta publiskais kodols, proti tā galvenie protokoli un infrastruktūra, kas ir globāls sabiedrisks labums, nodrošina interneta būtiskākās funkcijas kopumā un ir tā normālas darbības pamats. *ENISA* būtu jāatbalsta atklātā interneta publiskā kodola drošība un tā funkcionēšanas stabilitāte, tostarp – bet ne tikai – attiecībā uz galvenajiem protokoliem (jo īpaši *DNS*, *BGP* un *IPv6*), domēnu nosaukumu sistēmas darbību (piemēram, visu augstākā līmeņa domēnu darbība) un sakņu zonas darbību.

(24) *ENISA* pamatuzdevums ir veicināt attiecīgā tiesiskā regulējuma konsekventu īstenošanu, jo īpaši Direktīvas (ES) 2016/1148 un citu attiecīgo tiesību instrumentu efektīvu īstenošanu, kuros ir ietverti kiberdrošības aspekti, kas ir būtiski svarīgi kibernoturības līmeņa paaugstināšanai. Ņemot vērā strauji mainīgo kiberdraudu ainu, ir skaidrs, ka dalībvalstis ir jāatbalsta ar visaptverošu daudznozaru pieeju kibernoturības veidošanā.

(25) *ENISA* būtu jāatbalsta dalībvalstu un Savienības iestāžu, struktūru, biroju un aģentūru centieni veidot un uzlabot spējas un gatavību novērst un atklāt kiberdraudus un incidentus, un reaģēt uz tiem, kā arī attiecībā uz tīklu un informācijas sistēmu drošību. *ENISA* jo īpaši būtu jāatbalsta Direktīvā (ES) 2016/1148 paredzēto valstu un Savienības datordrošības incidentu reaģēšanas vienību ("*CSIRT*") izveide un uzlabošana ar mērķi Savienībā tajās panākt vienādi augsta līmeņa gatavību. Darbībām, ko *ENISA* veic saistībā ar dalībvalstu operatīvajām spējām, būtu aktīvi jāpapildina dalībvalstu rīcība nolūkā pildīt to saistības saskaņā ar Direktīvu (ES) 2016/1148, un tādēļ ar tām nevajadzētu aizstāt dalībvalstu rīcību.

(26) *ENISA* arī būtu jāpalīdz izstrādāt un atjaunināt Savienības un – pēc pieprasījuma – dalībvalstu tīklu un informācijas sistēmu drošības, jo īpaši kiberdrošības, stratēģijas, un būtu jāveicina to izplatīšana un jāseko to īstenošanas virzībai. *ENISA* būtu arī jāsekmē tas, ka tiek apmierināta vajadzība pēc apmācībām un mācību materiāliem, tostarp publisko struktūru vajadzības, un attiecīgā gadījumā lielā mērā vajadzība pēc "mācībspēku apmācīšanas", pamatojoties uz iedzīvotāju digitālās kompetences satvaru nolūkā palīdzēt dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām attīstīt pašām savas apmācības spējas.

(27) *ENISA* dalībvalstis būtu jāatbalsta kiberdrošības izpratnes veicināšanas un izglītības jomā, sekmējot ciešāku koordināciju un paraugprakšu apmaiņu starp dalībvalstīm. Šāds atbalsts var izpausties kā valsts izglītības kontaktpunktu tīkla izveide un kiberdrošības apmācības platformas izveide. Valsts izglītības kontaktpunktu tīkls varētu darboties valsts sadarbības koordinatoru tīkla ietvaros un kļūt par turpmākas koordinācijas aizsākumu dalībvalstīs.

(28) *ENISA* būtu jāpalīdz ar Direktīvu (ES) 2016/1148 izveidotajai Sadarbības grupai pildīt tās uzdevumus, jo īpaši daloties lietpratībā, sniedzot padomus un veicinot paraugprakses apmaiņu, cita starpā attiecībā uz pamatpakalpojumu sniedzēju identifikāciju, ko veic dalībvalstis, kā arī pievēršoties pārrobežu atkarībai saistībā ar riskiem un incidentiem.

(29) Lai stimulētu sadarbību starp publisko un privāto sektoru un starp privātā sektora dalībniekiem, jo īpaši nolūkā atbalstīt kritiskās infrastruktūras aizsardzību, *ENISA* būtu jāatbalsta informācijas apmaiņa nozarēs un starp tām, jo īpaši nozarēs, kas uzskaitītas Direktīvas (ES) 2016/1148 II pielikumā, nodrošinot paraugpraksi un norādījumi par pieejamajiem rīkiem un procedūrām, kā arī sniedzot norādījumus, kā pievērsties regulatīviem problēmjautājumiem saistībā ar informācijas apmaiņu, piemēram, veicinot nozaru informācijas apmaiņas un analīzes centru izveidi.

(30) Apstākļos, kad arvien palielinās potenciālā negatīvā ietekme, kas izriet no IKT produktu, IKT pakalpojumu un IKT procesu ievainojamībām, šādu ievainojamību atrašana un novēršana ir ārkārtīgi nozīmīga, lai samazinātu vispārējo kiberdrošības risku. Sadarbība starp organizācijām, tādiem ražotājiem vai pakalpojumu sniedzējiem, kuru IKT produktiem, IKT pakalpojumiem un IKT procesiem piemīt ievainojamības, un kiberdrošības pētniecības kopienu un valdībām, kas ievainojamības atklāj, ir parādījusi, ka tā būtiski palielina IKT produktu, IKT pakalpojumu un IKT procesu ievainojamību atklāšanu un novēršanu. Koordinēta ievainojamību atklāšana ir strukturēts sadarbības process, kurā par ievainojamībām tiek ziņots informācijas sistēmas īpašniekam, dodot attiecīgajai organizācijai iespēju diagnosticēt un novērst ievainojamību pirms detalizēta informācija par to tiek darīta zināma trešām pusēm vai sabiedrībai. Šis process arī paredz koordināciju starp ievainojamības atklājēju un attiecīgo organizāciju par minēto ievainojamību publiskošanu. Koordinētai ievainojamību atklāšanas politikai varētu būt ļoti svarīga nozīme dalībvalstu centienos pastiprināt kiberdrošību.

(31) Lai informācijas apmaiņas vajadzībām sekmētu kopīgu procedūru, valodas lietojuma un terminoloģijas ieviešanu, Aģentūrai būtu jāapkopo un jāanalizē valstu brīvprātīgā kārtā sniegtie *CSIRT* ziņojumi un starpiestāžu datorapdraudējumu reaģēšanas vienības Savienības iestādēm, struktūrām un aģentūrām, kas izveidota ar Vienošanos 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 ([14]) ziņojumi. Šajā saistībā *ENISA* būtu jāiesaista privātais sektors saistībā ar Direktīvu (ES) 2016/1148, kurā izklāstīti iemesli brīvprātīgai tehniskās informācijas apmaiņai operatīvā līmenī datordrošības incidentu reaģēšanas vienību tīkla ("*CSIRT* tīkls"), kas izveidots ar minēto direktīvu, iekšienē.

(32) *ENISA* būtu jāpalīdz nodrošināt Savienības līmeņa reaģēšanu uz plašapmēra pārrobežu incidentiem un krīzēm saistībā ar kiberdrošību. Minētais uzvedums būtu jāveic atbilstīgi *ENISA* pilnvarām saskaņā ar šo regulu un ar pieeju, par kuru dalībvalstīm jāvienojas saistībā ar Komisijas Ieteikumu (ES) 2017/1584 ([15]) un Padomes 2018. gada 26. jūnija secinājumiem par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm. Minētais uzdevums varētu ietvert attiecīgas informācijas vākšanu un starpniecības veicināšanu starp *CSIRT* tīklu un tehniskajiem speciālistiem, kā arī starp par krīžu pārvarēšanu atbildīgajiem lēmumu pieņēmējiem. Turklāt *ENISA* – ja to prasa viena vai vairākas dalībvalstis – tehniskā ziņā būtu jāatbalsta dalībvalstu operatīvā sadarbība incidentu risināšanā, sekmējot attiecīgo tehnisko risinājumu apmaiņu starp dalībvalstīm un sniedzot ieguldījumu informācijas publiskošanas jomā. *ENISA* būtu jāatbalsta operatīvā sadarbība, pārbaudot šādas sadarbības kārtību regulārās kiberdrošības mācībās.

(33) Sniedzot atbalstu operatīvajai sadarbībai, *ENISA* būtu jāizmanto pieejamā *CERT-EU* tehniskā un operatīvā lietpratība, izmantojot strukturētu sadarbību. Šādas strukturētās sadarbības pamatā varētu būt *ENISA* lietpratība. Attiecīgā gadījumā starp abām vienībām būtu jāpanāk īpaša vienošanās par šādas sadarbības praktiskas īstenošanas kārtību un jāizvairās no darbību dublēšanās.

(34) Īstenojot uzdevumu atbalstīt operatīvo sadarbību *CSIRT* tīkla iekšienē *ENISA* būtu jāspēj sniegt atbalstu dalībvalstīm pēc to pieprasījuma, piemēram, sniedzot padomus par to, kā uzlabot to spējas novērst un atklāt incidentus un reaģēt uz tiem, atvieglojot tādu incidentu tehnisku novēršanu, kuriem ir būtiska vai nozīmīga ietekme vai nodrošinot kiberdraudu un incidentu analīzi. *ENISA* būtu jāsekmē tādu incidentu tehniska novēršana, kuriem ir būtiska vai nozīmīga ietekme, jo īpaši atbalstot brīvprātīgu apmaiņu ar tehniskiem risinājumiem starp dalībvalstīm vai izstrādājot apvienotu tehnisko informāciju, piemēram, tehniskus risinājumus, ar kuriem dalībvalstis ir dalījušās brīvprātīgi. Ieteikumā (ES) 2017/1584 ieteikts dalībvalstīm godprātīgi sadarboties un bez liekas kavēšanās savā starpā un ar *ENISA* dalīties ar informāciju par plašapmēra incidentiem un krīzēm saistībā ar kiberdrošību. Šādai informācijai vēl vairāk palīdzētu *ENISA* pildīt operatīvās sadarbības atbalsta uzdevumu.

(35) Lai regulāras tehniskās sadarbības ietvaros veicinātu situācijas apzināšanos Savienībā, *ENISA* ciešā sadarbībā ar dalībvalstīm būtu jāsagatavo regulārs padziļināts ES kiberdrošības tehniskās situācijas ziņojums par incidentiem un kiberdraudiem, kuri balstīti uz publiski pieejamu informāciju, Aģentūras veikto analīzi un ziņojumiem, ko tai snieguši dalībvalstu *CSIRT* vai Direktīvā (ES) 2016/1148 paredzētie valsts vienotie kontaktpunkti, kas atbild par tīklu un informācijas sistēmu drošību ("vienotie kontaktpunkti") – abos gadījumos brīvprātīgi –, Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), *CERT-EU* un – attiecīgā gadījumā – Eiropas Ārējās darbības dienesta Eiropas Savienības Izlūkdatu analīzes centrs (*EU INTCEN*). Minētais ziņojums būtu jādara pieejams Padomei, Komisijai, Savienības Augstajam pārstāvim ārlietās un drošības politikas jautājumos un *CSIRT* tīklam.

(36) *ENISA* atbalstā, ko tā pēc attiecīgo dalībvalstu pieprasījuma sniedz, lai veiktu ex post tehnisko izmeklēšanu par incidentiem, kam ir būtiska vai nozīmīga ietekme, būtu jāorientējas uz turpmāku incidentu novēršanu. Attiecīgajām dalībvalstīm būtu jārīkojas, sniedzot nepieciešamo informāciju un palīdzību, lai dotu *ENISA* iespēju efektīvi atbalstīt *ex post* tehnisko izmeklēšanu.

([14]) OV C 12, 13.1.2018., 1. lpp.
([15]) 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.).

(37) Dalībvalstis var aicināt uzņēmumus, kurus skāris incidents, sadarboties un sniegt *ENISA* nepieciešamo informāciju un palīdzību, neskarot to tiesības aizsargāt sensitīvu komercinformāciju un ar sabiedrisko drošību saistītu informāciju.

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

(39) Lai palielinātu Savienības noturību, *ENISA*, sniedzot padomus, izdodot pamatnostādnes un apmainoties ar paraugpraksi, būtu jāattīsta lietpratība infrastruktūru kiberdrošības jomā, jo īpaši, lai atbalstītu Direktīvas (ES) 2016/1148 II pielikumā uzskaitītās nozares un tās, ko izmanto digitālo pakalpojumu sniedzēji, kas ir uzskaitīti minētās direktīvas III pielikumā. Lai nodrošinātu vienkāršāku piekļuvi labāk strukturētai informācijai par kiberdrošības riskiem un iespējamiem risinājumiem, *ENISA* būtu jāizveido un jāuztur Savienības "informācijas mezgls", kas darbotos kā vienots kontaktpunkts – portāls, kurā plašāka sabiedrība varētu iepazīties ar Savienības un dalībvalstu iestāžu, struktūru, biroju un aģentūru sniegto informāciju par kiberdrošību. Atvieglota piekļuve labāk strukturētai informācijai par kiberdrošības riskiem un iespējamiem risinājumiem varētu arī palīdzēt dalībvalstīm uzlabot to spējas un saskaņot praksi, tādējādi palielinot to vispārējo noturību pret kiberuzbrukumiem.

(40) *ENISA* būtu jāpalīdz uzlabot sabiedrības izpratni par kiberdrošības riskiem, tostarp izvēršot ES mēroga izpratnes veicināšanas kampaņu un veicinot izglītošanos šajos jautājumos, un būtu jāsniedz iedzīvotājiem, organizācijām un uzņēmumiem adresēti norādījumi par labu praksi individuāliem lietotājiem. *ENISA* iedzīvotāju, organizāciju un uzņēmumu līmenī arī būtu jāpalīdz veicināt paraugpraksi un risinājumus, tostarp attiecībā uz kiberhigiēnu un kiberpratību, apkopojot un analizējot publiski pieejamu informāciju par būtiskiem incidentiem un apkopojot un publicējot ziņojumus un norādījumus iedzīvotājiem, organizācijām un uzņēmumiem vispārējās sagatavotības līmeņa un noturības uzlabošanai. *ENISA* arī būtu jācenšas sniegt patērētājiem attiecīgu informāciju par piemērojamām sertifikācijas shēmām, piemēram, sniedzot pamatnostādnes un ieteikumus. Turklāt *ENISA* atbilstīgi Digitālās izglītības rīcības plānam, kas paredzēts Komisijas 2018. gada 17. janvāra paziņojumā, un sadarbībā ar dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām būtu jāorganizē uz galalietotājiem vērstas regulāras informatīvās un sabiedrības izglītošanas kampaņas, lai veicinātu indivīdu tiešsaistes uzvedības drošākus paradumus un digitālo pratību, palielinātu izpratni par potenciālajiem kiberdraudiem, tostarp par tādiem kriminālpārkāpumiem tiešsaistē kā pikšķerēšanas uzbrukumi, robottīkli, krāpšana finanšu un banku darījumos, datu krāpšanas incidenti, kā arī veicināt pamatieteikumus attiecībā uz daudzfaktoru autentifikāciju, nepilnību lāpīšanu, šifrēšanu, anonimizāciju un datu aizsardzību.

(41) *ENISA* būtu jāuzņemas nozīmīga loma, straujāk uzlabojot galalietotāju izpratni par ierīču drošību un pakalpojumu drošu izmantošanu un Savienības līmenī būtu jāsekmē integrētā drošība un integrētā privātuma aizsardzība. Tiecoties uz minēto mērķi, *ENISA* būtu jāizmanto pieejamā paraugprakse un pieredze, jo īpaši akadēmisko iestāžu un IT drošības pētnieku paraugprakse un pieredze.

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

(43) *ENISA* kiberdrošības jomā būtu jāsekmē Savienības centieni sadarboties ar starptautiskām organizācijām, kā arī attiecīgajos starptautiskās sadarbības satvaros. Jo īpaši *ENISA* attiecīgā gadījumā būtu jāsekmē sadarbība ar tādām organizācijām kā *OECD*, EDSO un NATO. Šāda sadarbība varētu ietvert kopīgas kiberdrošības mācības un kopīgas reaģēšanas koordinēšanu incidentu gadījumā. Minētās darbības jāveic, pilnībā respektējot iekļautības, savstarpības un Savienības lēmumu pieņemšanas autonomijas principus, neskarot dalībvalstu drošības un aizsardzības politikas specifiskās iezīmes.

(44) Lai nodrošinātu savu mērķu pilnīgu sasniegšanu, *ENISA* būtu jāsadarbojas ar attiecīgām Savienības uzraudzības iestādēm un citām kompetentajām iestādēm Savienībā, Savienības iestādēm, struktūrām, birojiem un aģentūrām, tostarp *CERT-EU*, *EC3*, Eiropas Aizsardzības aģentūru (EAA), Eiropas Globālās navigācijas satelītu sistēmas aģentūru (Eiropas *GNSS* aģentūru), Eiropas Elektronisko komunikāciju regulatoru iestādi (*BEREC*), Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*), Eiropas Centrālo banku (ECB), Eiropas Banku iestādi (EBI), Eiropas Datu aizsardzības kolēģiju, Energoregulatoru sadarbības aģentūru (*ACER*) Eiropas Savienības Aviācijas drošības aģentūru (*EASA*) un visām citām Savienības aģentūrām, kas iesaistītas kiberdrošības jautājumu risināšanā. *ENISA* būtu jāsadarbojas arī ar iestādēm, kas nodarbojas ar datu aizsardzību, lai apmainītos ar zinātību un paraugpraksi, un būtu jāsniedz padomi par kiberdrošības aspektiem, kas varētu ietekmēt to darbu. Valstu un Savienības tiesībaizsardzības un datu aizsardzības iestāžu pārstāvjiem vajadzētu būt tiesībām piedalīties *ENISA* Padomdevēju grupā. Sadarbojoties ar tiesībaizsardzības iestādēm attiecībā uz tīklu un informācijas drošības aspektiem, kas varētu ietekmēt viņu darbu, *ENISA* būtu jāņem vērā pastāvošie informācijas kanāli un izveidotie tīkli.

(45) Varētu veidot partnerības ar akadēmiskām iestādēm, kuras īsteno pētniecības iniciatīvas attiecīgajās jomās, un vajadzētu būt atbilstīgiem kanāliem patērētāju un citu organizāciju ieguldījumam, kas būtu jāpieņem zināšanai.

(46) *ENISA*, pildot *CSIRT* tīkla sekretariāta pienākumus, būtu jāatbalsta dalībvalstu *CSIRT* un *CERT-EU* operatīvā sadarbība saistībā ar attiecīgajiem *CSIRT* tīkla uzdevumiem, kā minēts Direktīvā (ES) 2016/1148. Turklāt *ENISA*, pienācīgi ņemot vērā *CSIRT* tīkla darbības standartprocedūras, būtu jāveicina un jāatbalsta sadarbība starp attiecīgām *CSIRT* vienībām, ja *CSIRT* pārvaldītu vai aizsargātu tīklu vai infrastruktūru ir skāris incidents, uzbrukums vai traucējumi, kas attiecas vai varētu attiekties vismaz uz divām *CSIRT*.

(47) Lai uzlabotu Savienības gatavību saistībā ar reaģēšanu uz incidentiem, *ENISA* būtu regulāri jāorganizē kiberdrošības mācības Savienības līmenī un pēc to pieprasījuma jāsniedz atbalsts šādu mācību organizēšanā dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām. Reizi divos gados būtu jāorganizē liela mēroga visaptverošas mācības, kuras aptver tehniskus, operatīvus vai stratēģiskus elementus. Turklāt *ENISA* vajadzētu būt iespējai regulāri organizēt mācības, kas nav tik visaptverošas, bet ar tādu pašu mērķi, proti, – uzlabot Savienības gatavību reaģēt uz incidentiem.

(48) *ENISA* būtu vēl vairāk jāattīsta un jāsaglabā sava lietpratība kiberdrošības sertifikācijas jautājumos, lai tā spētu atbalstīt Savienības politiku minētajā jomā. *ENISA* būtu jāizmanto pastāvošā paraugprakse un jāveicina kiberdrošības sertifikācijas ieviešana Savienībā, tostarp Savienības līmenī palīdzot izveidot un uzturēt kiberdrošības sertifikācijas satvaru (Eiropas kiberdrošības sertifikācijas satvars), lai uzlabotu IKT produktu, IKT pakalpojumu un IKT procesu kiberdrošības apliecinājuma pārredzamību, tādējādi stiprinot uzticēšanos digitālajam iekšējam tirgum un tā konkurētspēju.

(49) Efektīvas kiberdrošības politikas pamatā gan publiskajā, gan privātajā sektorā vajadzētu būt labi izstrādātām riska izvērtēšanas metodēm. Riska izvērtēšanas metodes izmanto dažādos līmeņos, un nav vienotas prakses attiecībā uz to efektīvu piemērošanu. Publiskā sektora un privātā sektora organizācijās veicinot un attīstot riska izvērtēšanas un sadarbspējīgu riska pārvaldības risinājumu paraugpraksi, tiks paaugstināts kiberdrošības līmenis Savienībā. Tādēļ *ENISA* būtu jāatbalsta ieinteresēto personu sadarbība Savienības līmenī un jāpalīdz tām izveidot un pārņemt Eiropas un starptautiskos standartus, ko izmanto, lai pārvaldītu riskus un izmērītu drošību attiecībā uz elektroniskiem produktiem, sistēmām, tīkliem un pakalpojumiem, kas kopā ar programmatūru veido tīkla un informācijas sistēmas.

(50) *ENISA* būtu jāmudina dalībvalstis, IKT produktu, IKT pakalpojumu vai IKT procesu ražotāji vai sniedzēji paaugstināt savus vispārīgos drošības standartus tā, lai visi interneta lietotāji varētu veikt nepieciešamos pasākumus paši savas kiberdrošības panākšanai un būtu jānodrošina stimuls to darīt. Jo īpaši, IKT produktu, IKT pakalpojumu vai IKT procesu ražotājiem vai sniedzējiem būtu jānodrošina visi nepieciešamie atjauninājumi un būtu jāatsauc, jāizņem no tirgus vai jāpārstrādā kiberdrošības standartiem neatbilstoši IKT produkti, IKT pakalpojumi un IKT procesi, savukārt importētājiem un izplatītājiem būtu jāpārliecinās, ka IKT produkti, IKT pakalpojumi un IKT procesi, ko tie laiž Savienības tirgū, atbilst piemērojamajām prasībām un nerada risku Savienības patērētājiem.

(51) Sadarbībā ar kompetentajām iestādēm *ENISA* vajadzētu būt iespējai izplatīt informāciju par iekšējā tirgū piedāvāto IKT produktu, IKT pakalpojumu un IKT procesu kiberdrošības līmeni un būtu jāizdod IKT produktu, IKT pakalpojumu vai IKT procesu ražotājiem vai sniedzējiem brīdinājumi un jāprasa tiem uzlabot savu IKT produktu, IKT pakalpojumu un IKT procesu drošību, tostarp kiberdrošību.

(52) *ENISA* būtu pilnībā jāņem vērā aktuālie pētniecības, izstrādes un tehnoloģiju izvērtēšanas pasākumi, jo īpašie tie, kas notiek saskaņā ar dažādām Savienības pētniecības iniciatīvām, lai Savienības iestādēm, struktūrām, birojiem un aģentūrām, kā arī attiecīgos gadījumos pēc to pieprasījuma dalībvalstīm sniegtu padomus par pētījumu vajadzībām un prioritātēm kiberdrošības jomā. Nolūkā apzināt pētniecības vajadzības un prioritātes *ENISA* būtu jāapspriežas arī ar attiecīgajām lietotāju grupām. Konkrētāk, varētu iedibināt sadarbību ar Eiropas Pētniecības padomi, Eiropas Inovāciju un tehnoloģiju institūtu un ar Eiropas Savienības Drošības izpētes institūtu.

(53) *ENISA*, gatavojot Eiropas kiberdrošības sertifikācijas shēmas, būtu regulāri jāapspriežas ar standartizācijas organizācijām, jo īpaši Eiropas standartizācijas organizācijām.

(54) Kiberdraudi ir pasaules mēroga problēma. Lai uzlabotu kiberdrošības standartus, ir nepieciešams ciešāk sadarboties starptautiskā līmenī, tostarp ir nepieciešams noteikt kopīgas uzvedības normas, pieņemt rīcības kodeksus, lietot starptautiskos standartus un veikt informācijas apmaiņu, kas veicinātu raitāku starptautisko sadarbību, reaģējot uz tīklu un informācijas drošības problēmām, un sekmētu vienotu globālu pieeju šādām problēmām. Tādēļ *ENISA* būtu jāatbalsta plašāka Savienības iesaistīšanās un sadarbība ar trešām valstīm un starptautiskām organizācijām, vajadzības gadījumā attiecīgām Savienības iestādēm, struktūrām, birojiem un aģentūrām sniedzot nepieciešamos lietpratības atzinumus un veicot analīzi.

(55) *ENISA* būtu jāspēj reaģēt uz dalībvalstu un Savienības iestāžu, struktūru, biroju un aģentūru *ad hoc* pieprasījumiem pēc padomiem un palīdzības jautājumos, kas atbilst *ENISA* pilnvarām.

(56) Ir lietderīgi un ieteicams *ENISA* pārvaldībā ieviest noteiktus principus, lai panāktu atbilstību kopīgajam paziņojumam un kopīgajai pieejai, par ko 2012. gada jūlijā vienojās starpiestāžu darba grupa ES decentralizēto aģentūru jautājumos, kuras mērķis ir racionalizēt decentralizēto aģentūru darbību un uzlabot to sniegumu. Ieteikumi, kas doti kopīgajā paziņojumā un kopīgajā pieejā, attiecīgā gadījumā būtu jāatspoguļo arī *ENISA* darba programmās, *ENISA* izvērtējumos un *ENISA* pārskatu sniegšanas un administratīvajā praksē.

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

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

(59) Lai *ENISA* darbība būtu sekmīga, tās izpilddirektors jāieceļ, ņemot vērā nopelnus un ar dokumentiem apliecinātas administratīvā un pārvaldības darba iemaņas, kā arī kompetenci un pieredzi kiberdrošības jomā. Izpilddirektora pienākumi būtu jāpilda pilnīgi neatkarīgi. Izpilddirektoram būtu jāsagatavo priekšlikums *ENISA* gada darba programmai, iepriekš apspriežoties ar Komisiju, un būtu jāveic visi vajadzīgie pasākumi, lai nodrošinātu minētās darba programmas pienācīgu īstenošanu. Izpilddirektoram būtu jāsagatavo gada darbības pārskata projekts, kas jāiesniedz Administratīvajai padomei un kurš aptver *ENISA* gada darba programmas īstenošanu, jāizstrādā *ENISA* ieņēmumu un izdevumu tāmes projekts un jāizpilda budžets. Turklāt izpilddirektoram vajadzētu būt iespējai veidot

ad hoc darba grupas, lai risinātu specifiskus jautājumus, jo īpaši zinātniskus, tehniskus, juridiskus vai sociālekonomiskus jautājumus. Jo īpaši, *ad hoc* darba grupas izveide tiek uzskatīta par nepieciešamu attiecībā uz specifiskas Eiropas kiberdrošības sertifikācijas kandidātshēmas ("kandidātshēma") sagatavošanu. Izpilddirektoram būtu jāgādā, lai *ad hoc* darba grupu locekļi tiktu izraudzīti saskaņā ar augstākajiem lietpratības standartiem, lai dalībvalstu administrāciju, Savienības iestāžu, struktūru, biroju un aģentūru un privātā sektora, tostarp nozares, lietotāju un tīklu un informācijas drošības jomas akadēmisko ekspertu vidū nodrošinātu dzimumu līdzsvaru un pienācīgu līdzsvaru atbilstoši konkrētiem risināmajiem jautājumiem.

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

(61) Lai uzturētu regulāru dialogu ar privāto sektoru, patērētāju organizācijām un citām attiecīgajām ieinteresētajām personām, *ENISA* vajadzētu izveidot *ENISA* Padomdevēju grupu, kas būtu padomdevēja struktūra. *ENISA* Padomdevēju grupai, ko pēc izpilddirektora priekšlikuma izveido Administratīvā padome, galvenokārt būtu jārisina ieinteresētajām personām svarīgi jautājumi un par tiem jāinformē *ENISA*. Ar *ENISA* Padomdevēju grupu būtu jāapspriežas, jo īpaši attiecībā uz *ENISA* gada darba programmas projektu. *ENISA* Padomdevēju grupas sastāvam un tai uzdotajiem uzdevumiem būtu jānodrošina pietiekami liela ieinteresēto personu pārstāvība *ENISA* darbā.

(62) Būtu jāizveido Ieinteresēto personu kiberdrošības sertifikācijas grupa, kas palīdzētu *ENISA* un Komisijai atvieglināt konsultācijas ar attiecīgajām ieinteresētajām personām. Ieinteresēto personu kiberdrošības sertifikācijas grupa būtu jāveido no locekļiem, kas līdzvērtīgās proporcijās pārstāv nozari, gan IKT produktu un IKT pakalpojumu pieprasījuma pusē, gan piedāvājuma pusē, jo īpaši iekļaujot MVU, digitālo pakalpojumu sniedzējus, Eiropas un starptautiskās standartizācijas organizācijas, valsts akreditācijas struktūras, datu aizsardzības pārraudzības iestādes un atbilstības novērtējuma struktūras saskaņā ar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 765/2008 ([16]), un akadēmisko aprindu pārstāvjus, kā arī patērētāju organizācijas.

(63) *ENISA* vajadzētu būt ieviestiem noteikumiem par to, kā novērst un risināt interešu konfliktus. *ENISA* būtu arī jāievēro atbilstīgi Savienības noteikumi par publisku piekļuvi dokumentiem, kā noteikts Eiropas Parlamenta un Padomes Regulā (EK) Nr. 1049/2001 ([17]). Personas datu apstrādei *ENISA* būtu jānotiek saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 ([18]). *ENISA* būtu jāievēro Savienības iestādēm, struktūrām, birojiem un aģentūrām piemērojamie noteikumi un valstu tiesību akti, kas attiecas uz rīkošanos ar informāciju, jo īpaši sensitīvu, bet neklasificētu informāciju un Eiropas Savienības klasificētu informāciju (ESKI).

(64) Lai garantētu *ENISA* pilnīgu autonomiju un neatkarību un ļautu tai veikt papildu uzdevumus, tostarp neparedzētus ārkārtas uzdevumus, būtu jāpiešķir *ENISA* pietiekams un atsevišķs budžets, kura ieņēmumus būtu galvenokārt jāveido Savienības un *ENISA* darbā iesaistīto trešo valstu iemaksām. Atbilstīgs budžets ir būtiski svarīgs, lai nodrošinātu, ka *ENISA* ir pietiekamas spējas pildīt visus tās uzdevumus, kuri kļūst arvien plašāki, un sasniegt tās mērķus. Lielākajai daļai *ENISA* darbinieku vajadzētu būt tieši iesaistītai to darbību īstenošanā, kas saistītas ar *ENISA* pilnvarām. Mītnes dalībvalstij un jebkurai citai dalībvalstij vajadzētu būt iespējai veikt brīvprātīgas iemaksas *ENISA* budžetā. Savienības budžeta procedūru būtu jāturpina piemērot attiecībā uz visām subsīdijām, ko piešķir no Savienības vispārējā budžeta. Turklāt Revīzijas palātai būtu jāveic *ENISA* finanšu pārskatu revīzija, lai nodrošinātu pārredzamību un pārskatatbildību.

(65) Kiberdrošības sertifikācija ir būtiska, lai vairotu uzticēšanos IKT produktiem, IKT pakalpojumiem un IKT procesiem un lai stiprinātu to drošību. Digitālais vienotais tirgus, un jo īpaši datu ekonomika un lietu internets, var attīstīties vienīgi tad, ja plašai sabiedrībai ir pārliecība par to, ka šādiem produktiem, pakalpojumiem un procesiem ir noteikta līmeņa kiberdrošība. Satiklotās un automatizētās automašīnas, elektroniskās medicīniskās ierīces, ražošanas automatizācijas vadības sistēmas un viedtīkli – tie ir tikai daži to nozaru piemēri, kurās jau tagad plaši izmanto sertifikāciju vai kurās to varētu izmantot tuvākajā nākotnē. Arī Direktīvas (ES) 2016/1148 reglamentētajās nozarēs kiberdrošības sertifikācijai ir izšķiroša nozīme.

([16]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp.).

([17]) 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.).

([18]) 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.).

(66) 2016. gada paziņojumā "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari" Komisija uzsvēra nepieciešamību pēc augstas kvalitātes, cenas ziņā pieejamiem un sadarbspējīgiem kiberdrošības produktiem un risinājumiem. IKT produktu, IKT pakalpojumu un IKT procesu piedāvājums vienotajā tirgū ģeogrāfiskajā ziņā joprojām ir ļoti sadrumstalots. Tas ir tādēļ, ka kiberdrošības nozare Eiropā lielā mērā ir veidojusies, pamatojoties uz valsts valdību pieprasījumu. Turklāt kiberdrošības jomā vienotajā tirgū ir arī citas nepilnības, piemēram, trūkst sadarbspējīgu risinājumu (tehniskie standarti) un sertifikācijas prakses un Savienības mēroga mehānismu. Tas Eiropas uzņēmumiem apgrūtina konkurēšanu valsts, Savienības un pasaules mērogā. Tā tiek arī samazināts privātpersonām un uzņēmumiem pieejamo derīgo un izmantojamo kiberdrošības tehnoloģiju klāsts. Līdzīgi, 2017. gada Paziņojumā par digitālā vienotā tirgus stratēģijas īstenošanas viduposma pārskatā "Satīklots digitālais vienotais tirgus visiem" Komisija ir uzsvērusi vajadzību pēc drošiem satīklotiem produktiem un sistēmām un norādījusi, ka tāda Eiropas IKT drošības satvara izveide, kas paredz noteikumus par IKT drošības sertifikācijas organizēšanu Savienībā, varētu gan saglabāt uzticēšanos internetam, gan atrisināt pašreizējo iekšējā tirgus sadrumstalotības problēmu.

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

(68) Ir bijuši zināmi centieni Savienībā nodrošināt sertifikātu savstarpēju atzīšanu. Tomēr tie bijuši tikai daļēji sekmīgi. Vissvarīgākais piemērs šajā ziņā ir Augstāko amatpersonu grupa informācijas sistēmu drošības (*SOG-IS*) savstarpējās atzīšanas nolīguma (SAN) jautājumos. *SOG-IS* ir visnozīmīgākais sadarbības un savstarpējās atzīšanas modelis drošības sertifikācijas jomā, tomēr tajā ir iekļauta tikai daļa Savienības dalībvalstu. Ņemot vērā iekšējā tirgus aspektu, minētais fakts ir ierobežojis *SOG-IS* SAN efektivitāti.

(69) Tāpēc ir jāpieņem kopēja pieeja un jāizveido Eiropas kiberdrošības sertifikācijas satvars, kas nosaka galvenās horizontālās prasības izstrādājamajām Eiropas kiberdrošības sertifikācijas shēmām un atļauj IKT produktu, IKT pakalpojumu vai IKT procesu Eiropas kiberdrošības sertifikātu un ES atbilstības apliecinājumu atzīšanu un izmantošanu visās dalībvalstīs. Šādi rīkojoties, ir ļoti svarīgi pamatoties uz pašreizējām valstu un starptautiskajām shēmām, kā arī uz savstarpējās atzīšanas sistēmām, jo īpaši *SOG-IS*, un nodrošināt vienmērīgu pāreju no pašreizējām šādu sistēmu shēmām uz jaunā Eiropas kiberdrošības sertifikācijas satvara shēmām. Eiropas kiberdrošības sertifikācijas satvars būtu jāveido atbilstīgi divējādam mērķim. Pirmkārt, tam būtu jāsekmē lielāka uzticēšanās atbilstīgi Eiropas kiberdrošības sertifikācijas shēmām sertificētiem IKT produktiem, IKT pakalpojumiem un IKT procesiem. Otrkārt, tam būtu jāpalīdz izvairīties no valsts kiberdrošības sertifikācijas shēmu aizvien izplatītākā pretrunīguma vai pārklāšanās un tādējādi samazināt to uzņēmumu izmaksas, kuri darbojas digitālajā vienotajā tirgū. Eiropas kiberdrošības sertifikācijas shēmām vajadzētu būt nediskriminējošām un balstītām uz Eiropas vai starptautiskiem standartiem, taču tas neattiektos uz standartiem, kas ir neefektīvi vai nepietiekami atbilstoši, lai īstenotu Savienības leģitīmos mērķus šajā jomā.

(70) Eiropas kiberdrošības sertifikācijas satvars būtu saskaņoti jāizveido visās dalībvalstīs, lai novērstu izdevīgākās sertifikācijas izvēlēšanās praksi, ko izraisa prasību stingrības līmeņa atšķirības dažādās dalībvalstīs.

(71) Eiropas kiberdrošības sertifikācijas shēmas pamatā vajadzētu būt iestrādēm, kas jau pastāv valstu un starptautiskā līmenī, un vajadzības gadījumā forumu un konsorciju tehniskām specifikācijām, ņemot vērā pašreizējās stiprās puses un izvērtējot un novēršot vājās vietas.

(72) Ir nepieciešami elastīgi kiberdrošības risinājumi, lai nozare būtu sagatavota kiberdraudiem, tāpēc ikviena sertifikācijas shēma būtu jāizstrādā tā, lai novērstu risku, ka tā ātri zaudētu aktualitāti.

(73) Komisijai vajadzētu būt pilnvarotai pieņemt Eiropas kiberdrošības sertifikācijas shēmas attiecībā uz konkrētām IKT produktu, IKT pakalpojumu un IKT procesu grupām. Minētās shēmas būtu jāīsteno un jāpārrauga valstu kiberdrošības sertifikācijas iestādēm, un saskaņā ar minētajām shēmām izsniegtajiem sertifikātiem vajadzētu būt derīgiem un atzītiem visā Savienībā. Nozarē vai citās privātās organizācijās izmantotajām sertifikācijas shēmām nebūtu jāietilpst šīs regulas darbības jomā. Tomēr struktūrām, kas izmanto šādas shēmas, vajadzētu būt iespējai ierosināt, lai Komisija apsvērtu iespēju tās izmantot par pamatu, lai tās apstiprinātu kā Eiropas kiberdrošības sertifikācijas shēmu.

(74) Šīs regulas noteikumiem nebūtu jāskar Savienības tiesību akti, kuros izklāstīti īpaši noteikumi par IKT produktu, IKT pakalpojumu un IKT procesu sertifikāciju. Jo īpaši, Regulā (ES) 2016/679 ir izklāstīti noteikumi par sertifikācijas mehānismu ieviešanu un datu aizsardzības zīmogiem un marķējumu, kam uzskatāmi jāparāda datu pārziņu un apstrādātāju veikto apstrādes darbību atbilstība minētajai regulai. Ar šādiem sertifikācijas mehānismiem un datu aizsardzības zīmogiem un marķējumiem vajadzētu būt nodrošinātai iespējai datu subjektam ātri novērtēt attiecīgo IKT produktu, IKT pakalpojumu un IKT procesu datu aizsardzības līmeni. Šī regula neskar datu apstrādes darbību sertifikāciju saskaņā ar Regulu (ES) 2016/679, arī tad, kad šādas darbības ir iestrādātas IKT produktos, IKT pakalpojumos un IKT procesos.

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

(76) Tehniskās specifikācijas, kas jāizmanto Eiropas kiberdrošības sertifikācijas shēmās, būtu jāatbilst Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012 ([19]) II pielikumā izklāstītajām prasībām. Tomēr dažas novirzes no minētajām prasībām varētu uzskatīt par nepieciešamām pienācīgi pamatotos gadījumos, ja minētās tehniskās specifikācijas paredzēts izmantot Eiropas kiberdrošības sertifikācijas shēmā, kurā ir norāde uz apliecinājuma līmeni "augsts". Iemesli šādām novirzēm būtu jādara publiski pieejami.

(77) Atbilstības novērtējums ir procedūra, lai novērtētu, vai noteiktās prasības attiecībā uz IKT produktu, IKT pakalpojumu vai IKT procesu ir izpildītas. Minēto procedūru veic neatkarīga trešā persona, kas nav to IKT produktu, IKT pakalpojumu vai IKT procesu ražotājs vai sniedzējs, kurus novērtē. Eiropas kiberdrošības sertifikāts būtu jāizdod pēc veiksmīgas IKT produkta, IKT pakalpojuma vai IKT procesa izvērtēšanas. Eiropas kiberdrošības sertifikāts būtu uzskatāms par apstiprinājumu, ka izvērtējums ir veikts pienācīgi. Atkarībā no apliecinājuma līmeņa Eiropas kiberdrošības sertifikācijas shēmai būtu jānorāda, vai Eiropas kiberdrošības sertifikātu izdod privāta vai publiska struktūra. Atbilstības novērtējums vai sertifikācija paši par sevi nevar garantēt, ka sertificēti IKT produkti, IKT pakalpojumi un IKT procesi ir kiberdroši. Tās drīzāk ir procedūras un tehniskās metodikas, lai apliecinātu, ka IKT produkti, IKT pakalpojumi un IKT procesi ir testēti un ka tie atbilst konkrētām kiberdrošības prasībām, kuras noteiktas citur, piemēram, tehniskajos standartos.

(78) Eiropas kiberdrošības sertifikātu lietotāju izvēlei attiecībā uz piemērotu sertifikāciju un ar to saistītajām drošības prasībām būtu jāpamatojas uz analīzi par riskiem saistībā ar attiecīgā IKT produkta, IKT pakalpojuma vai IKT procesa lietojumu. Attiecīgi apliecinājuma līmenim tātad būtu jāatbilst riska līmenim, kas saistīts ar IKT produkta, IKT pakalpojuma vai IKT procesa paredzamo lietojumu.

([19]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1025/2012 (2012. gada 25. oktobris) par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp.).

(79) Eiropas kiberdrošības sertifikācijas shēmās varētu paredzēt atbilstības novērtējumu, kura veikšana ir tikai IKT produktu, IKT pakalpojumu vai IKT procesu ražotāja vai sniedzēja atbildībā ("atbilstības pašnovērtējums"). Šādos gadījumos vajadzētu būt pietiekami, ja IKT produktu, IKT pakalpojumu vai IKT procesu ražotājs vai sniedzējs pats veic visas pārbaudes, lai nodrošinātu, ka IKT produkts, IKT pakalpojums vai IKT process atbilst Eiropas kiberdrošības sertifikācijas shēmai. Atbilstības pašnovērtējums būtu uzskatāms par piemērotu IKT produktiem, IKT pakalpojumiem vai IKT procesiem ar zemu sarežģītības pakāpi, kas rada zemu risku sabiedrības interesēm, piemēram, vienkārša konstrukcija un ražošanas mehānismi. Turklāt atbilstības pašnovērtējumu IKT produktiem, IKT pakalpojumiem vai IKT procesiem būtu jāļauj veikt tikai tad, ja tie atbilst apliecinājuma līmenim "pamata".

(80) Eiropas kiberdrošības sertifikācijas shēmās varētu paredzēt gan IKT produktu, IKT pakalpojumu vai IKT procesu atbilstības pašnovērtējumu, gan to sertifikāciju. Šādā gadījumā shēmā būtu jāparedz skaidri un saprotami līdzekļi, ar kuriem patērētāji vai citi lietotāji varētu atšķirt IKT produktus, IKT pakalpojumus vai IKT procesus, par kuru novērtējumu atbild IKT produktu, IKT pakalpojumu vai IKT procesu ražotājs vai sniedzējs, un IKT produktus, IKT pakalpojumus vai IKT procesus, kurus sertificējusi trešā persona.

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

(82) IKT produktu, IKT pakalpojumu vai IKT procesu ražotājiem vai sniedzējiem ES atbilstības apliecinājums, tehniskā dokumentācija un visa cita attiecīgā informācija, kas saistīta ar IKT produktu, IKT pakalpojumu vai IKT procesu atbilstību Eiropas kiberdrošības sertifikācijas shēmai, būtu jādara pieejama kompetentajai valsts kiberdrošības sertifikācijas iestādei uz laiku, kas paredzēts attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā. Tehniskajā dokumentācijā būtu jānorāda saskaņā ar shēmu piemērojamās prasības un, ciktāl tas ir nepieciešams atbilstības pašnovērtēšanai, būtu jāaptver IKT produkta, IKT pakalpojuma vai IKT procesa projektēšana, ražošana un ekspluatācija. Tehniskā dokumentācija būtu jāapkopo tā, lai būtu iespējams novērtēt, vai IKT produkts vai IKT pakalpojums atbilst prasībām, kas piemērojamas saskaņā ar minēto shēmu.

(83) Eiropas kiberdrošības sertifikācijas satvara pārvaldībā ņem vērā dalībvalstu iesaisti, kā arī ieinteresēto personu pienācīgu iesaisti un nosaka Komisijas lomu Eiropas kiberdrošības sertifikācijas shēmu plānošanas un ierosināšanas, pieprasīšanas, sagatavošanas, pieņemšanas un pārskatīšanas procesā.

(84) Komisijai – ar Eiropas Kiberdrošības sertifikācijas grupas (*ECCG*) un Ieinteresēto personu kiberdrošības sertifikācijas grupas atbalstu un pēc atklātas un plašas apspriešanās – būtu jāsagatavo Savienības mainīgā darba programma Eiropas kiberdrošības sertificēšanai, kura būtu jāpublicē kā nesaistošs instruments. Savienības mainīgajai darba programmai vajadzētu būt stratēģiskam dokumentam, kas nozarei, valsts iestādēm un standartizācijas struktūrām ļauj jo īpaši iepriekš sagatavoties nākotnē gaidāmajām Eiropas kiberdrošības sertifikācijas shēmām. Savienības mainīgajā darba programmā vajadzētu būt iekļautam daudzgadu pārskatam par kandidātshēmu pieprasījumiem, ko Komisija plāno iesniegt *ENISA*, balstoties uz konkrētiem iemesliem. Komisijai būtu jāņem vērā Savienības mainīgā darba programma, sagatavojot savu IKT standartizācijas mainīgo plānu un standartizācijas pieprasījumus Eiropas Standartizācijas organizācijām. Ņemot vērā to, ka strauji tiek ieviestas jaunas tehnoloģijas un ka tās sāk izmantot, un to, ka parādās iepriekš nezināmi kiberdrošības riski un notiek leģislatīvas izmaiņas un izmaiņas tirgū, Komisijai vai *ECCG* vajadzētu būt tiesībām pieprasīt *ENISA* sagatavot kandidātshēmas, kuras nebija iekļautas Savienības mainīgajā darba programmā. Šādos gadījumos Komisijai un *ECCG* būtu arī jāizvērtē šāda pieprasījuma nepieciešamība, ņemot vērā šīs regulas vispārējos mērķus un uzdevumus un vajadzību nodrošināt *ENISA* plānošanas un resursu izmantojuma nepārtrauktību.

Pēc šāda pieprasījuma saņemšanas *ENISA* bez liekas kavēšanās būtu jāsagatavo kandidātshēmas konkrētiem IKT produktiem, IKT pakalpojumiem vai IKT procesiem. Komisijai būtu jānovērtē sava pieprasījuma pozitīvā un negatīvā ietekme uz konkrēto tirgu, jo īpaši tā ietekme uz MVU, inovāciju, šķēršļiem ienākšanai minētajā tirgū un izmaksām galalietotājiem. Pamatojoties uz *ENISA* sagatavoto kandidātshēmu, Komisijai vajadzētu būt pilnvarotai ar īstenošanas aktiem pieņemt Eiropas kiberdrošības sertifikācijas shēmu. Ņemot vērā šajā regulā noteikto vispārējo mērķi un drošības mērķus, Komisijas pieņemtās Eiropas kiberdrošības sertifikācijas shēmās būtu jānosaka minimālais elementu kopums, kas izmantojams attiecībā uz katras shēmu priekšmetu, tvērumu un darbību. Cita starpā minētajiem elementiem būtu jāietver kiberdrošības sertifikācijas tvērums un priekšmets, tostarp IKT produktu, IKT pakalpojumu un IKT procesu kategorijas, detalizēti noteiktas kiberdrošības prasības, piemēram, atsaucoties uz standartiem vai tehniskajām specifikācijām, specifiskie izvērtēšanas kritēriji un metodes, kā arī plānotais apliecinājuma līmenis ("pamata", "būtisks" vai "augsts") un attiecīgā gadījumā – izvērtējuma līmeņi. *ENISA* vajadzētu būt iespējai noraidīt *ECCG* pieprasījumu. Šādus lēmumus būtu jāpieņem Administratīvajai padomei, un tiem vajadzētu būt pienācīgi pamatotiem.

(85) *ENISA* būtu jāuztur tīmekļa vietne, kurā sniedz informāciju un publicitāti par Eiropas kiberdrošības sertifikācijas shēmām un kurā cita starpā būtu jāiekļauj pieprasījumi par kandidātshēmas sagatavošanu, kā arī atsauksmes, kas saņemtas *ENISA* veiktajā apspriešanās procesā sagatavošanās posmā. Tīmekļa vietnē būtu jāsniedz arī informācija par Eiropas kiberdrošības sertifikātiem un ES atbilstības apliecinājumiem, kas izdoti saskaņā ar šo regulu, tostarp par šādu Eiropas kiberdrošības sertifikātu un ES atbilstības apliecinājumu atsaukšanu un termiņa beigām. Tīmekļa vietnē būtu arī jānorāda tās valsts kiberdrošības sertifikācijas shēmas, kuras ir aizstātas ar Eiropas kiberdrošības sertifikācijas shēmu.

(86) Eiropas sertifikācijas shēmas apliecinājuma līmenis ir pamats pārliecībai, ka IKT produkts, IKT pakalpojums vai IKT process atbilst konkrētas Eiropas kiberdrošības sertifikācijas shēmas drošības prasībām. Lai nodrošinātu Eiropas kiberdrošības sertifikācijas satvara konsekvenci, Eiropas kiberdrošības sertifikācijas shēmā būtu jāvar noteikt apliecinājuma līmeņus Eiropas kiberdrošības sertifikātiem un ES atbilstības apliecinājumiem, ko izdod saskaņā ar minēto shēmu. Katrā Eiropas kiberdrošības sertifikātā varētu norādīt vienu no apliecinājuma līmeņiem, proti, "pamata", "būtisks" vai "augsts", savukārt ES atbilstības apliecinājumā varētu norādīt tikai apliecinājuma līmeni "pamata". Apliecinājuma līmeņi paredzētu atbilstošas stingrības un dziļuma IKT produkta, IKT pakalpojuma un IKT procesa izvērtēšanu, un tos raksturotu atsauce uz to saistītām tehniskajām specifikācijām, standartiem un procedūrām, tostarp tehniskām kontrolēm, kuru mērķis ir mazināt vai novērst incidentus. Katram apliecinājuma līmenim vajadzētu būt konsekventam dažādās nozaru jomās, kur sertifikācija tiek piemērota.

(87) Eiropas kiberdrošības sertifikācijas shēmā varētu noteikt vairākus izvērtējuma līmeņus atkarībā no izmantotās izvērtēšanas metodikas stingrības un dziļuma. Izvērtējuma līmeņiem būtu jāatbilst vienam no apliecinājuma līmeņiem un vajadzētu būt saistītam ar apliecinājuma komponentu piemērotu kombināciju. Visos apliecinājuma līmeņos IKT produktam, IKT pakalpojumam vai IKT procesam būtu jāietver virkne drošu funkciju, kā precizēts shēmā, un tās cita starpā var būt: droša iepriekš iestatīta konfigurācija, parakstīts kods, drošas atjauninašanas un ļaunprātīgas izmantošanas mazināšanas iespējas un pilnvērtīga steka vai kaudzes atmiņas aizsardzība. Minētām funkcijām vajadzētu būt izstrādātām un tās būtu jāuztur, izmantojot uz drošību orientētas izstrādes pieejas un ar tām saistītus rīkus, lai nodrošinātu, ka uzticami ir iestrādāti efektīvi programmatūras un aparatūras mehānismi.

(88) Attiecībā uz apliecinājuma līmeni "pamata" izvērtējumā būtu jāvadās pēc vismaz šādiem apliecinājuma komponentiem: izvērtējumā būtu jāietver vismaz IKT produkta, IKT pakalpojuma vai IKT procesa tehniskās dokumentācijas pārskats, ko veic atbilstības novērtēšanas struktūra. Ja sertifikācija aptver IKT procesus, tehniskajā pārskatīšanā būtu jāizvērtē arī process, kas izmantots IKT produkta vai IKT pakalpojuma projektēšanā, izstrādē un uzturēšanā. Ja Eiropas kiberdrošības sertifikācijas shēmā paredzēts atbilstības pašnovērtējums, vajadzētu pietikt ar to, ka IKT produktu, IKT pakalpojumu vai IKT procesu ražotājs vai sniedzējs ir veicis pašnovērtējumu par IKT produkta, IKT pakalpojuma vai IKT procesa atbilstību sertifikācijas shēmai.

(89) Attiecībā uz apliecinājuma līmeni "būtisks" izvērtējumā papildus prasībām apliecinājuma līmenim "pamata" būtu jāorientējas uz to, lai tiktu pārbaudīta vismaz IKT produkta, IKT pakalpojuma vai IKT procesa drošības funkciju atbilstība tā tehniskajai dokumentācijai.

(90) Attiecībā uz apliecinājuma līmeni "augsts" izvērtējumā papildus prasībām apliecinājuma līmenim "būtisks" būtu jāorientējas uz to, lai tiktu veikta vismaz efektivitātes testēšana, kurā novērtē IKT produkta, IKT pakalpojums vai IKT procesa drošības funkciju noturību pret sarežģītiem kiberuzbrukumiem, ko veic personas ar nozīmīgām prasmēm un resursiem.

(91) Eiropas kiberdrošības sertifikācijas un ES atbilstības apliecinājumu izmantošanai būtu jāpaliek fakultatīvai, ja vien Savienības tiesību aktos vai dalībvalstu tiesību aktos, kas pieņemti saskaņā ar Savienības tiesību aktiem, nav noteikts citādi. Ja saskaņotu Savienības tiesību aktu nav, dalībvalstis var pieņemt valsts tehniskos noteikumus atbilstīgi Eiropas Parlamenta un Padomes Direktīvai (ES) 2015/1535 ([20]), kurā paredzēta obligāta sertifikācija saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu. Dalībvalstis var izmantot arī Eiropas kiberdrošības sertifikāciju saistībā ar publisko iepirkumu un Eiropas Parlamenta un Padomes Direktīvu 2014/24/ES ([21]).

(92) Dažās jomās varētu būt nepieciešams turpmāk noteikt īpašas kiberdrošības prasības un paredzēt obligātu sertifikāciju attiecībā uz konkrētiem IKT produktiem, IKT pakalpojumiem vai IKT procesiem nolūkā uzlabot kiberdrošības līmeni Savienībā. Komisijai būtu regulāri jāpārrauga, kā pieņemtās Eiropas kiberdrošības sertifikācijas shēmas ietekmē drošu IKT produktu, IKT pakalpojumu vai IKT procesu pieejamību iekšējā tirgū, un būtu regulāri jānovērtē, cik plaši IKT produktu, IKT pakalpojumu vai IKT procesu ražotāji vai sniedzēji Savienībā izmanto sertifikācijas shēmas. Eiropas kiberdrošības sertifikācijas shēmu efektivitāte un tas, vai konkrētas shēmas būtu jāpadara par obligātām, būtu jāvērtē, ņemot vērā Savienības tiesību aktus kiberdrošības jomā, jo īpaši Direktīvu (ES) 2016/1148, un pamatpakalpojumu sniedzēju izmantoto tīklu un informācijas sistēmu drošību.

(93) Eiropas kiberdrošības sertifikātiem un ES atbilstības apliecinājumiem būtu jāpalīdz galalietotājiem izdarīt uz informāciju pamatotu izvēli. Tāpēc IKT produktiem, IKT pakalpojumiem un IKT procesiem, kuri ir sertificēti vai par kuriem ir izdots ES atbilstības apliecinājums, vajadzētu būt pievienotai strukturētai informācijai, kas pielāgota paredzētā galalietotāja sagaidāmajam tehniskās izpratnes līmenim. Visai šādai informācijai vajadzētu būt pieejamai tiešsaistē, un attiecīgā gadījumā – fiziskā veidā. Galalietotājam vajadzētu būt pieejamai informācijai par sertifikācijas shēmas atsauces numuru, apliecinājuma līmeni, aprakstu par kiberdrošības riskiem saistībā ar IKT produktu, IKT pakalpojumu vai IKT procesu un izdevēju iestādi vai struktūru, vai vajadzētu būt iespējai saņemt Eiropas kiberdrošības sertifikāta kopiju. Turklāt galalietotājam vajadzētu būt informētam par IKT produktu, IKT pakalpojumu vai IKT procesu ražotāja vai sniedzēja kiberdrošības atbalsta politiku, proti, cik ilgi galalietotājs varētu saņemt ar kiberdrošību saistītus atjauninājumus vai labojumus. Attiecīgā gadījumā būtu jāsniedz norādījumi par darbībām vai iestatījumiem, ko galalietotājs var veikt, lai saglabātu vai palielinātu IKT produkta vai IKT pakalpojuma kiberdrošību, un vienota kontaktpunkta kontaktinformāciju, kuram ziņot par kiberuzbrukumiem un no kura saņemt atbalstu kiberuzbrukumu gadījumā (papildus automātiskajai ziņošanai). Minētajai informācijai vajadzētu būt regulāri atjauninātai un darītai pieejamai tīmekļa vietnē, kur sniedz informāciju par Eiropas kiberdrošības sertifikācijas shēmām.

(94) Lai sasniegtu šīs regulas mērķus un izvairītos no iekšējā tirgus sadrumstalotības, valsts kiberdrošības sertifikācijas shēmām vai procedūrām, kas piemērojamas kādā Eiropas kiberdrošības sertifikācijas shēmā ietvertajiem IKT produktiem, IKT pakalpojumiem vai IKT procesiem, no Komisijas īstenošanas aktos noteiktas dienas vairs nevajadzētu būt spēkā. Turklāt dalībvalstīm vairs nebūtu jāievieš jaunas valsts kiberdrošības sertifikācijas shēmas IKT produktiem, IKT pakalpojumiem vai IKT procesiem, uz kuriem jau attiecas spēkā esoša Eiropas kiberdrošības sertifikācijas shēma. Tomēr dalībvalstīm nevajadzētu aizliegt pieņemt vai saglabāt valsts kiberdrošības sertifikācijas shēmas nacionālās drošības vajadzībām. Dalībvalstīm būtu Komisija un *ECCG* jāinformē par jebkuru savu nolūku izstrādāt jaunas valsts kiberdrošības sertifikācijas shēmas. Komisijai un *ECCG* būtu jāizvērtē jauno valsts kiberdrošības sertifikācijas shēmu ietekme uz iekšējā tirgus pienācīgu darbību un, ņemot vērā stratēģiskās intereses, jāapsver iespēja tās vietā pieprasīt Eiropas kiberdrošības sertifikācijas shēmu.

(95) Eiropas kiberdrošības sertifikācijas shēmu mērķis ir palīdzēt saskaņot kiberdrošības praksi Savienībā. Tām jādod ieguldījums kiberdrošības līmeņa paaugstināšanā Savienībā. Eiropas kiberdrošības sertifikācijas shēmu izstrādē būtu jāņem vērā arī inovācijas kiberdrošības jomā un jādod iespēja attīstīt tās.

([20]) Eiropas Parlamenta un Padomes Direktīva (ES) 2015/1535 (2015. gada 9. septembris), ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā (OV L 241, 17.9.2015., 1. lpp.).

([21]) Eiropas Parlamenta un Padomes Direktīva 2014/24/ES (2014. gada 26. februāris) par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65. lpp.).

(96) Eiropas kiberdrošības sertifikācijas shēmās būtu jāņem vērā pašreizējās programmatūras un aparatūras izstrādes metodes un jo īpaši – biežu programmatūras un aparātprogrammatūras atjauninājumu ietekme uz atsevišķiem Eiropas kiberdrošības sertifikātiem. Eiropas kiberdrošības sertifikācijas shēmās būtu jāparedz nosacījumi, saskaņā ar kuriem atjauninājuma rezultātā var būt nepieciešama IKT produkta, IKT pakalpojuma vai IKT procesa atkārtota sertifikācija vai konkrēta Eiropas kiberdrošības sertifikāta tvēruma samazināšana, ņemot vērā atjauninājuma iespējamu nelabvēlīgu ietekmi uz atbilstību minētā sertifikāta drošības prasībām.

(97) Pēc Eiropas kiberdrošības sertifikācijas shēmas pieņemšanas IKT produktu, IKT pakalpojumu vai IKT procesu ražotājiem vai sniedzējiem vajadzētu būt iespējai savus IKT produktu vai IKT pakalpojumu sertifikācijas pieteikumus iesniegt pašu izvēlētai atbilstības novērtēšanas struktūrai jebkur Savienībā. Atbilstības novērtēšanas struktūras būtu jāakreditē valsts akreditācijas struktūrai, ja tās atbilst dažām konkrētām šajā regulā izklāstītām prasībām. Akreditācija būtu jāpiešķir uz laikposmu, kas nav ilgāks par pieciem gadiem, un to būtu jāatjauno ar tādiem pašiem nosacījumiem, ja atbilstības novērtēšanas struktūra joprojām ievēro prasības. Valstu akreditācijas struktūrām atbilstības novērtēšanas struktūras akreditācija būtu jāierobežo, jāaptur vai jāatsauc, ja akreditācijas nosacījumi nav vai vairs netiek izpildīti vai ja atbilstības novērtēšanas struktūra pārkāpj šo regulu.

(98) Valstu tiesību aktos iekļautās atsauces uz valsts standartiem, kas vairs nav spēkā sakarā ar Eiropas kiberdrošības sertifikācijas shēmas stāšanos spēkā, var radīt neskaidrību. Tāpēc dalībvalstīm būtu jāapsver Eiropas kiberdrošības sertifikācijas shēmas pieņemšana savos tiesību aktos.

(99) Lai visā Savienībā panāktu līdzvērtīgus standartus, veicinātu savstarpēju atzīšanu un sekmētu Eiropas kiberdrošības sertifikātu un ES atbilstības apliecinājumu vispārējo atzīšanu, ir jāievieš salīdzinošas izvērtēšanas sistēma starp valstu kiberdrošības sertifikācijas iestādēm. Salīdzinošajā izvērtēšanā būtu jāietilpst procedūrām attiecībā uz IKT produktu, IKT pakalpojumu vai IKT procesu ar Eiropas kiberdrošības sertifikātiem atbilstības uzraudzīšanu, uz IKT produktu, IKT pakalpojumu vai IKT procesu ražotāju vai sniedzēju pienākumu pārraudzīšanu, kuri veic atbilstības pašnovērtējumu, uz atbilstības novērtēšanas struktūru pārraudzīšanu, kā arī uz to struktūru darbinieku lietpratības piemērotību, kuras izdod sertifikātus par apliecinājuma līmeni "augsts". Komisijai ar īstenošanas aktu vajadzētu būt iespējai izstrādāt vismaz piecu gadu plānu salīdzinošajai izvērtēšanai, kā arī noteikt salīdzinošās izvērtēšanas sistēmas darbības kritērijus un metodes.

(100) Neskarot vispārējo salīdzinošās izvērtēšanas sistēmu, ko paredzēts ieviest visās valsts kiberdrošības sertifikācijas iestādēs Eiropas kiberdrošības sertifikācijas satvarā, konkrētās Eiropas kiberdrošības sertifikācijas shēmās var būt iekļauts salīdzinošās izvērtēšanas mehānisms struktūrām, kuras IKT produktiem, IKT pakalpojumiem un IKT procesiem izdod Eiropas kiberdrošības sertifikātus par apliecinājuma līmeni "augsts" saskaņā ar šādām shēmām. *ECCG* būtu jāatbalsta šādu salīdzinošās izvērtēšanas mehānismu īstenošana. Salīdzinošajā izvērtēšanā jo īpaši būtu jāizvērtē, vai attiecīgās struktūras savus uzdevumus veic saskaņoti, un tā varētu ietvert pārsūdzības mehānismus. Salīdzinošās izvērtēšanas rezultāti būtu jādara publiski pieejami. Attiecīgās struktūras var pieņemt piemērotus pasākumus, lai attiecīgi pielāgotu savu praksi un lietpratību.

(101) Dalībvalstīm būtu jāizraugās viena vai vairākas valsts kiberdrošības sertifikācijas iestādes, lai uzraudzītu atbilstību no šīs regulas izrietošajiem pienākumiem. Valsts kiberdrošības sertifikācijas iestāde var būt pastāvoša vai jauna iestāde. Dalībvalstij arī vajadzētu būt iespējai, vienojoties ar citu dalībvalsti, izraudzīties vienu vai vairākas valsts kiberdrošības sertifikācijas iestādes minētās citas dalībvalsts teritorijā.

(102) Valstu kiberdrošības sertifikācijas iestādēm jo īpaši būtu jāpārrauga IKT produktu, IKT pakalpojumu vai IKT procesu ražotāju vai sniedzēju, kas veic uzņēmējdarbību iestādes attiecīgajā teritorijā, pienākumi, kas saistīti ar ES atbilstības apliecinājumu, un jānodrošina šo pienākumu izpilde, būtu jāpalīdz valsts akreditācijas struktūrām atbilstības novērtēšanas struktūru darbību pārraudzīšanā un uzraudzīšanā, nodrošinot tām lietpratību un attiecīgu informāciju, būtu jāpilnvaro atbilstības novērtēšanas struktūras veikt to uzdevumus, ja tās ir izpildījušas Eiropas kiberdrošības sertifikācijas shēmā izklāstītās papildu prasības, un būtu jāpārrauga nozīmīgas norises kiberdrošības sertifikācijas jomā. Valstu kiberdrošības sertifikācijas iestādēm būtu arī jāizskata sūdzības, ko fiziskas vai juridiskas personas iesniegušas saistībā ar minēto iestāžu izdotiem Eiropas kiberdrošības sertifikācijas sertifikātiem vai atbilstības novērtēšanas struktūru izdotiem Eiropas kiberdrošības sertifikātiem, ja tajos norādītais apliecinājuma līmenis ir "augsts", pienācīgā mērā būtu jāizmeklē sūdzības priekšmeti un samērīgā laikposmā jāinformē sūdzības

iesniedzējs par lietas virzību un izskatīšanas rezultātiem. Turklāt valstu kiberdrošības sertifikācijas iestādēm būtu jāsadarbojas ar citām valsts kiberdrošības sertifikācijas iestādēm vai citām publiskām iestādēm, tostarp, apmainoties ar informāciju par IKT produktu, IKT pakalpojumu vai IKT procesu iespējamu neatbilstību šīs regulas prasībām vai konkrētām Eiropas kiberdrošības sertifikācijas shēmām. Komisijai būtu jāveicina minētā informācijas apmaiņa, darot pieejamu vispārēju elektronisku informācijas atbalsta sistēmu, piemēram, tirgus uzraudzības informācijas un saziņas sistēmu (*ICSMS*) un ātrās brīdināšanas sistēmu bīstamu nepārtikas preču jomā (*RAPEX*), ko tirgus uzraudzības iestādes jau izmanto, ievērojot Regulu (EK) Nr. 765/2008.

(103) Lai nodrošinātu Eiropas kiberdrošības sertifikācijas satvara konsekventu piemērošanu, būtu jāizveido *ECCG*, kas sastāv no valstu kiberdrošības sertifikācijas iestāžu vai citu attiecīgu valstu iestāžu pārstāvjiem. *ECCG* galvenais uzdevums būtu dot padomus un palīdzēt Komisijai tās darbā, lai nodrošinātu Eiropas kiberdrošības sertifikācijas satvara konsekventu īstenošanu un piemērošanu, palīdzēt *ENISA* un ar to cieši sadarboties kiberdrošības sertifikācijas kandidātshēmu izveidē, pienācīgi pamatotos gadījumos lūgt *ENISA* izveidot kandidātshēmu, pieņemt *ENISA* adresētus atzinumus par kandidātshēmām un Komisijai adresētus atzinumus par esošo Eiropas kiberdrošības sertifikācijas shēmu uzturēšanu un pārskatīšanu. *ECCG* būtu jāveicina labas prakses un lietpratības apmaiņa starp dažādām valstu kiberdrošības sertifikācijas iestādēm, kas atbild par atļauju izsniegšanu atbilstības novērtēšanas struktūrām un par Eiropas kiberdrošības sertifikātu izdošanu.

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

(105) Lai vēl vairāk veicinātu tirdzniecību un, atzīstot, ka IKT piegādes ķēdes ir globālas, Savienība saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 218. pantu var slēgt savstarpējās atzīšanas nolīgumus par Eiropas kiberdrošības sertifikātiem. Komisija, ņemot vērā *ENISA* un *ECCG* padomus, var ieteikt attiecīgu sarunu sākšanu. Katrā Eiropas kiberdrošības sertifikācijas shēmā būtu jāparedz konkrēti nosacījumi attiecībā uz šādiem savstarpējās atzīšanas nolīgumiem ar trešām valstīm.

(106) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir Komisijai īstenošanas pilnvaras gadījumiem. Minētās pilnvaras būtu jāīsteno saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 ([22]).

(107) Pārbaudes procedūra būtu jāizmanto, lai pieņemtu īstenošanas aktus par Eiropas kiberdrošības sertifikācijas shēmām, kas izmantojamas attiecībā uz IKT produktiem, IKT pakalpojumiem vai IKT procesiem; par kārtību, kādā *ENISA* veic izmeklēšanu; par valsts kiberdrošības sertifikācijas iestāžu salīdzinošās izvērtēšanas plānu, kā arī par tādu atbilstības novērtēšanas struktūru paziņojumu sniegšanas apstākļiem, veidu un kārtību, kurus Komisijai sniedz valsts kiberdrošības sertifikācijas iestādes.

(108) *ENISA* darbība būtu jānovērtē regulāri un neatkarīgi. Minētajā novērtējumā būtu jāņem vērā *ENISA* mērķi, tās darba prakse un uzdevumu, jo īpaši to uzdevumu, kas saistīti ar operatīvo sadarbību Savienības līmenī, būtiskums. Minētajā novērtējumā būtu arī jānovērtē Eiropas kiberdrošības sertifikācijas satvara ietekme, lietderība un efektivitāte. Pārskatīšanas gadījumā Komisijai būtu jānovērtē, kā var stiprināt *ENISA* kā padomu un lietpratības uzziņas punkta lomu, kā arī novērtēt iespējamu *ENISA* lomu attiecībā uz atbalstu tādu trešo valstu IKT produktu, IKT pakalpojumu un IKT procesu izvērtēšanai, kuri neatbilst Savienības noteikumiem, ja šādi produkti, pakalpojumi vai procesi ienāk Savienībā.

([22]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

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

(110) Regula (ES) Nr. 526/2013 būtu jāatceļ,

IR PIEŅĒMUŠI ŠO REGULU.

I SADAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets un darbības joma

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

a) *ENISA* (Eiropas Savienības Kiberdrošības aģentūras) mērķi, uzdevumi un organizatoriskie aspekti; un

b) satvars, kurā jāizveido Eiropas kiberdrošības sertifikācijas shēmas, lai Savienībā 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.

Pirmās daļas b) apakšpunktā minēto satvaru piemēro, neskarot citu Savienības tiesību aktu īpašos noteikumus par brīvprātīgu vai obligātu sertifikāciju.

2. Šī regula neskar dalībvalstu kompetenci attiecībā uz darbībām, kas saistītas ar sabiedrisko drošību, aizsardzību, valsts drošību, un valsts pasākumus krimināltiesību jomā.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "kiberdrošība" ir darbības, kas jāveic, lai aizsargātu tīklu un informācijas sistēmas, to lietotājus un citas personas, kuras skar kiberdraudi;

2) "tīklu un informācijas sistēma" ir tīklu un informācijas sistēma, kas definēta Direktīvas (ES) 2016/1148 4. panta 1. punktā;

3) "valsts tīklu un informācijas sistēmu drošības stratēģija" ir valsts stratēģija par tīklu un informācijas sistēmu drošību, kas definēta Direktīvas (ES) 2016/1148 4. panta 3. punktā;

4) "pamatpakalpojumu sniedzējs" ir pamatpakalpojumu sniedzējs, kas definēts Direktīvas (ES) 2016/1148 4. panta 4. punktā;

5) "digitālā pakalpojuma sniedzējs" ir digitālā pakalpojuma sniedzējs, kas definēts Direktīvas (ES) 2016/1148 4. panta 6. punktā;

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

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

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

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 vai IKT procesu 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 un IKT procesu sertifikāciju vai atbilstības novērtēšanu, kuri ietilpst konkrētās shēmas tvērumā;

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

12) "IKT produkts" ir jebkurš tīkla vai informācijas sistēmas elements vai elementu grupa;

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

14) "IKT process" ir tādu darbību kopums, kuru mērķis ir izstrādāt, attīstīt, nodrošināt vai uzturēt IKT produktu vai IKT pakalpojumu;

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

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

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

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

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

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

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

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

II SADAĻA

ENISA (EIROPAS SAVIENĪBAS KIBERDROŠĪBAS AĢENTŪRA)

I NODAĻA

Pilnvaras un mērķi

3. pants

Pilnvaras

1. *ENISA* veic ar šo regulu tai noteiktos uzdevumus, lai visā Savienībā panāktu vienādi augstu kiberdrošības līmeni, tostarp aktīvi palīdzot dalībvalstīm, Savienības iestādēm, struktūrām, birojiem un aģentūrām uzlabot kiberdrošību. *ENISA* kiberdrošības jomā darbojas kā padomu un lietpratības uzziņas punkts Savienības iestādēm, struktūrām, birojiem un aģentūrām, kā arī citām attiecīgām Savienības ieinteresētajām personām.

ENISA, pildot tai saskaņā ar šo regulu noteiktos uzdevumus, veicina iekšējā tirgus sadrumstalotības mazināšanu.

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

3. Pildot savus uzdevumus, *ENISA* rīkojas neatkarīgi, vienlaikus izvairoties no dublēšanās ar dalībvalsts darbībām un ņemot vērā dalībvalstu esošo lietpratību.

4. *ENISA* attīsta pati savus resursus, tostarp tehniskās un cilvēkresursu spējas un prasmes, kas nepieciešamas, lai varētu veikt tai ar šo regulu noteiktos uzdevumus.

4. pants

Mērķi

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

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

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

4. Aģ *ENISA* entūra ar kiberdrošību saistītos jautājumos veicina Savienības līmeņa sadarbību, tostarp informācijas apmaiņu, un koordināciju starp dalībvalstīm, Savienības iestādēm, struktūrām, birojiem un aģentūrām un attiecīgām privātām un publiskām ieinteresētajām personām.

5. *ENISA* sekmē kiberdrošības spēju uzlabošanu Savienības līmenī, lai atbalstītu dalībvalstu rīcību, kuras nolūks ir novērst kiberdraudus un reaģēt uz tiem, jo īpaši pārrobežu incidentu gadījumā.

6. *ENISA* veicina Eiropas kiberdrošības sertifikācijas izmantošanu nolūkā izvairīties no iekšējā tirgus sadrumstalotības. *ENISA* palīdz izveidot un uzturēt Eiropas kiberdrošības sertifikācijas satvaru saskaņā ar šīs regulas III sadaļu, lai uzlabotu IKT produktu, pakalpojumu un IKT procesu kiberdrošības apliecinājuma pārredzamību, tādējādi stiprinot uzticēšanos digitālajam iekšējam tirgum un tā konkurētspējai.

7. *ENISA* sekmē iedzīvotāju, organizāciju un uzņēmumu dziļu izpratni par kiberdrošību, tostarp kiberhigiēnu un kiberpratību.

II NODAĻA

Uzdevumi

5. pants

Savienības politikas un tiesību aktu izstrāde un īstenošana

Savienības politikas un tiesību aktu izstrādi un īstenošanu *ENISA* sekmē šādi:

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

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

3) palīdz dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām izstrādāt un sekmēt kiberdrošības politiku saistībā ar atklātā interneta publiskā kodola vispārējās pieejamības vai integritātes uzturēšanu;

4) daloties lietpratībā un sniedzot palīdzību, sekmē Sadarbības grupas darbu, ievērojot Direktīvas (ES) 2016/1148 11. pantu;

5) atbalsta:

   a) Savienības politikas izstrādi un īstenošanu elektroniskās identifikācijas un uzticamības pakalpojumu jomā, jo īpaši ar padomu un tehnisko pamatnostādņu izdošanu, kā arī veicinot paraugprakses apmaiņu kompetento iestāžu starpā;

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

   c) dalībvalstis Savienības politikas un tiesību īpašu kiberdrošības aspektu īstenošanā datu aizsardzības un privātuma jomā, tostarp pēc lūguma – sniedzot padomus Eiropas Datu aizsardzības kolēģijai;

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

   a) informāciju par dalībvalstu paziņojumiem par incidentiem, ko Sadarbības grupai sniedz vienotie kontaktpunkti, ievērojot Direktīvas (ES) 2016/1148 10. panta 3. punktu;

   b) tādu paziņojumu par drošības pārkāpumiem vai integritātes zudumu kopsavilkumiem, kas saņemti no uzticamības pakalpojumu sniedzējiem; šos paziņojumus *ENISA* iesniedz uzraudzības iestādes, ievērojot Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 ([23]) 19. panta 3. punktu;

   c) paziņojumiem par drošības incidentiem, ko nosūtījuši publisko elektronisko sakaru tīklu vai publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji; šos paziņojumus *ENISA* iesniedz kompetentās iestādes, ievērojot Direktīvas (ES) 2018/1972 40. pantu.

([23]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).

6. pants

Spēju veidošana

1. *ENISA* palīdz:

a) dalībvalstīm to centienos uzlabot kiberdraudu un incidentu novēršanu, atklāšanu un analīzi un kiberdraudu un incidentu risināšanas spējas, sniedzot tām nepieciešamās zināšanas un daloties lietpratībā;

b) dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām brīvprātīgā kārtā izstrādāt ievainojamības publiskošanas politikas pasākumus un īstenot tos;

c) Savienības iestādēm, struktūrām, birojiem un aģentūrām to centienos uzlabot kiberdraudu un incidentu novēršanu, atklāšanu un analīzi un uzlabot šādu kiberdraudu un incidentu risināšanas spējas, jo īpaši sniedzot pienācīgu atbalstu *CERT-EU*;

d) dalībvalstīm pēc to lūguma izveidot valstu *CSIRT*, ievērojot Direktīvas (ES) 2016/1148 9. panta 5. punktu;

e) dalībvalstīm izstrādāt valstu tīklu un informācijas sistēmu drošības stratēģijas, ja tas lūgts, ievērojot Direktīvas (ES) 2016/1148 7. panta 2. punktu, un veicina minēto stratēģiju izplatīšanu un pieņem zināšanai to īstenošanas progresu Savienībā, lai sekmētu paraugprakses izveidi;

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

g) paaugstināt valstu un Savienības *CSIRT* spēju līmeni, tostarp veicinot dialogu un informācijas apmaiņu, lai nodrošinātu, ka attiecībā uz nozares jaunākajiem sasniegumiem katrai *CSIRT* ir kopīgs spēju minimums un tās darbojas saskaņā ar paraugpraksi;

h) dalībvalstīm, regulāri – vismaz reizi divos gados – organizējot kiberdrošības mācības Savienības līmenī, kā minēts 7. panta 5. punktā, un sniedzot politikas ieteikumus, kuri sagatavoti, balstoties uz šo mācību izvērtējumu un tajās gūto pieredzi;

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

j) Sadarbības grupai, izmantojot paraugprakses apmaiņu, īpaši saistībā ar dalībvalstu veikto pamatpakalpojumu sniedzēju identifikāciju, ievērojot Direktīvas (ES) 2016/1148 11. panta 3. punkta l) apakšpunktu, tostarp attiecībā uz pārrobežu atkarību saistībā ar riskiem un incidentiem.

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

7. pants

Savienības līmeņa operatīvā sadarbība

1. *ENISA* atbalsta operatīvo sadarbību starp dalībvalstīm, Savienības iestādēm, struktūrām, birojiem un aģentūrām un starp ieinteresētajām personām.

2. *ENISA* sadarbojas operatīvā līmenī un veido sinerģiju ar Savienības iestādēm, struktūrām, birojiem un aģentūrām, tostarp *CERT-EU*, dienestiem, kas darbojas kibernoziedzības apkarošanas jomā, un uzraudzības iestādēm, kuru pārziņā ir privātuma un personas datu aizsardzība, un ar mērķi risināt kopīgas problēmas, tostarp šādi:

a) apmainoties ar zinātību un paraugpraksi;

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

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

3. *ENISA* nodrošina *CSIRT* tīkla sekretariātu, ievērojot Direktīvas (ES) 2016/1148 12. panta 2. punktu, un, pildot minēto pienākumu, aktīvi atbalsta informācijas apmaiņu un sadarbību starp tā locekļiem.

4. *ENISA* atbalsta dalībvalstis attiecībā uz operatīvo sadarbību *CSIRT* tīklā:

a) dodot padomus par to, kā uzlabot to spējas novērst un atklāt incidentus un reaģēt uz tiem, un pēc vienas vai vairāku dalībvalstu lūguma dodot padomus saistībā ar konkrētiem kiberdraudiem;

b) pēc vienas vai vairāku dalībvalstu lūguma palīdzot novērtēt tādus incidentus, kam ir būtiska vai nozīmīga ietekme, daloties lietpratībā un atvieglojot šādu incidentu tehnisku risināšanu, tostarp jo īpaši atbalstot attiecīgas informācijas un tehnisko risinājumu brīvprātīgu apmaiņu dalībvalstu starpā;

c) analizējot ievainojamības un incidentus, pamatojoties uz publiski pieejamo informāciju vai informāciju, ko minētajā nolūkā brīvprātīgi sniedz dalībvalstis; un

d) pēc vienas vai vairāku dalībvalstu lūguma sniedzot atbalstu tādu incidentu, kam ir būtiska vai nozīmīga ietekme Direktīvas (ES) 2016/1148 nozīmē, *ex-post* tehniskajā izmeklēšanā.

Veicot minētos uzdevumus, *ENISA* un *CERT-EU* īsteno strukturētu sadarbību, lai gūtu labumu no sinerģijām un izvairītos no darbību dublēšanās.

5. *ENISA* regulāri organizē kiberdrošības mācības Savienības līmenī un pēc to lūguma atbalsta dalībvalstis un Savienības iestādes, struktūras, birojus un aģentūras kiberdrošības mācības organizēšanā. Šādas kiberdrošības mācības Savienības līmenī var ietvert tehniskus, operatīvus vai stratēģiskus elementus. Reizi divos gados *ENISA* organizē plaša mēroga visaptverošas mācības.

Vajadzības gadījumā *ENISA* arī veicina nozaru kiberdrošības mācības un palīdz tās organizēt kopā ar attiecīgajām organizācijām, kuras arī piedalās Savienības mēroga kiberdrošības mācībās.

6. Ciešā sadarbībā ar dalībvalstīm *ENISA* regulāri sagatavo padziļinātu ES kiberdrošības tehniskās situācijas ziņojumu par incidentiem un kiberdraudiem, kurš balstīts uz publiski pieejamo informāciju, *ENISA* veikto analīzi un ziņojumiem, ko tai cita starpā sniegušas dalībvalstu *CSIRT* vai ar Direktīvu (ES) 2016/1148 izveidotie vienotie kontaktpunkti – abi uz brīvprātības pamata –, EC3 un *CERT-EU*.

7. *ENISA* palīdz izstrādāt uz sadarbību balstītu reaģēšanu gan Savienības, gan dalībvalstu līmenī ar kiberdrošību saistītu plašapmēra pārrobežu incidentu vai krīžu gadījumos, galvenokārt:

a) apkopojot un analizējot no valstu avotiem saņemtus ziņojumus, kas ir pieejami atklātībā vai ar kuriem apmainās brīvprātīgi, ar mērķi palīdzēt nonākt pie kopīgas situācijas apzināšanās;

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

c) pēc lūguma veicinot šādu incidentu vai krīžu tehnisko aspektu risināšanu, tostarp jo īpaši atbalstot tehnisko risinājumu brīvprātīgu apmaiņu dalībvalstu starpā;

d) palīdzot Savienības iestādēm, struktūrām, birojiem un aģentūrām un – pēc to lūguma – dalībvalstīm publiskojot saistībā ar šādiem incidentiem vai krīzēm saistīto informāciju;

e) testējot sadarbības plānus reaģēšanai uz šādiem incidentiem vai krīzēm Savienības līmenī, un pēc dalībvalstu lūguma palīdzot tām testēt šādus plānus valsts līmenī.

8. pants

Tirgus, kiberdrošības sertifikācija un standartizācija

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

a) pastāvīgi pārraugot jaunumus saistītajās standartizācijas jomās un iesakot piemērotas tehniskās specifikācijas, kas būtu izmantojamas Eiropas kiberdrošības sertifikācijas shēmu izstrādē, ievērojot 54. panta 1. punkta c) apakšpunktu, gadījumos, kad standarti nav pieejami;

b) IKT produktiem, IKT pakalpojumiem un IKT procesiem sagatavojot Eiropas kiberdrošības sertifikācijas kandidātshēmas ("kandidātshēmas") saskaņā ar 49. pantu;

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

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

e) palīdzot Komisijai nodrošināt *ECCG* sekretariātu, ievērojot 62. panta 5. punktu.

2. *ENISA* nodrošina Ieinteresēto personu kiberdrošības sertifikācijas grupas sekretariātu, ievērojot 22. panta 4. punktu.

3. Sadarbībā ar valstu kiberdrošības sertifikācijas iestādēm un nozares pārstāvjiem oficiālā, strukturētā un pārredzamā veidā *ENISA* apkopo un publicē pamatnostādnes un izstrādā labu praksi saistībā ar IKT produktu, IKT pakalpojumu un IKT procesu kiberdrošības prasībām.

4. Apkopojot un izdodot pamatnostādnes, kā arī pēc dalībvalstu lūguma sniedzot tām atbalstu, *ENISA* veicina spēju veidošanu saistībā ar izvērtēšanu un sertifikācijas procesiem.

5. *ENISA* palīdz izveidot un ieviest Eiropas un starptautiskos riska pārvaldības un IKT produktu, IKT pakalpojumu un IKT procesu drošības standartus.

6. *ENISA* sadarbībā ar dalībvalstīm un nozari sagatavo padomus un pamatnostādnes par tehniskajām jomām, kas saistītas ar drošības prasībām pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem, kā arī par jau spēkā esošajiem standartiem, tostarp dalībvalstu standartiem, ievērojot Direktīvas (ES) 2016/1148 19. panta 2. punktu.

7. *ENISA* regulāri veic aktuālāko kiberdrošības tirgus – gan pieprasījuma, gan piedāvājuma – tendenču analīzi un izplata tās rezultātus, lai sekmētu kiberdrošības tirgu Savienībā.

9. pants

Zināšanas un informācija

ENISA:

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

b) veic kiberdraudu un incidentu ilgtermiņa stratēģisko analīzi, lai apzinātu jaunās tendences un palīdzētu novērst incidentus;

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

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

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

10. pants

Izpratnes uzlabošana un izglītošana

ENISA:

a) uzlabo sabiedrības izpratni par kiberdrošības riskiem un iedzīvotājiem, organizācijām un uzņēmumiem sniedz norādījumus par labu praksi, tostarp par kiberhigiēnu un kiberpratību, individuāliem lietotājiem;

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

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

d) atbalsta dalībvalstu ciešāku koordināciju un paraugprakses apmaiņu par izpratnes uzlabošanu un izglītību kiberdrošības jomā.

11. pants

Pētniecība un inovācija

Saistībā ar pētniecību un inovāciju *ENISA*:

a) dod padomus Savienības iestādēm, struktūrām, birojiem un aģentūrām un dalībvalstīm par pētniecības vajadzībām kiberdrošības jomā un šādu pētījumu prioritātēm, lai tās varētu efektīvi reaģēt uz pašreizējiem un jauniem riskiem un kiberdraudiem, tostarp attiecībā uz jaunām un topošām informācijas un komunikācijas tehnoloģijām, un iedarbīgi izmantot riska novēršanas tehnoloģijas;

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

c) sniedz ieguldījumu stratēģiskās pētniecības un inovācijas programmā Savienības līmenī kiberdrošības jomā.

12. pants

Starptautiska sadarbība

ENISA atbalsta Savienības centienus sadarboties ar trešām valstīm un starptautiskām organizācijām, kā arī attiecīgos starptautiskās sadarbības satvaros, lai veicinātu starptautisko sadarbību ar kiberdrošību saistītos jautājumos, un šajā sakarībā:

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

b) pēc Komisijas lūguma veicina paraugprakses apmaiņu;

c) pēc Komisijas lūguma nodrošina tai lietpratību;

d) sadarbībā ar *ECCG*, kas izveidota saskaņā ar 62. pantu, sniedz Komisijai padomus un atbalstu jautājumos, kas saistīti ar kiberdrošības sertifikātu savstarpēju atzīšanu attiecībās ar trešām valstīm.

III NODAĻA

ENISA organizācija

13. pants

***ENISA* struktūra**

ENISA administratīvo un pārvaldības struktūru veido:

a) Administratīvā padome;

b) Valde;

c) izpilddirektors;

d) *ENISA* Padomdevēju grupa;

e) valsts sadarbības koordinatoru tīkls.

1. iedaļa

Administratīvā padome

14. pants

Administratīvās padomes sastāvs

1. Administratīvajā padomē ir viens loceklis, kuru ieceļ katra dalībvalsts, un divi locekļi, kurus ieceļ Komisija. Visiem locekļiem ir balsstiesības.

2. Katram Administratīvās padomes loceklim ir aizstājējs. Minētais aizstājējs pārstāv locekli tā prombūtnes gadījumā.

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

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

15. pants

Administratīvās padomes funkcijas

1. Administratīvā padome:

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

b) pieņem 24. pantā minētā *ENISA* vienotā programmdokumenta projektu un pēc tam iesniedz to Komisijai, lai saņemtu tās atzinumu;

c) ņemot vērā Komisijas atzinumu, pieņem *ENISA* vienoto programmdokumentu;

d) uzrauga to, kā tiek īstenoti vienotajā programmdokumentā ietvertie daudzgadu plāni un gada plāni;

e) pieņem *ENISA* gada budžetu un pilda citas funkcijas attiecībā uz *ENISA* budžetu saskaņā ar IV nodaļu;

f) novērtē un pieņem konsolidēto gada pārskatu par *ENISA* darbību, tostarp grāmatvedības pārskatus un aprakstu par to, kā *ENISA* ir izpildījusi savus darbības rādītājus, un ne vēlāk kā līdz nākamā gada 1. jūlijam gan gada pārskatu, gan tā novērtējumu iesniedz Eiropas Parlamentam, Padomei, Komisijai un Revīzijas palātai un dara gada pārskatu publiski pieejamu;

g) saskaņā ar 32. pantu pieņem *ENISA* piemērojamos finanšu noteikumus;

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

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

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

k) pieņem savu reglamentu, tostarp noteikumus par pagaidu lēmumiem par konkrētu uzdevumu deleģēšanu, ievērojot 19. panta 7. punktu;

l) attiecībā uz *ENISA* darbiniekiem īsteno pilnvaras, kas Civildienesta noteikumos ("Civildienesta noteikumi") un Savienības Pārējo darbinieku nodarbināšanas kārtībā ("Pārējo darbinieku nodarbināšanas kārtība"), kas noteikti Padomes Regulā (EEK, Euratom, EOTK) Nr. 259/68 ([24]), piešķirtas iecēlējinstitūcijai un iestādei, kura pilnvarota slēgt darba līgumu ("iecēlējinstitūcijas pilnvaras") saskaņā ar šā panta 2. punktu;

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

n) ieceļ izpilddirektoru un attiecīgā gadījumā pagarina viņa pilnvaru laiku vai viņu atceļ no amata saskaņā ar 36. pantu;

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

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

q) atļauj vienoties par darbības mehānismu saistībā ar 7. pantu;

r) atļauj vienoties par vai noslēgt darba vienošanās saskaņā ar 42. pantu.

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

([24]) OV L 56, 4.3.1968., 1. lpp.

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

16. pants

Administratīvās padomes priekšsēdētājs

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

17. pants

Administratīvās padomes sanāksmes

1. Administratīvās padomes sanāksmes sasauc tās priekšsēdētājs.

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

3. Izpilddirektors Administratīvās padomes piedalās sanāksmēs, taču viņam nav balsstiesību.

4. *ENISA* Padomdevēju grupas locekļi Administratīvās padomes sanāksmēs var piedalīties pēc priekšsēdētāja uzaicinājuma, taču viņiem nav balsstiesību.

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

6. *ENISA* nodrošina Administratīvās padomes sekretariātu.

18. pants

Administratīvās padomes balsošanas noteikumi

1. Administratīvā padome pieņem lēmumus ar locekļu balsu vairākumu.

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

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

4. Administratīvās padomes priekšsēdētājs piedalās balsošanā.

5. Izpilddirektors nepiedalās balsošanā.

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

2. iedaļa

Valde

19. pants

Valde

1. Administratīvajai padomei palīdz Valde.

2. Valde:

a) sagatavo lēmumus, kas jāpieņem Administratīvajai padomei;

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

c) neskarot 20. pantā noteiktos izpilddirektora pienākumus, palīdz un sniedz padomus izpilddirektoram Administratīvās padomes lēmumu par administratīviem un budžeta jautājumiem īstenošanā, ievērojot 20. pantu.

3. Valde sastāv no pieciem locekļiem. Valdes locekļus ieceļ no Administratīvās padomes locekļiem. Viens no locekļiem ir Administratīvās padomes priekšsēdētājs, kas var būt arī Valdes priekšsēdētājs, un kāds cits ir viens no Komisijas pārstāvjiem. Ieceļot Valdes locekļus, tiecas nodrošināt dzimumu līdzsvarotību Valdē. Izpilddirektors piedalās Valdes sanāksmēs, bet viņam nav balsstiesību.

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

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

6. Valdes reglamentu nosaka Administratīvā padome.

7. Ja tas vajadzīgs steidzamības dēļ, Valde Administratīvās padomes vārdā var pieņemt konkrētus pagaidu lēmumus, jo īpaši administratīvās pārvaldības lietās, tostarp par iecēlējinstitūcijas pilnvaru deleģējuma apturēšanu un budžeta jautājumiem. Jebkuru šādu pagaidu lēmumu bez liekas kavēšanās paziņo Administratīvajai padomei. Tad ne vēlāk kā trīs mēnešus pēc lēmuma pieņemšanas Administratīvā padome lemj, vai pagaidu lēmumu apstiprināt vai noraidīt. Valde nepieņem tādus lēmumus Administratīvās padomes vārdā, kuru pieņemšanai vajadzīgs divu trešdaļu Administratīvās padomes locekļu balsu vairākums.

3. iedaļa

Izpilddirektors

20. pants

Izpilddirektora pienākumi

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

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

3. Izpilddirektors atbild par to, lai tiktu:

a) ikdienā vadīts *ENISA* darbs;

b) īstenoti Administratīvās padomes pieņemtie lēmumi;

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

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

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

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

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

h) sagatavots *ENISA* piemērojamo finanšu noteikumu projekts, kā minēts 32. pantā;

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

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

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

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

m) uzturēta regulāra saziņa un informācijas apmaiņa ar Savienības iestādēm, struktūrām, birojiem un aģentūrām saistībā ar to darbībām kiberdrošības jomā, lai nodrošinātu saskaņotību Savienības politikas veidošanā un īstenošanā;

n) veikti citi ar šo regulu izpilddirektoram noteikti uzdevumi.

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

5. Vajadzības gadījumā, lai *ENISA* uzdevumi tiktu pildīti rezultatīvi un efektīvi, un uz pienācīgas izmaksu un ieguvumu analīzes pamata izpilddirektors var nolemt izveidot vienu vai vairākus vietējus birojus vienā vai vairākās dalībvalstīs. Pirms izlemj izveidot vietējo biroju, izpilddirektors lūdz attiecīgo dalībvalstu viedokli, tostarp tās dalībvalsts, kurā atrodas *ENISA* mītne, un saņem iepriekšēju piekrišanu no Komisijas un Administratīvās padomes. Ja izpilddirektors un attiecīgās dalībvalstis apspriešanās gaitā nevar vienoties, jautājumu izvirza apspriešanai Padomē. Kopējais darbinieku skaits visos vietējos birojos ir minimāls un nav lielāks par 40 % no to *ENISA* darbinieku kopskaita, kuri atrodas dalībvalstī, kurā atrodas *ENISA* mītne. Darbinieku skaits katrā vietējā birojā nav lielāks par 10 % no to *ENISA* darbinieku kopskaita, kuri atrodas dalībvalstī, kurā atrodas *ENISA* mītne.

Lēmumā, ar ko izveido vietējo biroju, norāda vietējā birojā veicamo darbību tvērumu, izvairoties no liekām izmaksām un *ENISA* administratīvo funkciju dublēšanas.

4. iedaļa

ENISA Padomdevēju grupa, ieinteresēto personu kiberdrošības sertifikācijas grupa un valsts sadarbības koordinatoru tīkls

21. pants

ENISA Padomdevēju grupa

1. Pēc izpilddirektora priekšlikuma Administratīvā padome pārredzamā veidā izveido *ENISA* Padomdevēju grupu, kurā darbojas atzīti eksperti, kas pārstāv attiecīgas ieinteresētās personas, piemēram, IKT nozares pārstāvjus, sabiedrībai pieejamu elektronisko sakaru tīklu vai pakalpojumu nodrošinātājus, MVU, pamatpakalpojumu sniedzējus, patērētāju grupas, ekspertus no akadēmiskajām aprindām kiberdrošības jomā un pārstāvjus no kompetentajām iestādēm, par kurām paziņots saskaņā ar Direktīvu (ES) 2018/1972, Eiropas standartizācijas organizācijām, kā arī tiesībaizsardzības un datu aizsardzības uzraudzības iestādēm. Administratīvās padomes mērķis ir nodrošināt pienācīgu dzimumu un ģeogrāfisko līdzsvaru, kā arī līdzsvaru starp dažādām ieinteresēto personu grupām.

2. *ENISA* Padomdevēju grupā izmantojamās procedūras, jo īpaši attiecībā uz tās sastāvu, 1. punktā minēto izpilddirektora priekšlikumu, locekļu skaitu un kārtību, kādā tos ieceļ, un *ENISA* Padomdevēju grupas darbību, nosaka *ENISA* darbības iekšējos noteikumos un publicē.

3. *ENISA* Padomdevēju grupu vada izpilddirektors vai jebkura persona, kuru izpilddirektors ieceļ attiecīgajam gadījumam.

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

5. *ENISA* Padomdevēju grupa dod padomus *ENISA* attiecībā uz *ENISA* uzdevumu izpildi, izņemot šīs regulas III sadaļas noteikumu piemērošanu. Jo īpaši tā dod padomus izpilddirektoram par *ENISA* gada darba programmas priekšlikuma izstrādi un saziņas nodrošināšanu ar attiecīgajām ieinteresētajām personām par jautājumiem, kas attiecas uz gada darba programmu.

6. *ENISA* Padomdevēju grupa par savu darbību regulāri informē Administratīvo padomi.

22. pants

Ieinteresēto personu kiberdrošības sertifikācijas grupa

1. Izveido Ieinteresēto personu kiberdrošības sertifikācijas grupu.

2. Ieinteresēto personu kiberdrošības sertifikācijas grupa sastāv no locekļiem, kas izvēlēti no atzītu ekspertu vidus un kas pārstāv attiecīgās ieinteresētās personas. Ieinteresēto personu kiberdrošības sertifikācijas grupas locekļus pēc *ENISA* priekšlikuma izvēlas Komisija pārredzamā un atklātā konkursā, nodrošinot līdzsvaru starp dažādām ieinteresēto personu grupām, kā arī pienācīgu dzimumu un ģeogrāfisko līdzsvaru.

3. Ieinteresēto personu kiberdrošības sertifikācijas grupa:

a) dod padomus Komisijai stratēģiskos jautājumos attiecībā uz Eiropas kiberdrošības sertifikācijas satvaru;

b) pēc lūguma sniedz padomus *ENISA* par vispārīgiem un stratēģiskiem jautājumiem, kas attiecas uz *ENISA* uzdevumiem saistībā ar tirgu, kiberdrošības sertifikāciju un standartizāciju;

c) palīdz Komisijai sagatavot Savienības mainīgo darba programmu, kas minēta 47. pantā;

d) sniedz atzinumu par Savienības mainīgo darba programmu, ievērojot 47. panta 4. punktu; un

e) steidzamos gadījumos sniedz padomus Komisijai un *ECCG* par nepieciešamību ieviest papildu sertifikācijas shēmas, kas nav iekļautas Savienības mainīgajā darba programmā, kā minēts 47. un 48. pantā.

4. Ieinteresēto personu kiberdrošības sertifikācijas grupu kopīgi vada Komisijas un *ENISA* pārstāvji, un tās sekretariātu nodrošina *ENISA*.

23. pants

Valsts sadarbības koordinatoru tīkls

1. Pēc izpilddirektora priekšlikuma Administratīvā padome izveido valsts sadarbības koordinatoru tīklu, kurā darbojas visu dalībvalstu pārstāvji ("valsts sadarbības koordinatori"). Katra dalībvalsts valsts sadarbības koordinatoru tīklā ieceļ vienu pārstāvi. Valsts sadarbības koordinatoru tīkla sanāksmes var notikt dažādu ekspertu sastāvā.

2. Valsts sadarbības koordinatoru tīkls jo īpaši veicina informācijas apmaiņu starp *ENISA* un dalībvalstīm un palīdz *ENISA* izplatīt informāciju par savām darbībām, konstatējumus un ieteikumus ieinteresētajām personām visā Savienībā.

3. Valsts sadarbības koordinatori ir kontaktpunkts valsts līmenī, lai atvieglotu *ENISA* un valstu ekspertu sadarbību *ENISA* gada darba programmas īstenošanas kontekstā.

4. Lai gan valsts sadarbības koordinatori cieši sadarbojas ar savu attiecīgo dalībvalstu pārstāvjiem Administratīvajā padomē, valsts sadarbības koordinatoru tīkla darbs nedublē ne Administratīvās padomes, ne citu Savienības forumu darbu.

5. Valsts sadarbības koordinatoru tīkla funkcijas un procedūras nosaka *ENISA* darbības iekšējos noteikumos un publisko.

5. iedaļa

Darbība

24. pants

Vienotais programmdokuments

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

2. Izpilddirektors katru gadu atbilstīgi Komisijas Deleģētās regulas (ES) Nr. 1271/2013 ([25]) 32. pantam un Komisijas pamatnostādnēm izstrādā vienoto programmdokumentu ar gada plāniem un daudzgadu plāniem, kuros ietverts atbilstošo finanšu līdzekļu un cilvēkresursu plānojums.

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

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

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

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

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

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

8. Resursu plānu atjaunina reizi gadā. Stratēģisko plānu vajadzības gadījumā atjaunina, jo īpaši, lai ņemtu vērā 67. pantā minētās izvērtēšanas iznākumu.

25. pants

Interešu deklarācija

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

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

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

26. pants

Pārredzamība

1. *ENISA* savā darbībā nodrošina augsta līmeņa pārredzamību saskaņā ar 28. pantu.

2. *ENISA* gādā, lai sabiedrībai un visām ieinteresētajām personām tiek sniegta atbilstoša, objektīva, ticama un viegli pieejama informāciju, jo īpaši par Aģentūras darba rezultātiem. Tā publicē arī interešu deklarācijas, kas iesniegtas saskaņā ar 25. pantu.

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

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

27. pants

Konfidencialitāte

1. Neskarot 28. pantu, *ENISA* neizpauž trešām personām informāciju, ko tā apstrādā vai saņem, ja par to ir izteikts pamatots lūgums to uzskatīt par konfidenciālu.

2. Uz Administratīvās padomes locekļiem, izpilddirektoru, *ENISA* Padomdevēju grupas locekļiem, ārējiem ekspertiem, kas piedalās *ad hoc* darba grupās, un *ENISA* personāla locekļiem, tostarp dalībvalstu uz laiku norīkotajām amatpersonām, konfidencialitātes prasības saskaņā ar LESD 339. pantu attiecas arī pēc tam, kad šīs personas ir beigušas pildīt savus pienākumus.

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

4. Ja tas nepieciešams *ENISA* uzdevumu veikšanai, Administratīvā padome atļauj *ENISA* apstrādāt klasificētu informāciju. Tādā gadījumā *ENISA*, vienojoties ar Komisijas dienestiem, pieņem drošības noteikumus, piemērojot drošības principus, kas noteikti Komisijas Lēmumā (ES, Euratom) 2015/443 ([26]) un Lēmumā (ES, Euratom) 2015/444 ([27]). Minētie drošības noteikumi reglamentē klasificētas informācijas apmaiņu, apstrādi un glabāšanu.

28. pants

Piekļuve dokumentiem

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

2. Līdz 2019. gada 28. decembrim Valde pieņem Regulas (EK) Nr. 1049/2001 izpildei vajadzīgos pasākumus.

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

IV NODAĻA

ENISA *budžeta izveide un uzbūve*

29. pants

***ENISA* budžeta izveide**

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

2. Pamatojoties uz tāmes projektu, katru gadu Administratīvā padome sagatavo *ENISA* ieņēmumu un izdevumu tāmi nākamajam finanšu gadam.

3. Tāmes projektu, kas ir iekļauts vienotā programmdokumenta projektā, Administratīvā padome līdz katra gada 31. janvārim nosūta Komisijai un trešām valstīm, ar kurām Savienība ir noslēgusi nolīgumus, kā minēts 42. panta 2. punktā.

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

5. Eiropas Parlaments un Padome apstiprina Savienības iemaksu apropriācijas *ENISA*.

6. Eiropas Parlaments un Padome apstiprina *ENISA* štatu sarakstu.

([26]) Komisijas Lēmums (ES, Euratom) 2015/443 (2015. gada 13. marts) par drošību Komisijā (OV L 72, 17.3.2015., 41. lpp.).
([27]) Komisijas Lēmums (ES, Euratom) 2015/444 (2015. gada 13. marts) par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.).

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

30. pants

ENISA budžeta struktūra

1. Neskarot citus resursus, *ENISA* ieņēmumos ietilpst:

a) iemaksas no Savienības vispārējā budžeta;

b) ieņēmumi, kas konkrētiem izdevumu posteņiem piešķirti saskaņā ar tās finanšu noteikumiem, kas izklāstīti 32. pantā;

c) Savienības finansējums deleģēšanas nolīgumu vai *ad hoc* dotāciju veidā saskaņā ar tās finanšu noteikumiem, kas izklāstīti 32. pantā, un noteikumiem attiecīgajos tiesību aktos, ar kuriem atbalsta Savienības politikas jomas;

d) iemaksas no trešām valstīm, kuras piedalās *ENISA* darbā, kā minēts 42. pantā;

e) jebkādas dalībvalstu brīvprātīgas iemaksas naudā vai natūrā.

Dalībvalstis, kuras veic brīvprātīgās iemaksas saskaņā ar pirmās daļas e) apakšpunktu, šā iemesla dēļ nepieprasa īpašas tiesības vai pakalpojumus.

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

31. pants

ENISA budžeta izpilde

1. Par *ENISA* budžeta izpildi atbild izpilddirektors.

2. Komisijas iekšējam revidentam *ENISA* ir tādas pašas pilnvaras kā Komisijas dienestos.

3. *ENISA* grāmatvedis provizoriskos pārskatus par finanšu gadu (N gads) Komisijas grāmatvedim un Revīzijas palātai nosūta līdz nākamā finanšu gada 1. martam (N+1. gads).

4. Kad ir saņemti Revīzijas palātas apsvērumi par provizoriskajiem pārskatiem atbilstīgi Eiropas Parlamenta un Padomes Regulas (ES, Euratom) 2018/1046 ([28]) 246. pantam, *ENISA* grāmatvedis uz savu atbildību sagatavo *ENISA* galīgos pārskatus un iesniedz tos Administratīvajai padomei, lai saņemtu tās atzinumu.

5. Administratīvā padome sniedz atzinumu par *ENISA* galīgajiem pārskatiem.

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

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

([28]) 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.).

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

9. Līdz N+1. gada 15. novembrim izpilddirektors publicē galīgos pārskatus *Eiropas Savienības Oficiālajā Vēstnesī*.

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

11. Saskaņā ar Regulas (ES, Euratom) 2018/1046 261. panta 3. punktu pēc Eiropas Parlamenta lūguma izpilddirektors tam iesniedz visu informāciju, kas vajadzīga netraucētai attiecīgā finanšu gada budžeta izpildes apstiprinājuma procedūras piemērošanai.

12. Saskaņā ar Padomes ieteikumu Eiropas Parlaments pirms N+2. gada 15. maija sniedz izpilddirektoram apstiprinājumu par N gada budžeta izpildi.

32. pants

Finanšu noteikumi

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

33. pants

Krāpšanas apkarošana

1. Lai palīdzētu apkarot krāpšanu, korupciju un citas nelikumīgas darbības, kā paredzēts Eiropas Parlamenta un Padomes Regulā (ES, Euratom) Nr. 883/2013 ([29]), *ENISA* līdz 2019. gada 28. decembrim pievienojas Eiropas Parlamenta, Eiropas Savienības Padomes un Eiropas Kopienu Komisijas 1999. gada 25. maija Iestāžu nolīgumam par iekšējām izmeklēšanām, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*) ([30]). Izmantojot minētā nolīguma pielikumā doto paraugu, *ENISA* pieņem attiecīgus noteikumus, kas piemērojami visiem *ENISA* darbiniekiem.

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

3. *OLAF* var veikt izmeklēšanu, tostarp pārbaudes un apskates uz vietas, saskaņā ar noteikumiem un procedūrām, kas noteiktas Regulā (ES, Euratom) Nr. 883/2013 un Padomes Regulā (Euratom, EK) Nr. 2185/96 ([31]), lai noteiktu, vai nav notikusi krāpšana, korupcija vai kādas citas nelikumīgas darbības, kas ietekmē Savienības finanšu intereses, kuras saistītas ar *ENISA* finansētu dotāciju vai līgumu.

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

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

([30]) OV L 136, 31.5.1999., 15. lpp.

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

V NODAĻA

Darbinieki

34. pants

Vispārīgi noteikumi

Uz *ENISA* darbiniekiem attiecas Civildienesta noteikumi un Savienības pārējo darbinieku nodarbināšanas kārtība, kā arī noteikumi, kas pieņemti, vienojoties Savienības iestādēm, lai īstenotu Civildienesta noteikumus un Savienības pārējo darbinieku nodarbināšanas kārtību.

35. pants

Privilēģijas un imunitāte

Uz *ENISA* un tās darbiniekiem attiecas Protokols Nr. 7 par privilēģijām un imunitāti Eiropas Savienībā, kas pievienots LES un LESD.

36. pants

Izpilddirektors

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

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

3. Lai noslēgtu darba līgumu ar izpilddirektoru, *ENISA* pārstāv Administratīvās padomes priekšsēdētājs.

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

5. Izpilddirektora amata pilnvaru termiņš ir pieci gadi. Līdz minētā laikposma beigām Komisija veic novērtējumu par izpilddirektora sniegumu un *ENISA* turpmākajiem uzdevumiem un izaicinājumiem.

6. Administratīvās padomes lēmumus par izpilddirektora iecelšanu amatā, viņa pilnvaru laika pagarināšanu vai atbrīvošanu no amata pieņem saskaņā ar 18. panta 2. punktu.

7. Administratīvā padome, rīkojoties pēc Komisijas priekšlikuma, kurā ņemts vērā 5. punktā minētais novērtējums, izpilddirektora amata pilnvaru laiku var vienu reizi pagarināt par pieciem gadiem.

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

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

10. Izpilddirektoru no amata var atcelt tikai ar Administratīvās padomes lēmumu, kas pieņemts pēc Komisijas priekšlikuma.

37. pants

Norīkotie valsts eksperti un pārējie darbinieki

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

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

VI NODAĻA

***Vispārīgi noteikumi attiecībā uz** ENISA*

38. pants

ENISA juridiskais statuss

1. *ENISA* ir Savienības struktūra, un tai piemīt tiesībsubjektība.

2. Visās dalībvalstīs *ENISA* ir visplašākā tiesībspēja un rīcībspēja, ko attiecīgās valsts tiesību akti piešķir juridiskām personām. Konkrēti, tā var iegādāties vai atsavināt kustamu un nekustamu īpašumu, kā arī būt par pusi tiesas procesā.

3. *ENISA* pārstāv izpilddirektors.

39. pants

ENISA atbildība

1. *ENISA* līgumisko atbildību reglamentē attiecīgajam līgumam piemērojamās tiesības.

2. Pieņemt nolēmumus, ievērojot jebkuru šķīrējklauzulu, kas ietverta *ENISA* noslēgtā līgumā, ir Eiropas Savienības Tiesas jurisdikcijā.

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

4. Visi strīdi, kas saistīti ar 3. punktā minēto zaudējumu atlīdzināšanu, ir Eiropas Savienības Tiesas jurisdikcijā.

5. *ENISA* darbinieku personisko atbildību pret *ENISA* reglamentē attiecīgie nosacījumi, kas attiecas uz *ENISA* darbiniekiem.

40. pants

Valodu lietošanas kārtība

1. Uz *ENISA* attiecas Padomes Regula Nr. 1 ([32]). Dalībvalstis un pārējās struktūras, ko dalībvalstis ieceļ, var vērsties pie *ENISA* un saņemt atbildi jebkurā Eiropas Savienības iestāžu oficiālajā valodā pēc savas izvēles.

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

41. pants

Personas datu aizsardzība

1. Personas datu apstrādi *ENISA* reglamentē Eiropas Parlamenta un Padomes Regula (ES) 2018/1725.

2. Administratīvā padome pieņem īstenošanas noteikumus, kas minēti Regulas (ES) 2018/1725 45. panta 3. punktā. Administratīvā padome var pieņemt papildu pasākumus, kas vajadzīgi, lai *ENISA* piemērotu Regulu (ES) 2018/1725.

([32]) Regula Nr. 1, ar ko nosaka Eiropas Ekonomikas kopienā lietojamās valodas (OV 17, 6.10.1958., 385./58. lpp.).

42. pants

Sadarbība ar trešām valstīm un starptautiskām organizācijām

1. Ciktāl tas vajadzīgs, lai sasniegtu šajā regulā aprakstītos mērķus, *ENISA* var sadarboties ar trešo valstu kompetentajām iestādēm vai ar starptautiskajām organizācijām, vai abējādi. Šādā nolūkā *ENISA*, saņēmusi Komisijas iepriekšēju atļauju, ar trešo valstu iestādēm un starptautiskajām organizācijām var noslēgt darba vienošanās. Minētās darba vienošanās ne Savienībai, ne tās dalībvalstīm nerada juridiskas saistības.

2. *ENISA* ir atvērta to trešo valstu dalībai, kuras ar Savienību noslēgušas attiecīgus nolīgumus. Saskaņā ar šādu nolīgumu attiecīgajiem noteikumiem tiek izstrādāta darba vienošanās, ar ko jo īpaši nosaka, kā pēc būtības, kādā apjomā un kādā veidā minētās trešās valstis piedalās *ENISA* darbā, un ietver noteikumus par dalību *ENISA* iniciatīvās, finanšu iemaksām un darbiniekiem. Attiecībā uz personāla jautājumiem minētā darba vienošanās visos gadījumos ir saskaņā ar Civildienesta noteikumiem un Savienības pārējo darbinieku nodarbināšanas kārtību.

3. Administratīvā padome pieņem stratēģiju attiecībām ar trešām valstīm un starptautiskām organizācijām *ENISA* kompetencē esošos jautājumos. Komisija, noslēdzot attiecīgas darba vienošanās ar izpilddirektoru, nodrošina, ka *ENISA* darbojas atbilstīgi savām pilnvarām un pastāvošajai iestāžu sistēmai.

43. pants

Drošības noteikumi par sensitīvas neklasificētas informācijas un klasificētas informācijas aizsardzību

Pēc apspriešanās ar Komisiju, *ENISA* pieņem drošības noteikumus, kuros piemēroti drošības principi, kas ietverti Komisijas drošības noteikumos par sensitīvas neklasificētas informācijas un ESKI aizsardzību, kuri noteikti Lēmumos (ES, Euratom) 2015/443 un 2015/444. *ENISA* drošības noteikumi cita starpā ietver noteikumus par šādas informācijas apmaiņu, apstrādi un glabāšanu.

44. pants

Mītnes nolīgums un darbības nosacījumi

1. Nepieciešamo kārtību attiecībā uz *ENISA* paredzēto atrašanās vietu uzņēmējā dalībvalstī un telpām, kuru pieejamību nodrošina šī dalībvalsts, kopā ar specifiskajiem noteikumiem, kas uzņēmējā dalībvalstī piemērojami izpilddirektoram, Administratīvās padomes locekļiem, *ENISA* darbiniekiem un viņu ģimenes locekļiem, nosaka mītnes nolīgumā starp *ENISA* un uzņēmēju dalībvalsti, kuru noslēdz pēc tam, kad saņemts Administratīvās padomes apstiprinājums.

2. *ENISA* uzņēmēja dalībvalsts nodrošina iespējami labākos apstākļus, lai nodrošinātu pienācīgu *ENISA* darbību, ņemot vērā atrašanās vietas pieejamību, adekvātas izglītības iestādes darbinieku bērniem, atbilstošu piekļuvi darba tirgum, sociālajai drošībai un medicīniskajai aprūpei gan darbinieku bērniem, gan laulātajiem.

45. pants

Administratīvā kontrole

ENISA darbību saskaņā ar LESD 228. pantu uzrauga Eiropas Ombuds.

III SADAĻA

KIBERDROŠĪBAS SERTIFIKĀCIJAS SATVARS

46. pants

Eiropas kiberdrošības sertifikācijas satvars

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 un IKT procesu digitālu vienoto tirgu.

2. Eiropas kiberdrošības sertifikācijas satvars sniedz mehānismu Eiropas kiberdrošības sertifikācijas shēmas izveidei un tam, lai apliecinātu, 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, ko piedāvā izmantot minētie produkti, pakalpojumi un procesi, vai kam, tos izmantojot, var piekļūt.

47. pants

Savienības mainīgā darba programma Eiropas kiberdrošības sertificēšanai

1. Komisija publicē Savienības mainīgo darba programmu Eiropas kiberdrošības sertificēšanai ("Savienības mainīgā darba programma"), kurā nosaka stratēģiskās prioritātes turpmākajām Eiropas kiberdrošības sertificēšanas shēmām.

2. Savienības mainīgajā darba programmā jo īpaši iekļauj tādu IKT produktu, IKT pakalpojumu un IKT procesu vai to kategoriju sarakstu, kam iekļaušana Eiropas kiberdrošības sertificēšanas shēmas piemērošanas jomā var nākt par labu.

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

a) tādu valstu kiberdrošības sertifikācijas shēmu pieejamību un izstrādi, kurās iekļauta konkrēta IKT produktu, IKT pakalpojumu vai IKT procesu kategorija, jo īpaši attiecībā uz sadrumstalotības risku;

b) attiecīgu Savienības vai dalībvalstu tiesību aktiem vai politiku;

c) pieprasījumu tirgū;

d) tendencēm kiberdraudu vidē;

e) *ECCG* pieprasījumu izveidot konkrētu kandidātshēmu.

4. Komisija pienācīgi ņem vērā *ECCG* un Ieinteresēto personu sertifikācijas grupas izdotus atzinumus par Savienības mainīgās darba programmas projektu.

5. Pirmo Savienības mainīgo darba programmu publicē līdz 2020. gada 28. jūnijam. Savienības mainīgo darba programmu atjaunina vismaz reizi trīs gados un biežāk, ja vajadzīgs.

48. pants

Eiropas kiberdrošības sertifikācijas shēmas pieprasījums

1. Komisija var pieprasīt, lai *ENISA*, pamatojoties uz Savienības mainīgo darba programmu, izveido kandidātshēmu vai pārskata jau esošu Eiropas kiberdrošības sertifikācijas shēmu.

2. Pienācīgi pamatotos gadījumos Komisija vai *ECCG* var pieprasīt, lai *ENISA* izveido kandidātshēmu vai pārskata jau esošu Eiropas kiberdrošības sertifikācijas shēmu, kas nav iekļauta Savienības mainīgajā darba programmā. Savienības mainīgo darba programmu attiecīgi atjaunina.

49. pants

Eiropas kiberdrošības sertifikācijas shēmas izveidošana, pieņemšana un pārskatīšana

1. Pēc Komisijas lūguma, ievērojot 48. pantu, *ENISA* izveido kandidātshēmu, kas atbilst 51., 52. un 54. pantā noteiktajām prasībām.

2. Pēc *ECCG* lūguma, ievērojot 48. panta 2. punktu, *ENISA* var izveidot kandidātshēmu, kas atbilst 51., 52. un 54. pantā noteiktajām prasībām. Ja *ENISA* šādu lūgumu noraida, tā sniedz noraidīšanas iemeslus. Jebkuru lēmumu noraidīt šādu lūgumu pieņem Administratīvā padome.

3. Izveidojot kandidātshēmu, *ENISA* oficiālā, atklātā, pārredzamā un iekļaujošā apspriešanās procesā apspriežas ar visām attiecīgajām ieinteresētajām personām.

4. Attiecībā uz katru kandidātshēmu *ENISA* saskaņā ar 20. panta 4. punktu izveido *ad hoc* darba grupu, lai sniegtu *ENISA* konkrētus padomus un lietpratību.

5. *ENISA* cieši sadarbojas ar *ECCG*. *ECCG* sniedz *ENISA* palīdzību un ekspertu padomus saistībā ar kandidātshēmas izveidi un pieņem atzinumu par kandidātshēmu.

6. Pirms kandidātshēmas, kas izveidota saskaņā ar 3., 4. un 5. punktu, nosūtīšanas Komisijai *ENISA* vislielākajā mērā ņem vērā *ECCG* atzinumu. *ECCG* atzinums nav saistošs *ENISA*, bet tā neesamība neliedz *ENISA* nosūtīt kandidātshēmu Komisijai.

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

8. *ENISA* vismaz reizi piecos gados novērtē katru pieņemto Eiropas kiberdrošības sertifikācijas shēmu, ņemot vērā no ieinteresētajām pusēm saņemto atgriezenisko informāciju. Ja nepieciešams, Komisija vai *ECCG* var *ENISA* lūgt uzsākt pārskatītas kandidātshēmas izstrādes procesu saskaņā ar 48. un šo pantu.

50. pants

Eiropas kiberdrošības sertifikācijas shēmu tīmekļa vietne

1. *ENISA* uztur īpaši izveidotu tīmekļa vietni, kurā sniedz informāciju un publicē Eiropas kiberdrošības sertifikācijas shēmas, Eiropas kiberdrošības sertifikātus un ES atbilstības apliecinājumus, tostarp informāciju attiecībā uz Eiropas kiberdrošības sertifikācijas shēmām, kas vairs nav spēkā, Eiropas kiberdrošības sertifikātiem un ES atbilstības apliecinājumiem, kuri ir atcelti vai kuriem beidzies derīguma termiņš, un reģistru ar saitēm uz kiberdrošības informāciju, kas sniegta saskaņā ar 55. pantu.

2. Attiecīgā gadījumā 1. punktā minētajā tīmekļa vietnē norāda arī tās valsts kiberdrošības sertifikācijas shēmas, kuras ir aizstātas ar Eiropas kiberdrošības sertifikācijas shēmu.

51. pants

Eiropas kiberdrošības sertifikācijas shēmu drošības mērķi

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

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

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

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

d) konstatēt un dokumentēt zināmās atkarības un ievainojamības;

e) reģistrēt, kuriem datiem, pakalpojumiem vai funkcijām ir piekļūts, tie ir izmantoti vai citādi apstrādāti un kad un kurš to ir darījis;

f) ir iespējams pārbaudīt, kuriem datiem, pakalpojumiem vai funkcijām ir piekļūts, kuri ir izmantoti vai citādi apstrādāti un kad un kurš to ir darījis;

g) pārbaudīt to, vai IKT produktiem, IKT pakalpojumiem un IKT procesiem nav zināmu ievainojamību;

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

i) IKT produkti, IKT pakalpojumi un IKT procesi atbilst principiem "drošs pēc noklusējuma" (*secure by default*) un "konstruēts, lai būtu drošs" (*secure by design*);

j) IKT produktiem, IKT pakalpojumiem un IKT procesiem ir nodrošināta atjaunināta programmatūra un aparatūra, kam nav publiski zināmu ievainojamību, un tiem ir mehānismi, kas nodrošina drošus atjauninājumus.

52. pants

Eiropas kiberdrošības sertifikācijas shēmu apliecinājuma līmeņi

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

2. Eiropas kiberdrošības sertifikātos un ES atbilstības apliecinājumos jāatsaucas uz jebkuru apliecinājuma līmeni, kas norādīts Eiropas kiberdrošības sertifikācijas shēmā, saskaņā ar kuru izdots Eiropas kiberdrošības sertifikāts vai ES atbilstības apliecinājums.

3. Attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā jānorāda katram apliecinājuma līmenim atbilstošās drošības prasības, tostarp atbilstošās drošības funkcijas un IKT produktam, IKT pakalpojumam vai IKT procesam veicamā izvērtējuma atbilstošā stingrība un dziļums.

4. Sertifikātam vai ES atbilstības apliecinājumam ir norāde uz tehniskajām specifikācijām, standartiem un saistītajām procedūrām, tostarp uz tehniskajām kontrolēm, kuru nolūks ir samazināt vai novērst kiberdrošības incidentu risku.

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

6. Ar Eiropas kiberdrošības sertifikātu, kam ir norāde uz apliecinājuma līmeni "būtisks", sniedz apliecinājumu, ka IKT produkti, IKT pakalpojumi un IKT procesi, par kuriem izdots minētais sertifikāts, atbilst attiecīgajām drošības prasībām, tostarp drošības funkcijām, un ka tie ir izvērtēti tādā līmenī, kas paredz minimizēt zināmos kiberdrošības riskus un tādu incidentu un kiberuzbrukumu risku, ko veic aktori ar ierobežotām prasmēm un resursiem. Veicamās izvērtējuma darbības ietver vismaz: pārskatīšanu nolūkā pierādīt to, ka nav publiski zināmu ievainojamību, un pārbaudi nolūkā pierādīt to, ka ar IKT produktiem, IKT pakalpojumiem vai IKT procesiem ir pareizi īstenotas vajadzīgās drošības funkcijas. Ja neviena šāda izvērtējuma darbība nav piemērota, jāveic alternatīvas izvērtējuma darbības ar līdzvērtīgu ietekmi.

7. Ar Eiropas kiberdrošības sertifikātu, kam ir norāde uz apliecinājuma līmeni "augsts", sniedz apliecinājumu, ka IKT produkti, IKT pakalpojumi un IKT procesi, par kuriem izdots minētais sertifikāts, atbilst attiecīgajām drošības prasībām, tostarp drošības funkcijām, un ka tie ir izvērtēti tādā līmenī, kas paredz minimizēt sarežģītu kiberuzbrukumu risku, ko veic aktori ar būtiskām prasmēm un resursiem. Veicamās izvērtējuma darbības ietver vismaz: pārskatīšanu nolūkā pierādīt to, ka nav publiski zināmu ievainojamību; pārbaudi nolūkā pierādīt to, ka ar IKT produktiem, IKT pakalpojumiem vai IKT procesiem ir pareizi īstenotas vajadzīgās drošības funkcijas – augstākajā līmenī –; un izvērtējumu ar ielaušanās testiem par to, ka tie ir noturīgi pret prasmīgu uzbrucēju uzbrukumiem. Ja neviena šāda izvērtējuma darbība nav piemērota, jāveic alternatīvas izvērtējuma darbības ar līdzvērtīgu ietekmi.

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

53. pants

Atbilstības pašnovērtējums

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

2. IKT produktu, IKT pakalpojumu vai IKT procesu 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 vai IKT procesu ražotājs vai sniedzējs uzņemas atbildību par IKT produkta, IKT pakalpojuma vai IKT procesa atbilstību minētajā shēmā izklāstītajām prasībām.

3. IKT produktu, IKT pakalpojumu vai IKT procesu ražotājs vai sniedzējs uz attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā paredzēto laikposmu 58. pantā minētajai valsts kiberdrošības sertifikācijas iestādei dara pieejamu ES atbilstības apliecinājumu, tehnisko dokumentāciju un visu citu attiecīgo informāciju, kas saistīta ar IKT produktu vai IKT pakalpojumu atbilstību shēmai. ES atbilstības apliecinājuma kopiju iesniedz valsts kiberdrošības sertifikācijas iestādei un *ENISA*.

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

5. ES atbilstības apliecinājumi tiek atzīti visās dalībvalstīs.

54. pants

Eiropas kiberdrošības sertifikācijas shēmu elementi

1. Eiropas kiberdrošības sertifikācijas shēmā ir vismaz šādi elementi:

a) sertifikācijas shēmas priekšmets un tvērums, tostarp shēmā ietverto IKT produktu, IKT pakalpojumu un IKT procesu pakalpojumu tipi vai kategorijas;

b) skaidrs apraksts par shēmas nolūku un to, kā izvēlētie standarti, izvērtēšanas metodes un apliecinājuma līmeņi atbilst paredzamo shēmas lietotāju vajadzībām;

c) atsauce uz starptautiskiem, Eiropas vai valsts standartiem, kas piemēroti izvērtējumā, vai ja šādi standarti nav pieejami vai nav atbilstīgi, atsauce uz tehniskajām specifikācijām, kas atbilst Regulas (ES) Nr. 1025/2012 II pielikumā izklāstītajām prasībām, vai, ja šādas specifikācijas nav pieejamas, uz tehniskajām specifikācijām vai citām kiberdrošības prasībām, kas ir definētas Eiropas kiberdrošības sertifikācijas shēmā;

d) attiecīgā gadījumā – viens vai vairāki apliecinājuma līmeņi;

e) norāde par to, vai shēmā ir atļauts atbilstības pašnovērtējums;

f) attiecīgā gadījumā – specifiskas vai papildu prasības, kas attiecas uz atbilstības novērtēšanas struktūrām, lai nodrošinātu, ka tām ir tehniskā kompetence izvērtēt kiberdrošības prasības;

g) konkrēti izvērtēšanas kritēriji un izmantojamās metodes, tostarp izvērtēšanas veidi, ko izmanto, lai pierādītu, ka 51. pantā minētie drošības mērķi ir sasniegti;

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

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

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

k) attiecīgā gadījumā – nosacījumi Eiropas kiberdrošības sertifikātu izdošanai, saglabāšanai, turpmākai izmantošanai un atjaunošanai, kā arī nosacījumi sertifikācijas tvēruma paplašināšanai vai samazināšanai;

l) noteikumi par sekām, ko rada tādi IKT produkti, IKT pakalpojumi un IKT procesi, kas ir sertificēti vai par kuriem ir izdots ES atbilstības apliecinājums, bet kuri neatbilst shēmas prasībām;

m) noteikumi par kārtību, kādā jāziņo par iepriekš neidentificētām IKT produktu, IKT pakalpojumu un IKT procesu kiberdrošības ievainojamībām un kā tās jānovērš;

n) attiecīgā gadījumā – noteikumi par uzskaites datu glabāšanu atbilstības novērtēšanas struktūrās;

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

p) izdodamo Eiropas kiberdrošības sertifikātu un ES atbilstības apliecinājumu saturs un formāts;

q) pieejamības laikposms, uz kuru IKT produktu, IKT pakalpojumu vai IKT procesu ražotājam vai sniedzējam jādara pieejams ES atbilstības apliecinājums, tehniskā dokumentācija un visa cita attiecīgā informācija;

r) maksimālais saskaņā ar shēmu izdoto Eiropas kiberdrošības sertifikātu derīguma termiņš;

s) izpaušanas politika attiecībā uz Eiropas kiberdrošības sertifikātiem, kas izdoti, grozīti vai atsaukti saskaņā ar shēmu;

t) nosacījumi sertifikācijas shēmu savstarpējai atzīšanai sadarbībā ar trešām valstīm;

u) attiecīgā gadījumā – visu shēmā izveidoto salīdzinošās izvērtēšanas mehānismu noteikumi iestādēm vai struktūrām, kuras izdod Eiropas kiberdrošības sertifikātus par apliecinājuma līmeni "augsts", ievērojot 56. panta 6. punktu. Šādi mehānismi neskar salīdzinošo izvērtēšanu, kas paredzēta 59. pantā;

v) formāts un procedūra, kas jāievēro IKT produktu, IKT pakalpojumu vai IKT procesu ražotājiem vai sniedzējiem, sniedzot un atjauninot papildu kiberdrošības informāciju saskaņā ar 55. pantu.

2. Eiropas kiberdrošības sertifikācijas shēmas noteiktās prasības atbilst piemērojamajām juridiskajām prasībām, īpaši prasībām, kas izriet no saskaņotajiem Savienības tiesību aktiem.

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

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

55. pants

Sertificētu IKT produktu, IKT pakalpojumu un IKT procesu kiberdrošības papildu informācija

1. Sertificētu IKT produktu, IKT pakalpojumu vai IKT procesu ražotājs vai sniedzējs vai tādu IKT produktu, IKT pakalpojumu vai IKT procesu ražotājs vai sniedzējs, par kuriem ir izdots ES atbilstības apliecinājums, dara publiski pieejamu šādu kiberdrošības papildu informāciju:

a) norādījumi un ieteikumi nolūkā palīdzēt galalietotājiem veikt IKT produktu vai IKT pakalpojumu drošu konfigurāciju, uzstādīšanu, izvēršanu, ekspluatāciju un apkalpošanu;

b) laikposms, kādā galalietotājiem tiks piedāvāts drošības atbalsts, jo īpaši attiecībā uz ar kiberdrošību saistītu atjauninājumu pieejamību;

c) ražotāja vai sniedzēja kontaktinformācija un pieņemtās metodes informācijas par ievainojamībām saņemšanai no galalietotājiem un drošības pētniekiem;

d) atsauce uz tiešsaistes reģistriem, kuros uzskaitītas publiski atklātas ievainojamības saistībā ar IKT produktu, IKT pakalpojumu vai IKT procesu un uz jebkuriem attiecīgiem kiberdrošības padomdevējiem.

2. Šā panta 1. punktā minētā informācija ir pieejama elektroniskā veidā, un tā paliek pieejama un vajadzības gadījumā tiek atjaunināta vismaz līdz attiecīgā Eiropas kiberdrošības sertifikāta vai ES atbilstības apliecinājuma termiņa beigām.

56. pants

Kiberdrošības sertifikācija

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

2. Kiberdrošības sertifikācija ir brīvprātīga, ja vien Savienības vai dalībvalsts tiesību aktos nav norādīts citādi.

3. 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 pienācīgi augstu IKT produktu, IKT pakalpojumu un IKT procesu 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 novērtēšanu iznākumu, nosaka tos kādas esošas sertifikācijas shēmas aptvertus IKT produktus, IKT pakalpojumus un IKT procesus, uz kuriem jāattiecina obligāta sertificēšanas shēma.

Komisija prioritārā kārtā pievērš uzmanību nozarēm, kas uzskaitītas Direktīvas (ES) 2016/1148 II pielikumā, un tās novērtē vēlākais divus gadus pēc pirmās Eiropas kiberdrošības sertifikācijas shēmas pieņemšanas.

Sagatavojot novērtējumu, Komisija:

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

b) ņem vērā to, vai pastāv un tiek īstenoti attiecīgi dalībvalsts un trešās valsts tiesību akti;

c) veic atklātu, pārredzamu un iekļaujošu apspriešanās procesu ar visām attiecīgajām ieinteresētajām personām un dalībvalstīm;

d) ņem vērā jebkurus īstenošanas termiņus, pārejas pasākumus un periodus, jo īpaši attiecībā uz pasākumu iespējamo ietekmi uz IKT produktu, IKT pakalpojumu un IKT procesu ražotājiem vai sniedzējiem, tostarp MVU;

e) ierosina ātrāko un efektīvāko veidu, kādā īstenojama pāreja no brīvprātīgas un obligātu sertifikācijas shēmu.

4. Saskaņā ar šo pantu Eiropas kiberdrošības sertifikātu ar apliecinājuma līmeni "pamata" vai "būtisks" izdod 60. pantā minētās atbilstības novērtēšanas struktūras, pamatojoties uz kritērijiem, kuri iekļauti Komisijas saskaņā ar 49. pantu pieņemtajā Eiropas kiberdrošības sertifikācijas shēmā.

5. Atkāpjoties no 4. punkta, pienācīgi pamatotos gadījumos Eiropas kiberdrošības sertifikācijas shēma var paredzēt, ka atbilstīgi minētajai shēmai izveidotus Eiropas kiberdrošības sertifikātus izdod tikai publiska struktūra. Šāda struktūra ir viena no tālāk minētajām:

a) valsts kiberdrošības sertifikācijas iestāde, kā minēts 58. panta 1. punktā; vai

b) publiska struktūra, kas ir akreditēta kā atbilstības novērtēšanas struktūra saskaņā ar 60. panta 1. punktu.

6. Ja Eiropas kiberdrošības sertifikācijas shēmā, kas pieņemta, ievērojot 49. pantu, tiek prasīts apliecinājuma līmenis "augsts", Eiropas kiberdrošības sertifikātu saskaņā ar minēto shēmu izdod tikai valsts kiberdrošības sertifikācijas iestāde vai – turpmāk minētajos gadījumos – atbilstības novērtēšanas struktūra:

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

b) pamatojoties uz valsts kiberdrošības sertifikācijas iestādes vispārēju deleģējumu atbilstības novērtēšanas struktūrai izdot šādus Eiropas kiberdrošības sertifikātus.

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

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

9. Eiropas kiberdrošības sertifikātus izdod uz laikposmu, kas paredzēts Eiropas kiberdrošības sertifikācijas shēmā, un tos var atjaunot ar noteikumu, ka joprojām ir ievērotas attiecīgās prasības.

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

57. pants

Valsts kiberdrošības sertifikācijas shēmas un sertifikāti

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

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

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

4. Lai izvairītos no iekšējā tirgus sadrumstalotības, dalībvalstis par iniciatīvām izstrādāt jaunas valsts kiberdrošības sertifikācijas shēmas informē Komisiju un *ECCG*.

58. pants

Valsts kiberdrošības sertifikācijas iestādes

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

2. Katra dalībvalsts informē Komisiju par izraudzītajām valsts kiberdrošības sertifikācijas iestādēm. Ja kāda dalībvalsts izraugās vairāk nekā vienu iestādi, tā informē Komisiju arī par uzdevumiem, kuri uzticēti katrai no minētajām iestādēm.

3. Neskarot 56. panta 5. punkta a) apakšpunktu un 56. panta 6. punktu, katra valsts kiberdrošības sertifikācijas iestāde organizatoriskās, juridiskās struktūras un lēmumu pieņemšanas ziņā ir neatkarīga no tās uzraudzītajiem subjektiem.

4. Dalībvalstis nodrošina, ka valsts kiberdrošības sertifikācijas iestāžu darbības, kas saistītas ar 56. panta 5. punkta a) apakšpunktā un 56. panta 6. punktā minēto Eiropas kiberdrošības sertifikātu izdošanu, tiek strikti nodalītas no to šajā pantā izklāstītajām uzraudzības darbībām un ka minētās darbības tiek veiktas neatkarīgi viena no otras.

5. Dalībvalstis nodrošina, ka valsts kiberdrošības sertifikācijas iestāžu rīcībā ir pietiekami līdzekļi, lai tās varētu īstenot savas pilnvaras un efektīvi un rezultatīvi veikt savus uzdevumus.

6. Lai šīs regulas īstenošana būtu rezultatīva, ir lietderīgi noteikt, ka valsts kiberdrošības sertifikācijas iestādes aktīvi, efektīvi, rezultatīvi un drošā veidā piedalās *ECCG*.

7. Valsts kiberdrošības sertifikācijas iestādes:

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 un IKT procesu atbilstību to attiecīgajās teritorijās izdoto Eiropas kiberdrošības sertifikātu prasībām, un nodrošina to izpildi;

b) pārrauga to IKT produktu, IKT pakalpojumu vai IKT procesu ražotāju vai sniedzēju atbilstību un nodrošina, lai tiktu izpildīti viņu pienākumi, kuri veic uzņēmējdarbību šo iestāžu attiecīgajās teritorijās un kuri veic atbilstības pašnovērtēšanu, jo īpaši pārrauga šādu ražotāju vai sniedzēju atbilstību un nodrošina to viņu pienākumu izpildi, kas izklāstīti 53. panta 2. un 3. punktā un attiecīgajā Eiropas kiberdrošības sertifikācijas shēmā;

c) šīs regulas nolūkos, neskarot 60. panta 3. punktu, aktīvi palīdz un sniedz atbalstu valsts akreditācijas struktūrām atbilstības novērtēšanas struktūru darbību pārraudzībā un uzraudzībā;

d) pārrauga un uzrauga 56. panta 5. punktā minēto publisko struktūru darbības;

e) attiecīgā gadījumā – izsniedz atļauju atbilstības novērtēšanas struktūrām saskaņā ar 60. panta 3. punktu un ierobežo, aptur vai atsauc esošu atļauju, ja atbilstības novērtēšanas struktūras pārkāpj šīs regulas prasības;

f) izskata fizisku vai juridisku personu sūdzības saistībā ar valsts kiberdrošības sertifikācijas iestāžu vai – saskaņā ar 56. panta 6. punktu – atbilstības novērtēšanas struktūru izdotiem Eiropas kiberdrošības sertifikātiem vai saistībā ar ES atbilstības apliecinājumiem, kas izdoti saskaņā ar 53. pantu, un pienācīgā mērā izmeklē šādu sūdzību priekšmetu un samērīgā termiņā informē sūdzības iesniedzēju par lietas virzību un izmeklēšanas rezultātiem;

g) sniedz *ENISA* un *ECCG* gada kopsavilkuma ziņojumu par darbību, kas veikta saskaņā ar šā punkta b), c) un d) apakšpunktu vai saskaņā ar 8. punktu;

h) sadarbojas ar citām valsts kiberdrošības sertifikācijas iestādēm vai citām publiskām iestādēm, piemēram, daloties informācijā par IKT produktu, IKT pakalpojumu un IKT procesu iespējamu neatbilstību šīs regulas vai konkrētu Eiropas kiberdrošības sertifikācijas shēmu prasībām; un

i) uzrauga būtiskas norises kiberdrošības sertifikācijas jomā.

8. Katrai valsts kiberdrošības sertifikācijas iestādei ir vismaz šādas pilnvaras:

a) pieprasīt, lai atbilstības novērtēšanas struktūras, Eiropas kiberdrošības sertifikātu turētāji un ES atbilstības apliecinājumu izdevēji sniegtu informāciju, ko tā pieprasījusi savu uzdevumu izpildei;

b) atbilstības novērtēšanas struktūrās, Eiropas kiberdrošības sertifikātu turētāju un ES atbilstības apliecinājumu izdevēju struktūrās veikt izmeklēšanas, izmantojot revīzijas, lai pārbaudītu to atbilstību šai sadaļai;

c) saskaņā ar valsts tiesību aktiem veikt atbilstošus pasākumus, lai nodrošinātu, ka atbilstības novērtēšanas struktūras, Eiropas kiberdrošības sertifikātu turētāji un ES atbilstības apliecinājumu izdevēji atbilst šai regulai vai Eiropas kiberdrošības sertifikācijas shēmai;

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

e) saskaņā ar valsts tiesību aktiem atsaukt Eiropas kiberdrošības sertifikātus, kurus izdevušas valsts kiberdrošības sertifikācijas iestādes vai – saskaņā ar 56. panta 6. punktu – atbilstības novērtēšanas struktūras, ja šādi sertifikāti neatbilst šai regulai vai Eiropas kiberdrošības sertifikācijas shēmai;

f) saskaņā ar valsts tiesību aktiem piemērot sankcijas, kā paredzēts 65. pantā, un nekavējoties pieprasīt izbeigt pārkāpumus saistībā ar šajā regulā noteikto pienākumu neievērošanu.

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 un IKT procesu kiberdrošību.

59. pants

Salīdzinošā izvērtēšana

1. Lai visā Savienībā panāktu līdzvērtīgus standartus attiecībā uz Eiropas kiberdrošības sertifikātiem un ES atbilstības apliecinājumiem, valstu kiberdrošības sertifikācijas iestādēm veic salīdzinošo izvērtēšanu.

2. Salīdzinošo izvērtēšanu veic, pamatojoties uz pareiziem un pārredzamiem vērtēšanas kritērijiem un procedūrām, jo īpaši attiecībā uz strukturālām, cilvēkresursu un procesa prasībām, konfidencialitāti un sūdzībām.

3. Salīdzinošā izvērtēšanā vērtē:

a) attiecīgā gadījumā – to, vai valsts kiberdrošības sertifikācijas iestāžu darbības, kas saistītas ar 56. panta 5. punkta a) apakšpunktā un 56. panta 6. punktā minēto Eiropas kiberdrošības sertifikātu izdošanu, tiek strikti nodalītas no to uzraudzības darbībām, kas izklāstītas 58. pantā, un vai minētās darbības tiek veiktas neatkarīgi viena no otras;

b) procedūras, kas attiecas uz noteikumu, ar kuriem pārrauga IKT produktu, IKT pakalpojumu un IKT procesu atbilstību Eiropas kiberdrošības sertifikātiem, uzraudzību un to izpildes nodrošināšanu, ievērojot 58. panta 7. punkta a) apakšpunktu;

c) procedūras, kas attiecas uz IKT produktu, IKT pakalpojumu vai IKT procesu ražotāju vai sniedzēju pienākumu pārraudzību un to izpildes nodrošināšanu, ievērojot 58. panta 7. punkta b) apakšpunktu;

d) procedūras, kas attiecas uz atbilstības novērtēšanas struktūru darbību pārraudzību, pilnvarošanu un uzraudzību;

e) attiecīgā gadījumā – to, vai to iestāžu vai struktūru darbiniekiem, kuras izdod sertifikātus par apliecinājuma līmeni "augsts", ievērojot 56. panta 6. punktu, ir pienācīgu lietpratību.

4. Salīdzinošo izvērtēšanu veic vismaz divas citu dalībvalstu valsts kiberdrošības sertifikācijas iestādes un Komisija, un to veic vismaz reizi piecos gados. Salīdzinošajā izvērtēšanā var piedalīties *ENISA*.

5. Komisija var pieņemt īstenošanas aktus, ar kuriem izveido salīdzinošās izvērtēšanas plānu vismaz piecu gadu laikposmam, nosakot salīdzinošās izvērtēšanas grupas sastāva izveides kritērijus, salīdzinošajā izvērtēšanā izmantojamo metodoloģiju, laika grafiku, biežumu un citus ar to saistītus uzdevumus. Pieņemot minētos īstenošanas aktus, Komisija pienācīgi ņem vērā *ECCG* apsvērumus. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 66. panta 2. punktā.

6. Salīdzinošās izvērtēšanas iznākumus izskata *ECCG*, kas sagatavo kopsavilkumus, kurus var darīt publiski pieejamus, un kas vajadzības gadījumā izdod pamatnostādnes un ieteikumus par darbībām vai pasākumiem, kas jāveic attiecīgajiem subjektiem.

60. pants

Atbilstības novērtēšanas struktūras

1. Atbilstības novērtēšanas struktūru akreditāciju veic valsts akreditācijas struktūras, kuras izraugās saskaņā ar Regulu (EK) Nr. 765/2008. Šādu akreditāciju piešķir tikai tad, ja atbilstības novērtēšanas struktūra atbilst šīs regulas pielikumā izklāstītajām prasībām.

2. Ja Eiropas kiberdrošības sertifikātu ir izdevusi valsts kiberdrošības sertifikācijas iestāde, ievērojot 56. panta 5. punkta a) apakšpunktu un 56. panta 6. punktu, valsts kiberdrošības sertifikācijas iestādes sertifikācijas struktūru akreditē kā atbilstības novērtēšanas struktūru, ievērojot šā panta 1. punktu.

3. Ja Eiropas kiberdrošības sertifikācijas shēmās ir izklāstītas specifiskas vai papildu prasības, ievērojot 54. panta 1. punkta f) apakšpunktu, valsts kiberdrošības sertifikācijas iestāde var pilnvarot veikt uzdevumus šādu shēmu ietvaros vienīgi tās atbilstības novērtēšanas struktūras, kuras atbilst minētajām prasībām.

4. Šā panta 1. punktā minēto akreditāciju atbilstības novērtēšanas struktūrām piešķir uz laikposmu, kas nav ilgāks par pieciem gadiem, un to var atjaunot ar tādiem pašiem nosacījumiem, ja atbilstības novērtēšanas struktūra joprojām atbilst šajā pantā izklāstītajām prasībām. Ja akreditācijas nosacījumi nav vai vairs netiek izpildīti vai ja atbilstības novērtēšanas struktūra pārkāpj šo regulu, valsts akreditācijas struktūras saprātīgā termiņā veic visus atbilstošos pasākumus, lai ierobežotu, apturētu vai atsauktu atbilstības novērtēšanas struktūrai piešķirtu akreditāciju, ievērojot 1. punktu.

61. pants

Paziņošana

1. Par katru Eiropas kiberdrošības sertifikācijas shēmu valsts kiberdrošības sertifikācijas iestādes Komisijai paziņo atbilstības novērtēšanas struktūras, kas ir akreditētas, un attiecīgā gadījumā, ievērojot 60. panta 3. punktu, pilnvarotas izsniegt Eiropas kiberdrošības sertifikātus konkrētos apliecinājuma līmeņos, kā minēts 52. pantā. Valsts kiberdrošības sertifikācijas iestādes bez liekas kavēšanās paziņo Komisijai par tajā vēlāk veiktām izmaiņām.

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

3. Ja Komisija paziņojumu saņem pēc tam, kad ir beidzies 2. punktā minētais laikposms, tā divu mēnešu laikā no minētā paziņojuma saņemšanas dienas *Eiropas Savienības Oficiālajā Vēstnesī* publicē grozījumus to atbilstības novērtēšanas struktūru sarakstā, par kurām paziņots.

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

5. Komisija var pieņemt īstenošanas aktus, lai noteiktu apstākļus, formātus un procedūras, kas jāievēro saistībā ar šā panta 1. punktā minēto paziņošanu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 66. panta 2. punktā.

62. pants

Eiropas Kiberdrošības sertifikācijas grupa

1. Izveido Eiropas Kiberdrošības sertifikācijas grupu (“*ECCG*”).

2. *ECCG* veido valstu kiberdrošības sertifikācijas iestāžu pārstāvji vai citu attiecīgo valsts iestāžu pārstāvji. *ECCG* pārstāvis nepārstāv vairāk kā divas dalībvalstis.

3. Ieinteresētās personas un attiecīgās trešās personas var tikt uzaicinātas apmeklēt *ECCG* sanāksmes un piedalīties tās darbā.

4. *ECCG* ir šādi uzdevumi:

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

b) palīdzēt, dot padomus *ENISA* un sadarboties ar to saistībā ar kandidātshēmas izveidošanu, ievērojot 49. pantu;

c) pieņemt atzinumu par *ENISA* izveidotajām kandidātshēmām, ievērojot 49. pantu;

d) pieprasīt *ENISA* izveidot kandidātshēmas, ievērojot 48. panta 2. punktu;

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

f) izvērtēt attiecīgās attīstības tendences kiberdrošības sertifikācijas jomā un īstenot informācijas un labas prakses apmaiņu kiberdrošības sertifikācijas shēmu jautājumos;

g) sekmēt valstu kiberdrošības sertifikācijas iestāžu sadarbību atbilstīgi šai sadaļai, izmantojot spēju veidošanu un informācijas apmaiņu, jo īpaši ieviešot metodes efektīvai informācijas apmaiņai kiberdrošības sertifikācijas aspektos;

h) atbalstīt salīdzinošās izvērtēšanas mehānismu īstenošanai saskaņā ar Eiropas kiberdrošības sertifikācijas shēmā paredzētajiem noteikumiem, ievērojot 54. panta 1. punkta u) apakšpunktu;

i) veicināt Eiropas kiberdrošības sertifikācijas shēmu saskaņošanu ar starptautiski atzītiem standartiem, cita starpā pārskatot esošās Eiropas kiberdrošības sertifikācijas shēmas un attiecīgā gadījumā iesakot *ENISA* sadarboties ar attiecīgām starptautiskajām standartizācijas organizācijām, lai novērstu trūkumus vai nepilnības pieejamajos starptautiski atzītajos standartos.

5. Komisija, kurai palīdz *ENISA*, vada *ECCG* sanāksmes un saskaņā ar 8. panta 1. punkta e) apakšpunktu Komisija nodrošina *ECCG* sekretariātu.

63. pants

Tiesības iesniegt sūdzību

1. Fiziskām un juridiskām personām ir tiesības iesniegt sūdzību Eiropas kiberdrošības sertifikāta izdevējam vai – ja sūdzība attiecas uz Eiropas kiberdrošības sertifikātu, ko izdevusi kāda atbilstības novērtēšanas struktūra, rīkojoties saskaņā ar 56. panta 6. punktu,– attiecīgajai valsts kiberdrošības sertifikācijas iestādei.

2. Iestāde vai struktūra, kurai ir iesniegta sūdzība, informē sūdzības iesniedzēju par procesa virzību un pieņemto lēmumu, un par tiesībām uz efektīvu tiesību aizsardzību tiesā, kas minētas 64. pantā.

64. pants

Tiesības uz efektīvu tiesību aizsardzību tiesā

1. Neatkarīgi no jebkādas administratīvas vai citas ārpustiesas tiesību aizsardzības fiziskām un juridiskām personām ir tiesības uz efektīvu tiesību aizsardzību tiesā attiecībā uz:

a) 63. panta 1. punktā minētas iestādes vai struktūras pieņemtiem lēmumiem, tostarp – attiecīgā gadījumā – saistībā ar Eiropas kiberdrošības sertifikāta nepareizu izdošanu, neizdošanu vai atzīšanu, kura turētāji ir minētās fiziskās un juridiskās personas;

b) bezdarbību saistībā ar sūdzību, kas iesniegta 63. panta 1. punktā minētā iestādē vai struktūrā.

2. Process, ievērojot šo pantu, notiek tās dalībvalsts tiesās, kurā atrodas iestāde vai struktūra, attiecībā uz kuru notiek tiesību aizsardzības tiesā process.

65. pants

Sankcijas

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

IV SADAĻA

NOBEIGUMA NOTEIKUMI

66. pants

Komiteju procedūra

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

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

67. pants

Novērtēšana un pārskatīšana

1. Līdz 2024. gada 28. jūnijam un pēc tam reizi piecos gados Komisija novērtē *ENISA* un tās darba prakses ietekmi, rezultativitāti un efektivitāti, kā arī iespējamo vajadzību mainīt *ENISA* pilnvaras un jebkuru šādu izmaiņu finansiālo ietekmi. Novērtējumā ņem vērā visu atgriezenisko informāciju, kas sniegta *ENISA*, atbildot uz tās darbībām. Ja Komisija uzskata, ka *ENISA* turpmāka darbība vairs nav pamatota, ņemot vērā tai izvirzītos mērķus, piešķirtās pilnvaras un noteiktos uzdevumus, Komisija var ierosināt grozīt šīs regulas noteikumus, kuri attiecas uz *ENISA*.

2. Novērtējumā izvērtē arī šīs regulas III sadaļas noteikumu ietekmi, efektivitāti un rezultativitāti, raugoties uz mērķiem, kas paredz nodrošināt pienācīgi augstu IKT produktu, IKT pakalpojumu un IKT procesu 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 un IKT procesu nonākšanu Savienības tirgū.

4. Līdz 2024. gada 28. jūnijam un katrus piecus gadus pēc tam Komisija ziņojumu par novērtējumu kopā ar saviem secinājumiem nosūta Eiropas Parlamentam, Padomei un Administratīvajai padomei. Minētā ziņojuma konstatējumus publisko.

68. pants

Atcelšana un pēctecība

1. Regula (ES) Nr. 526/2013 tiek atcelta no 2019. gada 27. jūnija.

2. Atsauces uz Regulu (ES) Nr. 526/2013 un uz ar minēto regulu izveidoto *ENISA* uzskata par atsaucēm uz šo regulu un ar šo regulu izveidoto *ENISA*.

3. Ar šo regulu izveidotā *ENISA* pārņem visas ar Regulu (ES) Nr. 526/2013 izveidotās *ENISA* īpašumtiesības, nolīgumus, juridiskos pienākumus, darba līgumus, finanšu saistības un pienākumus. Visi Administratīvās padomes un Valdes lēmumi, kas pieņemti saskaņā ar Regulu (ES) Nr. 526/2013, paliek spēkā ar noteikumu, ka tie atbilst šai regulai.

4. *ENISA* izveido uz nenoteiktu laikposmu no 2019. gada 27. jūnija.

5. Izpilddirektors, kas iecelts saskaņā ar Regulas (ES) Nr. 526/2013 24. panta 4. punktu, paliek amatā un pilda izpilddirektora pienākumus, kā minēts šīs regulas 20. pantā, atlikušajā izpilddirektora pilnvaru termiņā. Pārējie izpilddirektora līguma nosacījumi paliek nemainīgi.

6. Administratīvās padomes locekļi un viņu aizstājēji, kas iecelti, ievērojot Regulas (ES) Nr. 526/2013 6. pantu, paliek amatā un pilda Administratīvās padomes funkcijas, kā minēts šīs regulas 15. pantā, atlikušajā viņu pilnvaru termiņā.

69. pants

Stāšanās spēkā

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

2. Regulas 58., 60., 61., 63., 64. un 65. pantu piemēro no 2021. gada 28. jūnija.

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

Strasbūrā, 2019. gada 17. aprīlī

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*
A. TAJANI	G. CIAMBA

PIELIKUMS

PRASĪBAS, KAS JĀIZPILDA ATBILSTĪBAS NOVĒRTĒŠANAS STRUKTŪRĀM

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

1. Atbilstības novērtēšanas struktūra ir izveidota saskaņā ar valsts tiesību aktiem, un tai piemīt tiesībsubjektība.

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

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

4. Atbilstības novērtēšanas struktūras, to augstākā vadība un personas, kas atbild par atbilstības novērtēšanas uzdevumu izpildi, nav ne vērtējamā IKT produkta, IKT pakalpojuma vai IKT procesa izstrādātājs, ražotājs, piegādātājs, uzstādītājs, pircējs, īpašnieks, lietotājs vai apkalpotājs, ne minēto personu pilnvarots pārstāvis. Minētais aizliegums neliedz izmantot vērtētos IKT produktus, ja tie nepieciešami atbilstības novērtēšanas struktūras darbībai, vai izmantot šādus IKT produktus personiskām vajadzībām.

5. Atbilstības novērtēšanas struktūras, to augstākā vadība un personas, kas atbild par atbilstības novērtēšanas uzdevumiem, nav tieši saistīti ar vērtējamo IKT produktu, IKT pakalpojumu vai IKT procesu izstrādi, ražošanu vai konstruēšanu, tirdzniecību, uzstādīšanu, lietošanu vai apkalpošanu, kā arī nepārstāv minētajās darbībās iesaistītās personas. Atbilstības novērtēšanas struktūras, to augstākā vadība un personas, kas atbild par atbilstības novērtēšanas uzdevumiem neiesaistās darbībās, kas var būt pretrunā to spriedumu neatkarībai vai godprātībai saistībā ar savām atbilstības novērtēšanas darbībām. Minētais aizliegums īpaši attiecas uz konsultatīvajiem pakalpojumiem.

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

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

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

9. Atbilstības novērtēšanas iestāde spēj veikt visus saskaņā ar šo regulu piešķirtos atbilstības novērtēšanas uzdevumus neatkarīgi no tā, vai tos veic pati vai tās uzdevumā kāds cits uz tās atbildību. Jebkuru apakšlīgumu slēgšanu vai konsultēšanos ar ārējiem darbiniekiem pienācīgi dokumentē, tajā neiesaista starpniekus un par to slēdz rakstisku vienošanos 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 vai IKT procesu veidam, kategorijai un apakškategorijai vienmēr ir vajadzīgie:

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

    b) to procedūru apraksti, saskaņā ar kurām veicama atbilstības novērtēšana, lai nodrošinātu minēto procedūru pārredzamību un iespēju tās atkārtot. Tai ir ieviesta piemērota politika un procedūras, kur uzdevumi, kurus tā veic saskaņā ar 61. pantu paziņotās struktūras statusā, ir nodalīti no citām tās darbībām;

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

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

12. Personām, kuri atbild par atbilstības novērtēšanas darbībām, ir:

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

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

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

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

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

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

15. Tiek apdrošināta atbilstības novērtēšanas struktūru civiltiesiskā atbildība, ja vien atbildību saskaņā ar valsts tiesību aktiem neuzņemas dalībvalsts vai dalībvalsts pati tieši neatbild 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, kas skar visu 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 jāizpauž saskaņā ar Savienības vai dalībvalstu tiesību aktiem, kuri šīm personām ir jāievēro, un izņemot attiecībā uz to dalībvalstu kompetentajām iestādēm, kurās tiek veiktas tās darbības. Īpašumtiesības tiek aizsargātas. Attiecībā uz šā punkta prasībām atbilstības novērtēšanas struktūra ievieš dokumentētas procedūras.

17. Izņemot 16. punktu, šī pielikuma 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 Regulā (EK) Nr. 765/2008 attiecībā uz to atbilstības novērtēšanas struktūru akreditāciju, kas veic IKT produktu, IKT pakalpojumu vai IKT procesu sertifikāciju.

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