UREDBA (EU) 2019/881EUROPSKOG PARLAMENTA I VIJEĆA

od 17. travnja 2019.

o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti)

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov Članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora ([1]),

uzimajući u obzir mišljenje Odbora regija ([2]),

u skladu s redovnim zakonodavnim postupkom ([3]),

budući da:

(1) Mrežni i informacijski sustavi i elektroničke komunikacijske mreže i usluge imaju ključnu ulogu u društvu i postali su okosnica gospodarskog rasta. Na informacijskoj i komunikacijskoj tehnologiji (IKT) temelje se složeni sustavi kojima se podupiru svakodnevne društvene aktivnosti, osigurava neprekinuto funkcioniranje naših gospodarstava u ključnim sektorima poput zdravstva, energetike, financija i prometa te se posebno podupire funkcioniranje unutarnjeg tržišta.

(2) Građani, organizacije i poduzeća u cijeloj Uniji sada se u znatnoj mjeri koriste mrežnim i informacijskim sustavima. Digitalizacija i povezivost postaju ključne značajke sve većeg broja proizvoda i usluga, a pojavom interneta stvari (IoT) očekuje se da će se u Uniji tijekom sljedećeg desetljeća upotrebljavati iznimno velik broj povezanih digitalnih uređaja. Iako se s internetom povezuje sve veći broj uređaja, pri njihovom dizajnu se ne vodi dovoljno računa o sigurnosti i otpornosti, što dovodi do nedostatne kibersigurnosti. U tom kontekstu, zbog ograničene uporabe certifikacije, pojedinačni korisnici, organizacije i poduzeća nemaju dovoljno informacija o kibersigurnosnim značajkama IKT proizvoda i IKT usluga, što smanjuje povjerenje u digitalna rješenja. Mrežni i informacijski sustavi imaju sposobnost podupiranja svih aspekata naših života i poticanja gospodarskog rasta Unije. Okosnica su za ostvarenje jedinstvenog digitalnog tržišta.

(3) Rast digitalizacije i povezivosti dovode do većih kibersigurnosnih rizika, zbog čega je društvo u cjelini osjetljivije na kiberprijetnje, a pojedinci se suočavaju sa sve većim opasnostima, uključujući ranjive osobe kao što su djeca. Kako bi se ti rizici ublažili, treba poduzeti sve nužne mjere za poboljšanje kibersigurnosti u Uniji s ciljem bolje zaštite od kiberprijetnji mrežnih i informacijskih sustava, telekomunikacijskih mreža, digitalnih proizvoda, usluga i uređaja kojima se koriste građani, organizacije i poduzeća, od malih i srednjih poduzeća (MSP-ovi), kako su definirana u Preporuci Komisije 2003/361/EZ ([4]) do operatora ključnih infrastruktura.

([1]) SL C 227, 28.6.2018., str. 86.
([2]) SL C 176, 23.5.2018., str. 29.
([3]) Stajalište Europskog parlamenta od 12. ožujka 2019. (još nije objavljeno u Službenom listu) i odluka Vijeća od 9. travnja 2019.
([4]) Preporuka Komisije od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

(4) Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA), osnovana Uredbom (EU) br. 526/2013. Europskog parlamenta i Vijeća ([5]) stavljanjem na raspolaganje relevantnih informacija javnosti doprinosi razvoju kibersigurnosnog sektora u Uniji, a posebice MSP-ova te novoosnovanih poduzeća. ENISA bi trebala nastojati ostvariti bližu suradnju sa sveučilištima i istraživačkim subjektima kako bi se doprinijelo smanjenju ovisnost o kibersigurnosnim proizvodima i uslugama izvan Unije i ojačalo opskrbne lance unutar Unije.

(5) Kibernapadi su sve češći te je potrebna snažnija obrana povezanoga gospodarstva i društva koje je osjetljivije na kiberprijetnje i napade. Međutim, dok su kibernapadi često prekogranični, nadležnost i politički odgovori nadležnih tijela za kibersigurnost i za izvršavanje zakonodavstva uglavnom su nacionalni. Veliki incidenti mogli bi uzrokovati prekid u pružanju ključnih usluga u cijeloj Uniji. Zbog toga su potrebni učinkoviti i koordinirani odgovori te upravljanje krizama na razini Unije, koji se temelje na ciljanim politikama i opsežnijim instrumentima za europsku solidarnost i uzajamnu pomoć. Nadalje, za oblikovatelje politika, industriju i korisnike važno je redovito ocjenjivanje stanja kibersigurnosti i otpornosti u Uniji na temelju pouzdanih podataka Unije i sustavno predviđanje budućeg razvoja, izazova i opasnosti na razini Unije i na globalnoj razni.

(6) Zbog sve većih kibersigurnosnih izazova s kojima se Unija suočava potrebno je donijeti sveobuhvatan skup mjera koje bi se temeljile na prethodnom djelovanju Unije i kojima bi se poticali ciljevi koji se uzajamno podupiru. Ti ciljevi uključuju daljnje povećanje sposobnosti i spremnosti država članica i poduzeća te poboljšanje suradnje, razmjene informacija i koordinacije među državama članicama i institucijama, tijelima, uredima i agencijama Unije. Nadalje, s obzirom na to da kiberprijetnje ne poznaju granice, trebalo bi povećati sposobnosti na razini Unije kojima bi se mogla dopuniti djelovanja država članica, posebno u slučajevima velikih prekograničnih incidenata i kriza uz istodobno vođenje računa o važnosti održavanja i daljnjeg poboljšavanja nacionalnih sposobnosti za odgovor na kiberprijetnje svih razmjera.

(7) Potrebno je također uložiti dodatne napore u podizanje osviještenosti građana, organizacija i poduzeća o pitanjima kibersigurnosti. Nadalje, budući da incidenti narušavaju povjerenje u pružatelje digitalnih usluga i u samo jedinstveno digitalno tržište, posebno u redovima potrošača, povjerenje bi trebalo dodatno ojačati transparentnom ponudom informacija o razini sigurnosti IKT proizvoda, IKT usluga i IKT procesa kojima se ističe da čak i visoka razina kibersigurnosne certifikacije nije jamstvo da su IKT proizvod, IKT usluga ili IKT proces potpuno sigurni. Jačanje povjerenja može se olakšati certifikacijom na razini Unije kojom će se osigurati zajednički kibersigurnosni zahtjevi i kriteriji za evaluaciju na svim nacionalnim tržištima i u svim sektorima.

(8) Kibersigurnost nije samo problem povezan s tehnologijom, već je za njega od jednake važnosti ljudsko ponašanje. Stoga bi trebalo snažno promicati „kiberhigijenu”, odnosno jednostavne, rutinske mjere kojima se, ako ih građani, organizacije i poduzeća redovito provode, na najmanju moguću mjeru smanjuje njihova izloženost rizicima od kiberprijetnji.

(9) Radi jačanja struktura Unije u području kibersigurnosti važno je održati i razviti sposobnosti država članica za sveobuhvatan odgovor na kiberprijetnje, što obuhvaća prekogranične incidente.

(10) Poduzeća i pojedinačni potrošači trebali bi imati točne informacije o tome do koje su jamstvene razine certificirani njihovi IKT proizvodi, IKT usluge i IKT procesi. Istodobno, nijedan IKT proizvod, IKT usluga ili IKT proces nije u potpunosti kibersiguran i potrebno je promicati i prioritizirati osnovna pravila kiberhigijene. S obzirom na sve veću dostupnost uređaja IoT-a postoji niz dobrovoljnih mjera koje privatni sektor može poduzeti kako bi ojačao povjerenje u sigurnost IKT proizvoda, IKT usluga i IKT procesa.

(11) Moderni IKT proizvodi i sustavi često se integriraju i oslanjaju se na jednu ili više tehnologija i komponenti treće strane, kao što su softverski moduli, knjižnice ili aplikacijska programska sučelja. To oslanjanje, koje se naziva „ovisnost”, moglo bi predstavljati dodatne kibersigurnosne rizike jer bi ranjivosti prisutne u komponentama treće strane mogle utjecati i na sigurnost IKT proizvoda, IKT usluga i IKT procesa. U mnogim slučajevima utvrđivanje i dokumentiranje takvih ovisnosti omogućuje krajnjim korisnicima IKT proizvoda, IKT usluga i IKT procesa da poboljšaju svoje aktivnosti upravljanja kibersigurnosnim rizicima poboljšanjem, primjerice, korisničkih postupaka upravljanja ranjivostima i otklanjanja ranjivosti u području kibersigurnosti.

([5]) Uredba (EU) br. 526/2013 Europskog parlamenta i Vijeća od 21. svibnja 2013. o Agenciji Europske unije za mrežnu i informacijsku sigurnost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004 (SL L 165, 18.6.2013., str. 41.).

(12) Trebalo bi poticati organizacije, proizvođače ili pružatelje usluga koji su uključeni u oblikovanje i razvoj IKT proizvoda, IKT usluga i IKT procesa da u najranijim fazama oblikovanja i razvoja provedu mjere radi zaštite sigurnosti tih proizvoda, procesa i usluga u najvećoj mogućoj mjeri, na način da se pretpostavlja pojava napada te da se njihov učinak očekuje i smanjuje na najmanju moguću mjeru („integrirana sigurnost"). Sigurnosti bi trebalo jamčiti tijekom cijelog životnog vijeka IKT proizvoda, IKT usluge i IKT procesa i to tako da se postupci oblikovanja i razvoja stalno razvijaju s ciljem smanjenja štete od zlonamjernog iskorištavanja.

(13) Poduzeća, organizacije i javni sektor trebali bi konfigurirati IKT proizvode, IKT procese ili IKT usluge koje osmišljavaju tako da se osigura viši stupanj sigurnosti, što bi prvom korisniku omogućilo da dobije zadanu konfiguraciju s najsigurnijim mogućim postavkama („zadana sigurnost") čime bi se smanjilo opterećenje za korisnike da na odgovarajući način moraju konfigurirati IKT proizvod, IKT uslugu i IKT procesd. Zadana sigurnost ne bi trebala zahtijevati opsežnu konfiguraciju ni specifično tehničko razumijevanje ili neintuitivno ponašanje korisnika već bi, ako je ugrađena, trebala funkcionirati jednostavno i pouzdano. Ako se na pojedinačnoj osnovi analizom rizika i upotrebljivosti pokaže da takve zadane postavke nisu ostvarive, korisnike bi trebalo upozoriti da se odluče za najsigurniju postavku.

(14) Uredbom (EZ) br. 460/2004 Europskog parlamenta i Vijeća ([6]) osnovana je ENISA za potrebe doprinosa ciljevima osiguravanja visoke i učinkovite razine mrežne i informacijske sigurnosti u Uniji te razvoja kulture mrežne i informacijske sigurnosti u korist građana, potrošača, poduzeća i javnih uprava. Uredbom (EZ) br. 1007/2008 Europskog parlamenta i Vijeća ([7]) produljen je mandat ENISA-e do ožujka 2012. Uredbom (EU) br. 580/2011 Europskog parlamenta i Vijeća ([8]) dodatno je produljen mandat ENISA-e do 13. rujna 2013. Uredbom (EU) br. 526/2013 mandat ENISA-e produljen je do 19. lipnja 2020.

(15) Unija je već poduzela važne korake kako bi osigurala kibersigurnost i povećala povjerenje u digitalne tehnologije. Godine 2013. donesena je Strategija Europske unije za kibersigurnost kako bi se usmjerio politički odgovor Unije na kiberprijetnje i kiberrizike. S ciljem bolje zaštite građana na internetu Unija je 2016. donijela prvi zakonodavni akt u području kibersigurnosti u obliku Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća ([9]). Direktivom (EU) 2016/1148 utvrđuju se zahtjevi u pogledu nacionalnih sposobnosti u području kibersigurnosti, uspostavljeni su prvi mehanizmi za jačanje strateške i operativne suradnje među državama članicama i uvedene su obveze u pogledu sigurnosnih mjera i obavijesti o incidentima u sektorima koji su od ključne važnosti za gospodarstvo i društvo, kao što su energetika, promet, opskrba pitkom vodom i njezina distribucija, bankarstvo, infrastruktura financijskog tržišta, zdravstvena skrb, digitalna infrastruktura i pružatelji ključnih digitalnih usluga (tražilice, usluge računalstva u oblaku i internetska tržišta).

ENISA je dobila ključnu ulogu u podupiranju provedbe te direktive. Nadalje, djelotvorna borba protiv kiberkriminaliteta važan je prioritet Europskog programa sigurnosti, čime se doprinosi općem cilju postizanja visoke razine kibersigurnosti. Drugi pravni akti, kao što su Uredba (EU) 2016/679 Europskog parlamenta i Vijeća ([10]) i direktive 2002/58/EZ ([11]) i (EU) 2018/1972 ([12]) Europskog parlamenta i Vijeća, također doprinose visokoj razini kibersigurnosti na jedinstvenom digitalnom tržištu.

([6]) Uredba (EZ) br. 460/2004 Europskog parlamenta i Vijeća od 10. ožujka 2004. o osnivanju Europske agencije za mrežnu i informacijsku sigurnost (SL L 77, 13.3.2004., str. 1.).

([7]) Uredba (EZ) br. 1007/2008 Europskog parlamenta i Vijeća od 24. rujna 2008. o izmjeni Uredbe (EZ) br. 460/2004 o osnivanju Europske agencije za mrežnu i informacijsku sigurnost u pogledu njezina trajanja (SL L 293, 31.10.2008., str. 1.).

([8]) Uredba (EU) br. 580/2011 Europskog parlamenta i Vijeća od 8. lipnja 2011. o izmjeni Uredbe (EZ) br. 460/2004 o osnivanju Europske agencije za mrežnu i informacijsku sigurnost u pogledu njezina trajanja (SL L 165, 24.6.2011., str. 3.).

([9]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

([10]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

([11]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

([12]) Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (SL L 321, 17.12.2018., str. 36.).

(16) Od donošenja strategije Europske unije o kibersigurnosti iz 2013. i posljednje revizije mandata ENISA-ee znatno se promijenio opći kontekst politike rastom neizvjesnosti i nesigurnosti globalnog okruženja. Imajući to u vidu te u kontekstu pozitivnog razvoja uloge ENISA-e kao referentne točke za savjetovanje i stručno znanje, posredovatelja suradnje i izgradnje kapaciteta te u okviru nove politike Unije u području kibersigurnosti nužno je preispitati mandat ENISA-e kako bi se utvrdila njezina uloga u promijenjenom kibersigurnosnom ekosustavu i osiguralo da ona djelotvorno doprinosi odgovoru Unije na kiberizazove koji proizlaze iz bitno preobraženog okruženja kiberprijetnji na koje ENISA, kao što se pokazalo tijekom njezine evaluacije, u okviru svojeg trenutačnog mandata, ne može dostatno odgovoriti.

(17) ENISA osnovana ovom Uredbom trebala bi naslijediti ENISA-u osnovanu Uredbom (EU) br. 526/2013. ENISA bi trebala izvršavati zadaće koje su joj povjerene ovom Uredbom i drugim pravnim aktima Unije u području kibersigurnosti pružanjem, među ostalim, savjeta i stručnog znanja te djelujući kao centar za informacije i znanje u Uniji. Ona bi trebala promicati razmjenu najbolje prakse među državama članicama i privatnim dionicima, Komisiji i državama članicama trebala bi davati prijedloge o politikama, djelovati kao referentna točka za sektorske inicijative politike Unije u području kibersigurnosti i poticati operativnu suradnju među državama članicama i između država članica i institucija, tijela, ureda i agencija Unije.

(18) Odlukom 2004/97/EZ, Euratom donesenom zajedničkim dogovorom predstavnika država članica koji su se sastali na razini šefova država i vlada ([13]), predstavnici država članica odlučili su da će sjedište ENISA-e biti u Grčkoj u gradu koji odredi grčka vlada. Država članica domaćin ENISA-e trebala bi osigurati najbolje moguće uvjete za njezin nesmetan i učinkovit rad. Za pravilno i učinkovito obavljanje zadaća, za odabir i zadržavanje osoblja te za jačanje učinkovitosti aktivnosti umrežavanja nužno je da se ENISA nalazi na odgovarajućoj lokaciji na kojoj su, među ostalim, osigurani odgovarajuća prometna povezanost te prostori za supružnike i djecu koji prate članove osoblja ENISA-e. Potrebne aranžmane trebalo bi utvrditi u sporazumu između ENISA-e i države članice domaćina koji se sklapa nakon dobivanja suglasnosti Upravljačkog odbora ENISA-e.

(19) S obzirom na sve veće rizike i izazove u području kibersigurnosti s kojima se Unija suočava, trebalo bi povećati financijske i ljudske resurse dodijeljene ENISA-i u skladu s njezinom pojačanom ulogom i zadaćama i njezinom ključnom ulogom u ekosustavu organizacija koje brane digitalni ekosustav Unije koji bi ENISA-i omogućili da učinkovito izvršava zadaće koje su joj dodijeljene ovom Uredbom.

(20) ENISA bi trebala razviti i održavati visoku razinu stručnosti i djelovati kao referentna točka koja svojom neovisnošću, kvalitetom savjeta i informacija koje pruža, transparentnošću postupaka i metoda rada te marljivošću u obavljanju svojih zadaća uspostavlja povjerenje u jedinstveno tržište. ENISA bi trebala aktivno podupirati nacionalne napore te bi trebala proaktivno doprinositi naporima Unije obavljajući pritom svoje zadaće u potpunoj suradnji s institucijama, tijelima, uredima i agencijama Unije te s državama članicama, uz izbjegavanje udvostručavanja posla i promicanje sinergije. Nadalje, rad ENISA-e trebao bi se temeljiti na informacijama dobivenima od privatnog sektora i relevantnih dionika i suradnji s njima. Skupom zadaća trebao bi se utvrditi način na koji će ENISA ostvariti svoje ciljeve, pri čemu joj se treba omogućiti fleksibilnost u radu.

(21) ENISA bi trebala dodatno ojačati vlastite tehničke i ljudske sposobnosti i vještine kako bi mogla pružiti odgovarajuću potporu operativnoj suradnji između država članica. ENISA bi trebala povećati svoje znanje i iskustvo te sposobnosti. ENISA i države članice mogli bi na dobrovoljnoj osnovi osmisliti programe za upućivanje nacionalnih stručnjaka u ENISA-u, stvaranje skupina stručnjaka i razmjenu osoblja.

(22) ENISA bi trebala pomagati Komisiji davanjem savjeta, mišljenja i analiza u vezi sa svim pitanjima Unije koja se odnose na razvoj, ažuriranje i preispitivanje politika i prava u području kibersigurnosti te njihovih sektorskih aspekata radi jačanja relevantnosti politika i prava Unije s dimenzijom kibersigurnosti i omogućavanja dosljednosti u njihovoj provedbi na nacionalnoj razini. ENISA bi trebala djelovati kao referentna točka za pružanje savjeta i stručnog znanja o sektorskoj politici i pravnim inicijativama Unije kada je riječ o pitanjima kibersigurnosti. ENISA bi trebala redovito obavješćivati Europski parlament o svojim aktivnostima.

([13]) Odluka 2004/97/EZ, Euratom donesena zajedničkim dogovorom predstavnika država članica koji su se sastali na razini šefova država i vlada od 13. prosinca 2003. o određivanju sjedišta određenih ureda i agencija Europske unije (SL L 29, 3.2.2004., str. 15.).

(23) Javna jezgra otvorenog interneta, odnosno njegovi glavni protokoli i infrastruktura koji su globalno javno dobro, omogućuje temeljnu funkcionalnost interneta i osnova je njegova normalnog funkcioniranja. ENISA bi trebala podupirati sigurnost i stabilnost funkcioniranja javne jezgre otvorenog interneta, uključujući, ali ne ograničavajući se na ključne protokole (posebno DNS, BGP i IPv6), rad sustava naziva domena (DNS) (kao što je funkcioniranje svih vršnih domena), te rad korijenske zone (root zone).

(24) Osnovna je zadaća ENISA-e promicati dosljednu provedbu odgovarajućeg pravnog okvira, a posebno učinkovitu provedbu Direktive (EU) 2016/1148 i drugih relevantnih pravnih instrumenata koji sadržavaju aspekte kibersigurnosti, što je od ključne važnosti za povećanje kiberotpornosti. S obzirom na kiberprijetnje koje se brzo razvijaju, jasno je da države članice trebaju potporu sveobuhvatnijeg, horizontalnog pristupa izgradnji kiberotpornosti.

(25) ENISA bi trebala pomagati državama članicama i institucijama, tijelima, uredima i agencijama Unije u njihovim naporima usmjerenima na izgradnju i jačanje sposobnosti i pripravnosti s ciljem sprječavanja i otkrivanja kiberprijetnji i kiberincidenata i odgovora na njih te u vezi sa sigurnošću mrežnih i informacijskih sustava. ENISA bi posebno trebala poduprijeti razvoj i jačanje nacionalnih i Unijinih timova za odgovor na računalne sigurnosne incidente („CSIRT-ovi”) iz Direktive (EU) 2016/1148 s ciljem postizanja visoke zajedničke razine njihove zrelosti u Uniji. Aktivnostima ENISA-e koje se odnose na operativne kapacitete država članica trebale bi se aktivno podupirati mjere koje države članice poduzimaju radi ispunjenja svojih obveza proizašlih iz Direktive (EU) 2016/1148 te ih stoga ne bi trebale nadomjestiti.

(26) ENISA bi usto trebala pomagati u razvoju i ažuriranju strategija o sigurnosti mrežnih i informacijskih sustava na razini Unije i, na zahtjev, na razini država članica, osobito o kibersigurnosti, te bi trebala promicati širenje tih strategija i pratiti njihovu provedbu. ENISA bi ujedno trebala doprinositi pokrivanju potreba za osposobljavanjem i obrazovnim materijalima, uključujući potrebe javnih tijela, i prema potrebi, u velikoj mjeri „osposobljavati voditelje osposobljavanja” nadovezujući se na Okvir digitalne kompetencije za građane kako bi pomogla državama članicama te institucijama, tijelima, uredima i agencijama Unije da razviju vlastite sposobnosti za osposobljavanje.

(27) ENISA bi trebala podupirati države članice u području podizanja svijesti i obrazovanja o kibersigurnosti olakšavanjem bliže koordinacije i razmjene najboljih praksi među državama članicama. Takva bi se potpora mogla sastojati od razvoja mreže nacionalnih obrazovnih kontaktnih točaka i razvoja platforme za osposobljavanje u području kibersigurnosti. Mreža nacionalnih obrazovnih kontaktnih točaka mogla bi djelovati u okviru mreže nacionalnih časnika za vezu te osigurati početnu točku za buduću koordinaciju unutar država članica.

(28) ENISA bi trebala pomagati Skupini za suradnju osnovanoj Direktivom (EU) 2016/1148 pri izvršavanju njezinih zadaća, posebno pružanjem stručnog znanja i savjeta te olakšavanjem razmjene najbolje prakse, među ostalim, u pogledu utvrđivanja operatora ključnih usluga u državama članicama, kao i u pogledu prekograničnih ovisnosti, rizika i incidenata.

(29) S ciljem poticanja suradnje između javnog i privatnog sektora te unutar privatnog sektora, posebice radi potpore zaštiti kritične infrastrukture, ENISA bi trebala podupirati unutarsektorsku i međusektorsku razmjenu informacija, osobito u sektorima s popisa u Prilogu II. Direktivi (EU) 2016/1148, pružanjem najboljih praksi i smjernica o dostupnim alatima i postupcima, kao i pružanjem smjernica za rješavanje regulatornih pitanja povezanih s razmjenom informacija, primjerice olakšavanjem uspostave sektorskih centara za razmjenu i analizu informacija.

(30) Budući da je mogući negativni učinak ranjivosti IKT proizvoda, IKT usluga i IKT procesa u stalnom porastu, pronalaženje i otklanjanje takvih ranjivosti ima važnu ulogu u smanjenju ukupnih kibersigurnosnih rizika. Pokazalo se da se suradnjom između organizacija, proizvođača ili pružatelja ranjivih IKT proizvoda, IKT usluga i IKT procesa te članova istraživačke zajednice u području kibersigurnosti i vladâ, koji pronalaze takve ranjivosti, znatno povećava i stopa otkrivanja i stopa uklanjanja ranjivosti IKT proizvoda, IKT usluga i IKT procesa. Koordinirano otkrivanje ranjivosti odvija se strukturiranim postupkom suradnje u kojem se ranjivosti prijavljuju vlasniku informacijskog sustava, čime se organizaciji omogućuje da dijagnosticira i otkloni ranjivost prije nego što se detaljne informacije o njoj otkriju trećim stranama ili javnosti. Tim se postupkom predviđa i koordinacija između strane koja je otkrila ranjivosti i organizacije u pogledu objave tih ranjivosti. Politike koordiniranog otkrivanja ranjivosti mogle bi imati važnu ulogu u nastojanjima država članica da poboljšaju kibersigurnost.

(31) ENISA bi trebala objedinjavati i analizirati dobrovoljno podijeljena zajednička nacionalna izvješća CSIRT-ova i međuinstitucijskog tima za hitne računalne intervencije za institucije, tijela i agencije Unije uspostavljenog Dogovorom između Europskog parlamenta, Europskog vijeća, Vijeća Europske unije, Europske komisije, Suda Europske unije, Europske središnje banke, Europskog revizorskog suda, Europske službe za vanjsko djelovanje, Europskog gospodarskog i socijalnog odbora, Europskog Odbora regija i Europske investicijske banke o organizaciji i radu tima za hitne računalne intervencije za institucije, tijela i agencije Unije (CERT-EU) ([14]) radi doprinosa uspostavi zajedničkih postupaka, jezika i terminologije za razmjenu informacija. U tom bi kontekstu ENISA trebala uključiti i privatni sektor u okvir Direktive (EU) 2016/1148 kojom se utvrđuje osnova za dobrovoljnu razmjenu tehničkih informacija na operativnoj razini u okviru mreže timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova") uspostavljene tom direktivom.

(32) ENISA bi trebala doprinijeti odgovorima na razini Unije u slučaju prekograničnih incidenata i kriza velikih razmjera povezanih s kibersigurnošću. Tu bi zadaću ENISA trebala obavljati sukladno svojem mandatu u skladu s ovom Uredbom i pristupom koji trebaju dogovoriti države članice u kontekstu Preporuke Komisije (EU) 2017/1584 ([15]) i Zaključaka Vijeća od 26. lipnja 2018. o koordiniranom odgovoru EU-a na kiberincidente i kiberkrize velikih razmjera. Ta bi zadaća mogla uključivati prikupljanje relevantnih informacija i posredovanje između mreže CSIRT-ova i tehničke zajednice te između donositelja odluka koji su odgovorni za upravljanje krizom. Nadalje, ENISA bi trebala podupirati operativnu suradnju među državama članicama, ako to zahtijeva jedna ili više država članica, pri rješavanju incidenata s tehničkog gledišta olakšavanjem relevantne razmjene tehničkih rješenja među državama članicama i doprinosom komunikaciji s javnošću. ENISA bi trebala podupirati operativnu suradnju ispitivanjem uređenja za takvu suradnju s pomoću redovnih vježbi u području kibersigurnosti.

(33) ENISA bi pri podupiranju operativne suradnje trebala iskoristiti dostupnu tehničku i operativnu stručnost CERT-EU-a u okviru strukturirane suradnje. Takvom strukturiranom suradnjom moglo bi se izgraditi stručno znanje ENISA-e. Prema potrebi trebalo bi definirati odgovarajuće namjenske aranžmane između ta dva subjekta kako bi se utvrdila praktična provedba takve suradnje i izbjeglo udvostručivanje aktivnosti.

(34) U obavljanju svoje zadaće pružanja potpore operativnoj suradnji u okviru mreže CSIRT-ova ENISA bi trebala moći pružiti potporu državama članicama na njihov zahtjev, primjerice pružanjem savjeta o tome kako poboljšati njihove sposobnosti za sprečavanje, otkrivanje i odgovor na incidente, olakšavanjem tehničkog rješavanja incidenata sa značajnim ili bitnim učinkom, ili osiguravanjem da kiberprijetnje i kiberincidenati budu podvrgnuti analizi. ENISA bi trebala olakšati tehničko rješavanje incidenata sa značajnim ili bitnim učinkom i to posebice podupiranjem dobrovoljne razmjene tehničkih rješenja među državama članicama ili izradom objedinjenih tehničkih informacija kao što su tehnička rješenja koja države članice dobrovoljno razmjenjuju. U Preporuci (EU) 2017/1584 preporučuje se da države članice surađuju u dobroj vjeri te da uzajamno i s ENISA-om bez nepotrebnog odlaganja razmjenjuju informacije o incidentima i krizama velikih razmjera povezanima s kibersigurnošću. Takvim bi se informacijama dodatno pomoglo ENISA-i pri izvršavanju zadaća podupiranja operativne suradnje.

(35) U okviru redovne suradnje na tehničkoj razini s ciljem podupiranja informiranosti o stanju u Uniji, ENISA bi trebala u bliskoj suradnji s državama članicama izrađivati redovito i temeljito tehničko izvješće o stanju kibersigurnosti EU-a u pogledu incidenata i kiberprijetnji, na temelju javno dostupnih informacija, vlastite analize i izvješća koje s njom dijele CSIRT-ovi država članica ili nacionalne jedinstvene kontaktne točke za sigurnost mrežnih i informacijskih sustava („jedinstvene kontaktne točke") iz Direktive (EU) 2016/1148,u oba slučaja na dobrovoljnoj osnovi, Europski centar za kiberkriminalitet (EC3) pri Europolu, CERT-EU i, prema potrebi, Obavještajni i situacijski centar EU-a (EU INTCEN) pri Europskoj službi za vanjsko djelovanje. To bi izvješće trebalo biti dostupno Vijeću, Komisiji, Visokom predstavniku Unije za vanjske poslove i sigurnosnu politiku i mreži CSIRT-ova.

(36) Potpora ENISA-e ex-post tehničkim istragama incidenata sa značajnim ili bitnim učinkom poduzete na zahtjev pogođenih država članica trebala bi biti usmjerena na sprečavanje budućih incidenata. Dotične države članice trebale bi pružiti potrebne informacije i pomoć kako bi ENISA mogla učinkovito podupirati ex-post tehničku istragu.

([14]) SL C 12, 13.1.2018., str. 1.
([15]) Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

(37) Države članice mogu pozvati poduzeća pogođena incidentom da surađuju pružanjem potrebnih informacija i pomoći ENISA-i ne dovodeći u pitanje njihovo pravo na zaštitu poslovno osjetljivih informacija i informacija koje se odnose na javnu sigurnost.

(38) Kako bi bolje razumjela izazove u području kibersigurnosti i s ciljem pružanja strateških dugoročnih savjeta državama članicama i institucijama, tijelima, uredima i agencijama Unije, ENISA mora analizirati postojeće i nove kibersigurnosne rizike. U tu svrhu ENISA bi trebala, u suradnji s državama članicama i, prema potrebi, s tijelima za statistiku i drugim tijelima, prikupljati relevantne javno dostupne informacije ili one dobrovoljno stavljene na raspolaganje i provoditi analize novih tehnologija te davati tematske procjene očekivanih društvenih, pravnih, gospodarskih i regulatornih učinaka tehnoloških inovacija na mrežnu i informacijsku sigurnost, a posebno na kibersigurnost. Nadalje, ENISA bi analizom kiberprijetnji, ranjivosti i incidenata trebala pomagati državama članicama i institucijama, tijelima, uredima i agencijama Unije u prepoznavanju novih kibersigurnosnih rizika i sprečavanju incidenata.

(39) S ciljem povećanja otpornosti Unije ENISA bi trebala razvijati stručnost u području kibersigurnosti infrastruktura posebno radi potpore sektorima iz Priloga II. Direktivi (EU) 2016/1148 i onih koje upotrebljavaju pružatelji digitalnih usluga navedeni u Prilogu III. toj direktivi pružanjem savjeta, izdavanjem smjernica i razmjenom najboljih praksi. Kako bi osigurala lakši pristup bolje strukturiranim informacijama o kibersigurnosnim rizicima i mogućim lijekovima, ENISA bi trebala razviti i održavati „informativni centar" Unije, središnji portal na kojem će javnost moći na jednom mjestu dobiti informacije o kibersigurnosti koje potječu od institucija, tijela, ureda i agencija na razini Unije i nacionalnoj razini. Olakšavanje pristupa bolje strukturiranim informacijama o kibersigurnosnim rizicima i mogućim lijekovima moglo bi također pomoći državama članicama da ojačaju svoje sposobnosti i usklade svoje prakse, čime bi povećale svoju ukupnu otpornost na kibernapade.

(40) ENISA bi trebala doprinositi podizanju osviještenosti javnosti o kibersigurnosti, među ostalim putem kampanje podizanja svijesti na razini EU-a promicanjem obrazovanja, i davanjem savjeta o dobrim praksama za pojedinačne korisnike koje su namijenjene građanima, organizacijama i poduzećima. ENISA bi trebala doprinositi i promicanju najboljih praksi i rješenja, među ostalim kiberhigijenu i kiberpismenost, na razini građana, organizacija i poduzeća prikupljanjem i analizom javno dostupnih informacija o značajnim incidentima te sastavljanjem i objavljivanjem izvješća i savjeta za građane, organizacije i poduzeća kako bi se poboljšala njihova opća razina pripravnosti i otpornosti. ENISA bi također trebala težiti tome da potrošačima pruži relevantne informacije o primjenjivim programima certifikacije, na primjer davanjem smjernica i preporuka. ENISA bi, nadalje, u skladu s akcijskim planom o digitalnom obrazovanju uspostavljenim u Komunikaciji Komisije od 17. siječnja 2018. i u suradnji s državama članicama i institucijama, tijelima, uredima i agencijama Unije trebala organizirati redovite kampanje informiranja i obrazovanja krajnjih korisnika s ciljem poticanja sigurnijeg ponašanja pojedinaca na internetu, digitalne pismenosti i podizanja osviještenosti o potencijalnim kiberprijetnjama, uključujući kriminalne aktivnosti na internetu kao što su phishing napadi, mreže zaraženih računala (botnet), financijske i bankovne prijevare, prijevare povezane s podacima, te promicanja osnovnih savjeta o višestrukoj autentifikaciji, zakrpama, enkripciji, anonimizaciji i zaštiti podataka.

(41) ENISA bi trebala imati glavnu ulogu u bržem osvješćivanju krajnjih korisnika o sigurnosti uređaja i sigurnom korištenju uslugama te bi trebala promicati integriranu sigurnost i integriranu privatnost na razini Unije. U postizanju tog cilja ENISA bi trebala najbolje iskoristiti dostupne najbolje prakse i iskustva, posebice najbolje prakse i iskustva akademskih institucija i istraživača u području IT sigurnosti.

(42) Kako bi pružala potporu poduzećima koja djeluju u sektoru kibersigurnosti i korisnicima kibersigurnosnih rješenja, ENISA bi trebala razviti i održavati „opservatorij tržišta" provođenjem redovitih analiza i širenjem informacija o glavnim kretanjima na kibersigurnosnom tržištu na strani ponude i potražnje.

(43) ENISA bi trebala doprinositi naporima Unije u suradnji s međunarodnim organizacijama te u okviru odgovarajućih okvira za međunarodnu suradnju u području kibersigurnosti. ENISA bi prema potrebi posebno trebala doprinositi suradnji s organizacijama kao što su OECD, OESS i NATO. Takva suradnja mogla bi, među ostalim, uključivati zajedničke vježbe u području kibersigurnosti i zajedničku koordinaciju odgovora na incidente. Te se aktivnosti trebaju provoditi u potpunosti poštujući Unijina načela uključivosti, uzajamnosti i autonomije u donošenju odluka, ne dovodeći u pitanje posebnu narav sigurnosne i obrambene politike nijedne države članice.

(44) Kako bi se osiguralo da ENISA u potpunosti ostvari svoje ciljeve, ona bi se trebala povezati s relevantnim nadzornim tijelima Unije i drugim nadležnim tijelima u Uniji, institucijama, tijelima, uredima i agencijama Unije, među ostalim s CERT-EU-om, EC3-om, Europskom obrambenom agencijom (EDA), Agencijom za europski globalni navigacijski satelitski sustav (Europska agencija za GNSS), Uredom tijela europskih regulatora za elektroničke komunikacije (BEREC), Europskom agencijom za operativno upravljanje opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde (eu-LISA), Europskom središnjom bankom (ESB), Europskim nadzornim tijelom za bankarstvo (EBA), Europskim odborom za zaštitu podataka, Agencijom Unije za suradnju energetskih regulatora (ACER), Europskom agencijom za sigurnost zračnog prometa (EASA) i sa svim drugim agencijama Unije koje djeluju u području kibersigurnosti. ENISA bi se trebala povezati i s nadležnim tijelima za zaštitu podataka s ciljem razmjene znanja i najbolje prakse i trebala bi davati savjete o aspektima kibersigurnosti koji bi mogli utjecati na njihov rad. Predstavnici nacionalnih tijela za izvršavanje zakonodavstva i tijela za izvršavanje zakonodavstva na razini Unije te nacionalnih tijela i tijela Unije za zaštitu privatnosti trebali bi imati pravo da budu zastupljeni u savjetodavnoj skupini ENISA-e. Pri povezivanju s tijelima za izvršavanje zakonodavstva u vezi s pitanjima mrežne i informacijske sigurnosti koji mogu utjecati na njihov rad, ENISA bi trebala poštovati postojeće informacijske kanale i uspostavljene mreže.

(45) Mogla bi se uspostaviti partnerstva s akademskim institucijama u kojima su pokrenute istraživačke inicijative u relevantnim područjima te bi trebali postojati odgovarajući kanali za doprinose organizacija potrošača i drugih organizacija koje bi trebalo uzeti u obzir.

(46) ENISA bi u svojoj ulozi tajništva mreže CSIRT-ova trebala podupirati CSIRT-ove u državama članicama i CERT-EU u operativnoj suradnji u vezi s relevantnim zadaćama mreže CSIRT-ova kako su navedene u Direktivi (EU) 2016/1148. Nadalje, ENISA bi trebala poticati i podržavati suradnju između relevantnih CSIRT-ova u slučaju incidenata, napada ili poremećaja mreža ili infrastrukture kojima upravljaju ili koje oni štite i koje uključuju ili imaju mogućnost uključivanja najmanje dva CSIRT-a uzimajući u obzir standardne operativne postupke mreže CSIRT-ova.

(47) S ciljem povećanja pripravnosti Unije za odgovor na incidente ENISA bi trebala redovito organizirati vježbe u području kibersigurnosti na razini Unije te državama članicama, institucijama, tijelima, uredima i agencijama Unije na njihov zahtjev pomagati pri organizaciji takvih vježbi. Jednom svake dvije godine trebalo bi organizirati sveobuhvatne vježbe velikog razmjera koja bi obuhvaćala tehničke, operativne ili strateške elemente. Osim toga, ENISA bi trebala moći redovito organizirati manje opsežne vježbe s istim ciljem povećanja pripravnosti Unije za odgovor na incidente

(48) ENISA bi trebala dalje razvijati i održavati svoje stručno znanje u području kibersigurnosne certifikacije radi potpore politici Unije u tom području. ENISA bi se trebala oslanjati na postojeće najbolje prakse te bi trebala promicati prihvaćanje kibersigurnosne certifikacije u Uniji, među ostalim doprinosom uspostavi okvira za kibersigurnosnu certifikaciju na razini Unije (europski okvir za kibersigurnosnu certifikaciju) i njegovu održavanju, s ciljem povećanja transparentnosti kibersigurnosnog jamstva za IKT proizvode, IKT usluge i IKT procese, jačajući time povjerenje u digitalno unutarnje tržište i njegovu konkurentnost.

(49) Učinkovita kibersigurnosna politika trebala bi se temeljiti na dobro razrađenim metodama procjene rizika i u javnom i u privatnom sektoru. Metode za procjenu rizika upotrebljavaju se na različitim razinama, međutim ne postoji zajednička praksa u pogledu njihove učinkovite primjene. Poticanjem i razvojem najboljih praksa za procjenu rizika i za interoperabilna rješenja za upravljanje rizicima u organizacijama javnog i privatnog sektora povećat će se razina kibersigurnosti u Uniji. U tu bi svrhu ENISA trebala podupirati suradnju između dionika na razini Unije i olakšavati njihova nastojanja u vezi s utvrđivanjem i preuzimanjem europskih i međunarodnih norma za upravljanje rizicima i za mjerljivu sigurnost elektroničkih proizvoda, sustava, mreža i usluga koji zajedno sa softverom čine mrežne i informacijske sustave.

(50) ENISA bi trebala ohrabrivati države članice, proizvođače ili pružatelje IKT proizvoda, IKT usluga ili IKT procesa da povećaju svoje opće sigurnosne norme kako bi svi korisnici interneta mogli poduzeti potrebne korake za osiguranje svoje osobne kibersigurnosti te bi ih trebala poticati da to učine. Konkretno, proizvođači i pružatelji IKT proizvoda, IKT usluga i IKT procesa trebali bi osigurati sva nužna ažuriranja i trebali bi opozvati, povući ili reciklirati IKT proizvode, IKT usluge i IKT procese koji ne zadovoljavaju kibersigurnosne norme, dok bi uvoznici i distributeri trebali osigurati da IKT proizvodi, IKT usluge i IKT procesi koje stavljaju na tržište Unije ispunjavaju primjenjive zahtjeve i ne predstavljaju rizik za potrošače Unije.

(51) ENISA bi, u suradnji s nadležnim tijelima, trebala moći širiti informacije o razini kibersigurnosti IKT proizvoda, IKT usluga i IKT procesa koje se nude na unutarnjem tržištu te bi pružateljima i proizvođačima IKT proizvoda, IKT usluga i IKT procesa trebala izdavati upozorenja u kojima od njih traži da poboljšaju sigurnost svojih IKT proizvoda, IKT usluga i IKT procesa, uključujući kibersigurnost.

(52) ENISA bi trebala u potpunosti uzeti u obzir aktualne aktivnosti istraživanja, razvoja i tehnoloških ocjena, a osobito one aktivnosti koje se provode u okviru različitih istraživačkih inicijativa Unije kako bi institucijama, tijelima, uredima i agencijama Unije te, kada je to relevantno, državama članicama na njihov zahtjev pružala savjete o istraživačkim potrebama i prioritetima u području kibersigurnosti. S ciljem utvrđivanja istraživačkih potreba i prioriteta ENISA bi se također trebala savjetovati s relevantnim skupinama korisnika. Konkretnije, mogla bi se uspostaviti suradnja s Europskim istraživačkim vijećem, Europskim institutom za inovacije i tehnologiju te s Institutom Europske unije za sigurnosne studije.

(53) Prilikom izrade europskih programa kibersigurnosne certifikacije ENISA bi se trebala redovito savjetovati s organizacijama za normizaciju, a posebno s europskim organizacijama za normizaciju.

(54) Kiberprijetnje su globalni problem. Potrebna je i bliža međunarodna suradnja radi unaprjeđenja kibersigurnosnih normi, što obuhvaća potrebu za definiranjem zajedničkih normi ponašanja, donošenja kodeksa ponašanja, upotrebu međunarodnih normi i razmjenu informacija, poticanje brže međunarodne suradnje kao odgovor na pitanja mrežne i informacijske sigurnosti, kao i poticanje zajedničkog globalnog pristupa tim pitanjima. ENISA bi u tu svrhu, prema potrebi, pružanjem potrebnog stručnog znanja i analize relevantnim institucijama, tijelima, uredima i agencijama Unije trebala podupirati daljnje uključivanje Unije te njezinu suradnju s trećim zemljama i međunarodnim organizacijama.

(55) ENISA bi trebala moći odgovoriti na ad hoc zahtjeve za savjet i pomoć država članica i institucija, tijela, ureda i agencija Unije o pitanjima koja su obuhvaćena njezinim mandatom.

(56) Razumno je i preporučuje se primijeniti određena načela u vezi s upravljanjem ENISA-om radi usklađenosti sa zajedničkom izjavom i zajedničkim pristupom koje je u srpnju 2012. dogovorila Međuinstitucionalna radna skupina za decentralizirane agencije EU-a, čija je svrha pojednostavnjivanje aktivnosti decentraliziranih agencija i poboljšanje njihova djelovanja. U ovoj bi Uredbi ujedno trebalo prema potrebi odraziti preporuke iz zajedničke izjave i zajedničkog pristupa za programe rada ENISA-e, evaluacije ENISA-e te prakse ENISA-e u vezi s izvješćivanjem i upravljanjem.

(57) Upravljački odbor sastavljen od predstavnika država članica i Komisije trebao bi utvrditi opće usmjerenje rada ENISA-e i osigurati da ona obavlja svoje zadaće u skladu s ovom Uredbom. Upravljačkom odboru trebalo bi povjeriti ovlasti potrebne za izradu proračuna, provjeru izvršenja proračuna, donošenje odgovarajućih financijskih pravila, uspostavu transparentnih radnih postupaka za donošenje odluka ENISA-e, donošenje jedinstvenog programskog dokumenta ENISA-e, donošenje svog poslovnika, imenovanje izvršnog direktora i odlučivanje o produljenju ili prestanku mandata izvršnog direktora.

(58) S ciljem pravilnog i djelotvornog funkcioniranja ENISA-e Komisija i države članice trebale bi osigurati da osobe koje će imenovati u Upravljački odbor imaju odgovarajuća stručna znanja i iskustvo. Komisija i države članice također bi trebale ograničiti učestalost izmjena njihovih predstavnika u Upravljačkom odboru kako bi se osigurao kontinuitet njihova rada.

(59) Kako bi se osiguralo nesmetano funkcioniranje ENISA-e, njezin izvršni direktor imenuje se na temelju zasluga i dokazanih administrativnih i rukovoditeljskih sposobnosti, kao i sposobnosti i iskustava relevantnih za kibersigurnost. Dužnosti izvršnog direktora trebalo bi obavljati potpuno neovisno. Izvršni direktor trebao bi, nakon prethodnog savjetovanja s Komisijom, pripremiti prijedlog godišnjeg programa rada ENISA-e te bi trebao poduzeti sve potrebne korake kako bi osigurao njegovu pravilnu provedbu. Izvršni direktor trebao bi izraditi godišnje izvješće koje se dostavlja Upravljačkom odboru, a koje obuhvaća provedbu godišnjeg programa rada ENISA-e, sastaviti nacrt izvješća o procjenama prihoda i rashoda ENISA-e te provoditi proračun. Nadalje, izvršni direktor trebao bi imati mogućnost osnivanja ad hoc radnih skupina za rješavanje određenih pitanja, a posebno pitanja znanstvene, tehničke, pravne ili socioekonomske prirode. Osobito, u vezi s pripremom posebnog prijedloga europskog

programa kibersigurnosne certifikacije („prijedlog programa certifikacije”), smatra se da je potrebno osnivanje ad hoc radne skupine.Izvršni direktor trebao bi osigurati odabir članova ad hoc radnih skupina u skladu s najvišim normama stručnosti, nastojeći pritom osigurati rodnu ravnotežu i primjerenu ravnotežu, ovisno o specifičnim pitanjima, među predstavnicima javnih uprava država članica, institucija, tijela, ureda i agencija Unije i privatnog sektora, uključujući industriju, korisnike i akademske stručnjake iz područja mrežne i informacijske sigurnosti.

(60) Izvršni odbor trebao bi doprinositi učinkovitosti Upravljačkog odbora. U okviru priprema povezanih s donošenjem odluka Upravljačkog odbora, Izvršni bi odbor trebao detaljno ispitivati relevantne informacije i istraživati dostupne mogućnosti te nuditi savjete i rješenja za pripremu odluka Upravljačkog odbora.

(61) ENISA bi trebala imati Savjetodavnu skupinu ENISA-e kao savjetodavno tijelo kako bi se osigurao redoviti dijalog s privatnim sektorom, organizacijama potrošača i drugim interesnim skupinama. Savjetodavna skupina ENISA-e, koju na prijedlog izvršnog direktora osniva Upravljački odbor, trebala bi se usredotočiti na pitanja relevantna za dionike te bi trebala ENISA-i skretati pozornost na njih. Sa Savjetodavnom skupinom ENISA-e posebno se treba savjetovati u pogledu nacrta godišnjeg programa rada ENISA-e. Sastav Savjetodavne skupine ENISA-e i zadaće koje su joj dodijeljene trebali bi osigurati dostatnu zastupljenost dionika u radu ENISA-e.

(62) Potrebno je uspostaviti Interesnu skupinu za kibersigurnosnu certifikaciju kako bi ENISA-i i Komisiji pomogla u olakšavanju savjetovanja relevantnih dionika. Interesna skupina za kibersigurnosnu certifikaciju trebala bi se sastojati od članova koji predstavljaju industriju u uravnoteženim udjelima, kako na strani potražnje tako i na strani ponude IKT proizvoda i IKT usluga, uključujući posebno MSP-ove, pružatelje digitalnih usluga, europska i međunarodna tijela za normizaciju, nacionalna akreditacijska tijela, nadzorna tijela za zaštitu podataka i tijela za ocjenjivanje sukladnosti u skladu s Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća ([16]) te akademsku zajednicu i organizacije potrošača.

(63) ENISA bi trebala uspostaviti pravila o sprečavanju sukoba interesa i upravljanju njime. ENISA bi trebala također primjenjivati relevantne odredbe Unije o javnom pristupu dokumentima u skladu s Uredbom (EZ) br. 1049/2001 Europskog parlamenta i Vijeća ([17]). ENISA bi trebala obrađivati osobne podatke u skladu s Uredbom (EU) 2018/1725 Europskog parlamenta i Vijeća ([18]) ENISA bi se trebala pridržavati odredaba primjenjivih na institucije, tijela, urede i agencije Unije i nacionalnog zakonodavstva u vezi s postupanjem s osjetljivim dokumentima, posebno s osjetljivim neklasificiranim podacima i klasificiranim podacima Europske unije.

(64) Kako bi se zajamčila potpuna autonomija i neovisnost ENISA-e i kako bi joj se omogućilo obavljanje dodatnih zadaća, uključujući nepredviđene hitne zadaće, ENISA-i bi trebalo osigurati dostatan i autonoman proračun čiji bi prihodi prvenstveno trebali dolaziti iz doprinosa Unije i doprinosa trećih zemalja koje sudjeluju u radu ENISA-e. Prikladan proračun od presudne je važnosti kako bi se osiguralo da ENISA ima dovoljne kapacitete za ispunjavanje svih svojih zadaća i postizanje ciljeva, koji su sve brojniji. Veći dio osoblja ENISA-e trebao bi izravno sudjelovati u operativnoj provedbi mandata ENISA-e. Državi članici domaćinu ili bilo kojoj drugoj državi članici trebalo bi omogućiti davanje dobrovoljnih doprinosa proračunu ENISA-e. Na subvencije koje se financiraju iz općeg proračuna Unije trebao bi se i dalje primjenjivati proračunski postupak Unije. Nadalje, Revizorski sud trebao bi provesti reviziju računovodstvene dokumentacije ENISA-e radi osiguranja transparentnosti i odgovornosti.

(65) Kibersigurnosna certifikacija ima važnu ulogu u jačanju povjerenja u IKT proizvode, IKT usluge i IKT procese. Jedinstveno digitalno tržište, posebno podatkovno gospodarstvo i IoT, mogu se razvijati samo ako postoji opće povjerenje javnosti da se takvim proizvodima, uslugama i procesima osigurava određena razina kibersigurnosti. Povezani i automatizirani automobili, elektronički medicinski proizvodi, industrijski automatizirani kontrolni sustavi i pametne mreže samo su primjeri sektora u kojima se certifikacija već u velikoj mjeri primjenjuje ili će se vjerojatno primjenjivati u skoroj budućnosti. Kibersigurnosna certifikacija od ključne je važnosti u sektorima uređenima Direktivom (EU) 2016/1148.

([16]) Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (SL L 218, 13.8.2008., str. 30.).

([17]) Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).

([18]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ. (SL L 295, 21.11.2018., str. 39.).

(66) U svojoj komunikaciji iz 2016. pod naslovom „Jačanje europskog sustava kibernetičke sigurnosti i poticanje konkurentne i inovativne industrije kibernetičke sigurnosti” Komisija je istaknula potrebu za visokokvalitetnim, povoljnim i interoperabilnim proizvodima i rješenjima za kibersigurnost. Ponuda IKT proizvoda, IKT usluga i IKT procesa na jedinstvenom tržištu vrlo je zemljopisno rascjepkana. To je zato što se industrija kibersigurnosti u Europi u velikoj mjeri razvila na temelju potražnje nacionalnih vlada. Nadalje, nepostojanje interoperabilnih rješenja (tehničke norme), praksi i mehanizama certifikacije na razini Unije neki su od nedostataka koji utječu na jedinstveno tržište kibersigurnosti. Time je europskim poduzećima otežano tržišno natjecanje na nacionalnoj razini, na razini Uniji i na globalnoj razini. Također je ograničen izbor održivih i iskoristivih kibersigurnosnih tehnologija koje su dostupne građanima i poduzećima.Slično tomu, u svojoj Komunikaciji iz 2017. o preispitivanju provedbe Strategije jedinstvenog digitalnog tržišta na sredini provedbenog razdoblja - Povezano jedinstveno digitalno tržište za sve, Komisija je istaknula da su potrebni sigurni povezani proizvodi i sustavi te navela je da bi se stvaranjem europskog okvira za sigurnost IKT-a kojim se utvrđuju pravila o organizaciji sigurnosne certifikacije u području IKT-a u Uniji moglo očuvati povjerenje u internet i riješiti trenutačni problem fragmentacije unutarnjeg tržišta.

(67) Trenutačno se kibersigurnosna certifikacija IKT proizvoda, IKT usluga i IKT procesa provodi samo u ograničenoj mjeri. Ako postoji, ona se većinom provodi na razini države članice ili u okviru programa industrijskih sektora. U tom kontekstu certifikat koji je izdalo nacionalno tijelo za kibersigurnosnu certifikaciju druge države članice u načelu ne priznaju. Trgovačka društva stoga možda moraju certificirati svoje IKT proizvode, IKT usluge i IKT procese u nekoliko država članica u kojima posluju, na primjer radi sudjelovanja u nacionalnim postupcima javne nabave, što povećava njihove troškove. Nadalje, iako se pojavljuju novi programi, čini se da ne postoji usklađen i holistički pristup pitanjima horizontalne kibersigurnosti, na primjer u području IoT-a. U postojećim programima postoje znatni nedostaci i razlike u pogledu pokrivenosti proizvoda, jamstvene razine, materijalnih kriterija i stvarne upotrebe, čime se otežava uspostava mehanizama uzajamnog priznavanja u Uniji.

(68) Bilo je pokušaja postizanja uzajamnog priznavanja certifikata u Uniji. Međutim, oni su bili samo djelomično uspješni. Najvažniji primjer u tome pogledu jest sporazum o uzajamnom priznavanju (MRA) Skupine viših dužnosnika za sigurnost informacijskih sustava (SOG-IS). Iako predstavlja najvažniji model suradnje i uzajamnog priznavanja u području sigurnosne certifikacije, SOG-IS obuhvaća samo dio država članica. Time je ograničena djelotvornost sporazuma o uzajamnom priznavanju SOG-IS-a sa stajališta unutarnjeg tržišta.

(69) Stoga je potrebno usvojiti zajednički pristup i uspostaviti europski okvir za kibersigurnosnu certifikaciju kojim se utvrđuju glavni horizontalni zahtjevi za razvoj budućih europskih programa kibersigurnosne certifikacije i koji omogućuje priznavanje i uporabu europskih kibersigurnosnih certifikata i EU izjava o sukladnosti za IKT proizvode, IKT usluge ili IKT procese u svim državama članicama. Pritom je ključno nadovezati se na postojeće nacionalne i međunarodne programe i sustave uzajamnog priznavanja, osobito SOG-IS, te omogućiti neometan prijelaz iz postojećih programa u takvim sustavima na programe u novom europskom okviru za kibersigurnosnu certifikaciju. Europski okvir za kibersigurnosnu certifikaciju trebao bi imati dvostruku svrhu. Prvo, njime bi se trebalo doprinijeti povećanju povjerenja u IKT proizvode, IKT usluge i IKT procese koji su certificirani u skladu s tim europskim programima kibersigurnosne certifikacije. Drugo, on bi trebao pomoći da se izbjegne umnožavanje proturječnih ili preklapajućih nacionalnih programa kibersigurnosne certifikacije i tako smanjiti troškove poduzećima koja djeluju na jedinstvenom digitalnom tržištu. Europski programi kibersigurnosne certifikacije trebali bi biti nediskriminirajući i temeljiti se na europskim ili međunarodnim normama, osim ako su te norme neučinkovite ili neprimjerene za ispunjavanje zakonitih ciljeva Unije u tom pogledu.

(70) Taj europski okvir za kibersigurnosnu certifikaciju trebalo bi na ujednačen način uspostaviti u svim državama članicama kako bi se izbjegla praksa „traženja povoljnije certifikacije” zbog razlika u razini strogoće u različitim državama članicama.

(71) Europske programe kibersigurnosne certifikacije trebalo bi temeljiti na onome što već postoji na međunarodnoj i nacionalnoj razini te, prema potrebi, na tehničkim specifikacijama iz foruma i konzorcijâ, učenju od sadašnjih pozitivnih primjera te analiziranju i ispravljanju nedostataka.

(72) Potrebna su fleksibilna rješenja kako bi taj sektor bio korak ispred kiberprijetnji te bi stoga trebalo osigurati da programi certifikacije budu tako osmišljeni da se izbjegne rizik da ubrzo postanu zastarjeli.

(73) Komisija bi trebala imati ovlasti donositi europske programe kibersigurnosne certifikacije za određene skupine IKT proizvoda, IKT usluga i IKT procesa. Te programe trebala bi provoditi i nadzirati nacionalna tijela za kibersigurnosnu certifikaciju, a certifikati izdani u okviru tih programa trebali bi biti valjani i priznati u cijeloj Uniji. Programi certifikacije kojima upravlja industrija ili privatne organizacije trebali bi biti izvan područja primjene ove Uredbe. Međutim, tijela koja provode takve programe trebala bi moći Komisiji predložiti da razmotri odobravanje tih programa kao europskih programa kibersigurnosne certifikacije.

(74) Odredbama ove Uredbe ne bi se smjelo dovoditi u pitanje pravo Unije kojim se propisuju posebna pravila o certifikaciji IKT proizvoda, IKT usluga i IKT procesa. Naime, u Uredbi (EU) 2016/679 utvrđene su odredbe o uspostavi mehanizama certifikacije te pečata i oznaka za zaštitu podataka za potrebe dokazivanja usklađenosti s tom Uredbom postupaka obrade koje obavljaju voditelji ili izvršitelji obrade. Tim mehanizmima certifikacije te pečatima i oznakama za zaštitu podataka trebalo bi se osobama čiji se podaci obrađuju omogućiti da brzo ocijene razinu zaštite podataka relevantnih IKT proizvoda, IKT usluga i IKT procesa. Ovom Uredbom ne dovodi se u pitanje certifikacija postupaka obrade podataka u skladu s Uredbom (EU) 2016/679, uključujući i kada su ti postupci ugrađeni u IKT proizvode, IKT usluge i IKT procese.

(75) Svrha europskih programa kibersigurnosne certifikacije trebala bi biti osiguravanje toga da IKT proizvodi, IKT usluge i IKT procesi koji su certificirani u okviru takvog programa zadovoljavaju određene zahtjeve čiji je cilj zaštita dostupnosti, izvornosti, cjelovitosti i povjerljivosti pohranjenih, poslanih ili obrađenih podataka ili povezanih funkcija ili usluga koje se nude ili kojima se može pristupiti s pomoću tih proizvoda, usluga i procesa, tijekom njihova životnog ciklusa. U ovoj Uredbi ne mogu se podrobno utvrditi kibersigurnosni zahtjevi povezani sa svim IKT proizvodima, IKT uslugama i IKT procesima. IKT proizvodi, IKT usluge i IKT procesi te kibersigurnosne potrebe povezane s tim proizvodima, uslugama i procesima toliko su različiti da je teško osmisliti opće kibersigurnosne zahtjeve koji se mogu primijeniti u svim okolnostima. Stoga je za potrebe certifikacije potrebno prihvatiti širok i općenit pojam kibersigurnosti koji bi trebalo dopuniti skupom kibersigurnosnih ciljeva koje treba uzeti u obzir pri izradi europskih programa kibersigurnosne certifikacije. Načine postizanja tih ciljeva u određenim IKT proizvodima, IKT uslugama i IKT procesima trebalo bi potom podrobnije opisati na razini pojedinačnog programa certifikacije koji je donijela Komisija, na primjer upućivanjem na norme ili tehničke specifikacije ako nisu dostupne odgovarajuće norme.

(76) Tehničke specifikacije koje treba upotrebljavati u europskom programu kibersigurnosne certifikacije trebale bi poštovati zahtjeve određene u Prilogu II. Uredbi (EU) br. 1025/2012 Europskog parlamenta i Vijeća ([19]). Neka odstupanja od tih zahtjeva mogla bi se ipak smatrati potrebnima u opravdanim slučajevima upotrebe tih tehničkih specifikacija u europskom programu kibersigurnosne certifikacije koji se odnosi na visoku jamstvenu razinu. Razlozi za takva odstupanja trebali bi biti javno dostupni.

(77) Ocjenjivanje sukladnosti postupak je kojim se evaluira jesu li ispunjeni određeni zahtjevi koji se odnose na IKT proizvod, IKT uslugu ili IKT proces. Taj postupak provodi neovisna treća strana koja nije proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa koji se ocjenjuje. Nakon uspješne evaluacije IKT proizvoda, IKT usluge ili IKT procesa trebalo bi izdati europski kibersigurnosni certifikat. Europski kibersigurnosni certifikat trebalo bi smatrati potvrdom da je evaluacija pravilno provedena. Ovisno o jamstvenoj razini, u okviru europskog programa kibersigurnosne certifikacije trebalo bi navesti izdaje li europski kibersigurnosni certifikat privatno ili javno tijelo. Ocjenjivanjem sukladnosti i certifikacijom ne može se samim po sebi jamčiti kibersigurnost certificiranih IKT proizvoda, IKT usluga i IKT procesa. Umjesto toga, riječ je o postupcima i tehničkoj metodologiji kojima se potvrđuje da su IKT proizvodi IKT usluge i IKT procesi testirani i da su u skladu s određenim kibersigurnosnim zahtjevima koji su propisani drugdje, na primjer u tehničkim normama.

(78) Odabir odgovarajuće certifikacije i pripadajućih joj sigurnosnih zahtjeva, koji vrše korisnici europskih kibersigirnosnih certifikata, trebao bi se temeljiti na analizi rizika povezanih s uporabom IKT proizvoda, IKT usluga ili IKT procesa. Slijedom toga, jamstvena razina trebala bi biti razmjerna razini rizika povezanog s predviđenom uporabom IKT proizvoda, IKT usluge ili IKT procesa.

([19]) Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

(79) Europskim programima kibersigurnosne certifikacije moglo bi se osigurati da se ocjenjivanje sukladnosti provodi pod isključivom odgovornošću proizvođača ili pružatelja IKT proizvoda IKT usluga ili IKT procesa („samoocjenjivanje sukladnosti"). U takvim bi slučajevima trebalo biti dovoljno da proizvođač ili pružatelj IKT proizvoda, IKT usluga i IKT procesa sam provodi sve provjere kako bi osigurao da su IKT proizvod, IKT usluga ili IKT proces budu sukladni s europskim programom kibersigurnosne certifikacije. Samoocjenjivanje sukladnosti trebalo bi smatrati primjerenom za IKT proizvode, IKT usluge i IKT procese niske razine složenosti koji predstavljaju nizak rizik za javnost kao što su mehanizmi jednostavnog dizajna i proizvodnje. Osim toga, samoocjenjivanje sukladnosti trebalo bi biti dopušteno samo za IKT proizvode, IKT usluge i IKT procese kada oni odgovaraju osnovnoj jamstvenoj razini.

(80) U okviru europskih programa kibersigurnosne certifikacije moglo bi se omogućiti i samoocjenjivanje sukladnosti i certifikaciju IKT proizvoda, IKT usluga i IKT procesa. U tom slučaju programom bi trebalo osigurati jasan i razumljiv način s pomoću kojeg bi potrošači ili drugi korisnici razlikovali IKT proizvode, IKT usluge i IKT procese s obzirom na to čiji je proizvođač ili pružatelj IKT proizvoda, IKT usluga i IKT procesa odgovoran za ocjenu te IKT proizvode, IKT usluge i IKT procese koje certificira treća strana.

(81) Proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa koji provodi samoocjenjivanje sukladnosti trebao bi moći sastaviti i potpisati EU izjavu o sukladnosti kao dio postupka ocjenjivanja sukladnosti. EU izjava o sukladnosti dokument je u kojem se navodi da određeni IKT proizvod, IKT usluga ili IKT proces ispunjava zahtjeve europskog programa kibersigurnosne certifikacije. Izdavanjem i potpisivanjem EU izjave o sukladnosti proizvođač ili pružatelj IKT proizvoda, IKT usluge ili IKT procesa preuzima odgovornost za sukladnost IKT proizvoda, IKT usluge ili IKT procesa s pravnim zahtjevima europskog programa kibersigurnosne certifikacije. Primjerak EU izjave o sukladnosti trebalo bi podnijeti nacionalnom tijelu za kibersigurnosnu certifikaciju i ENISA-i.

(82) Proizvođači ili pružatelji IKT proizvoda, IKT usluga ili IKT procesa trebali bi EU izjavu o sukladnosti, tehničku dokumentaciju i sve druge informacije o sukladnosti IKT proizvoda, IKT usluga ili IKT procesa s europskim programom kibersigurnosne certifikacije trebali bi držati dostupnom nadležnom nacionalnom tijelu za kibersigurnosnu certifikaciju u razdoblju utvrđenom u relevantnom europskom programu kibersigurnosne certifikacije. U tehničkoj bi dokumentacijom trebalo pobliže odrediti zahtjeve koji se primjenjuju u okviru programa i trebalo bi obuhvatiti dizajn, izrada i funkcioniranje IKT proizvoda, IKT usluge ili IKT procesa u mjeri u kojoj je to relevantno za samoocjenjivanje sukladnosti. Tehničku dokumentaciju trebalo bi sastaviti tako da se omogući ocjena jesu li IKT proizvod, IKT usluga ili IKT proces sukladni s zahtjevima koji se primjenjuju u okviru tog programa.

(83) Pri upravljanju europskim okvirom za kibersigurnosnu certifikaciju uzima se u obzir sudjelovanje država članica te odgovarajuće sudjelovanje dionika i utvrđuje uloga Komisije tijekom planiranja i predlaganja, traženja, izrade, donošenja i preispitivanja europskih programa kibersigurnosne certifikacije.

(84) Komisija bi uz potporu Europske skupine za kibersigurnosnu certifikaciju („ECCG") i Interesne skupine za kibersigurnosnu certifikaciju trebala pripremiti kontinuirani program rada Unije za europsku kibersigurnosnu certifikaciju te nakon otvorenog i širokog savjetovanja i objaviti ga u obliku pravno neobvezujućeg instrumenta. Kontinuirani program rada Unije trebao bi biti strateški dokument kojim se omogućuje industriji, nacionalnim tijelima i tijelima za normizaciju da se unaprijed pripreme za buduće europske programe kibersigurnosne certifikacije. Kontinuirani program rada Unije trebao bi obuhvaćati višegodišnji pregled zahtjeva za izradu prijedloga programa certifikacije koje Komisija namjerava dostaviti ENISA-i na izradu na temelju određenih razloga. Komisija bi kontinuirani program rada Unije trebala uzeti u obzir tijekom izrade svojeg Kontinuiranog plana normizacije IKT-a i zahtjevâ za normizacijom upućenih europskim organizacijama za normizaciju. S obzirom na brzo uvođenje i prihvaćanje novih tehnologija, pojavu prethodno nepoznatih kibersigurnosnih rizika i promjena u zakonodavstvu i na tržištu, Komisija ili ECCG trebali bi imati pravo zatražiti od ENISA-e da izradi prijedloge programa certifikacije koji nisu bili uključeni u kontinuirani program rada Unije. U takvim slučajevima, Komisija i ECCG također bi trebali procijeniti nužnost takvog zahtjeva uzimajući u obzir opće ciljeve ove Uredbe i potrebu osiguravanja kontinuiteta u pogledu planiranja i uporabe resursa ENISA-e.

Nakon takvog zahtjeva ENISA bi trebala izraditi prijedloge programa certifikacije za određene IKT proizvode, IKT usluge ili IKT procese. Komisija bi trebala procijeniti pozitivan i negativan učinak zahtjeva na određeno tržište u pitanju, a posebice njegov učinak u odnosu na mala i srednja poduzeća, na inovacije, na prepreke pristupa tom tržištu i na trošak za krajnje korisnike. Komisija bi na temelju prijedloga programa certifikacije koji je predložila ENISA trebala imati ovlasti donijeti europski program kibersigurnosne certifikacije s pomoću provedbenih akata. Uzimajući u obzir opću svrhu i sigurnosne ciljeve utvrđene u ovoj Uredbi, u europskim programima kibersigurnosne certifikacije koje donosi Komisija trebalo bi odrediti minimalni skup elemenata koji se odnose na predmet, područje primjene i funkcioniranje pojedinačnog programa. Ti elementi trebali bi uključivati, među ostalim, područje primjene i cilj kibersigurnosne certifikacije, uključujući kategorije obuhvaćenih IKT proizvoda, IKT usluga i IKT procesa, detaljnu specifikaciju kibersigurnosnih zahtjeva, na primjer upućivanjem na norme ili tehničke specifikacije, posebne kriterije i metode evaluacije i predviđenu jamstvenu razinu: osnovnu, znatnu ili visoku i prema potrebi, razine evaluacije. ENISA bi trebala moći odbiti zahtjev ECCG-a. Takve odluke trebao bi donositi Upravljački odbor i one bi trebale biti propisno obrazložene.

(85) ENISA bi trebala održavati internetske stranice na kojima se pružaju informacije o europskim programima kibersigurnosne certifikacije i daje im vidljivost, a koje bi, među ostalim, trebale uključivati zahtjeve za izradu prijedloga programa certifikacije kao i povratne informacije dobivene u okviru postupka savjetovanja koje ENISA provodi u pripremnoj fazi. Internetske stranice također bi trebale pružati informacije o europskim kibersigurnosnim certifikatima i EU izjavama o sukladnosti izdanima na temelju ove Uredbe, uključujući informacije o njihovu povlačenju i isteku valjanosti tih europskih kibersigurnosnih certifikata i EU izjava o sukladnosti. Na internetskim stranicama trebali bi se navoditi i oni nacionalni programi kibersigurnosne certifikacije koji su zamijenjeni europskim programom kibersigurnosne certifikacije.

(86) Jamstvena razina europskog programa certifikacije temelj je za povjerenje u to da IKT proizvod, IKT usluga ili IKT proces zadovoljava sigurnosne zahtjeve određenog europskog programa kibersigurnosne certifikacije. Kako bi se osigurala dosljednost europskog okvira za kibersigurnosnu certifikaciju, europskim programom kibersigurnosne certifikacije trebalo bi moći definirati jamstvene razine za europske kibersigurnosne certifikate i EU izjave o sukladnosti izdane u okviru tog programa. Svaki bi se europski kibersigurnosni certifikat mogao odnositi na jednu od jamstvenih razina: osnovnu, znatnu ili visoku, dok bi se EU izjava o sukladnosti mogla odnositi samo na osnovnu jamstvenu razinu. Jamstvene razine osigurale bi odgovarajuću strogoću i opsežnost evaluacije IKT proizvoda, IKT usluge ili IKT procesa i određivalo bi ih upućivanje na tehničke specifikacije, norme i s njima povezane procedure, uključujući tehničke kontrole, čija je svrha ublažiti ili spriječiti incidente. Svaka jamstvena razina trebala bi biti usklađena među različitim sektorima u kojima se primjenjuje certifikacija.

(87) U okviru europskog programa kibersigurnosne certifikacije moglo bi se utvrditi nekoliko razina evaluacije ovisno o strogoći i opsežnosti upotrijebljene metodologije evaluacije. Razine evaluacije trebale bi odgovarati jednoj od jamstvenih razina i trebale bi biti povezane s odgovarajućom kombinacijom sastavnica jamstva. Pri svim jamstvenim razinama IKT proizvod, IKT usluga ili IKT proces trebali bi sadržavati određen broj sigurnih funkcija, kako je predviđeno programom, koje mogu uključivati: sigurnu zadanu konfiguraciju, potpisanu šifru, sigurno ažuriranje i ublažavanje mogućnosti iskorištavanja te potpunu zaštitu stack ili heap memorije. Te bi funkcije trebale biti razvijene i održavati se upotrebom razvojnih pristupa usmjerenih na sigurnost i s njima povezanih alata kako bi se osiguralo da su učinkoviti mehanizmi softvera i hardvera pouzdano ugrađeni.

(88) Za osnovnu jamstvenu razinu evaluacija bi se trebala rukovoditi barem sljedećim sastavnicama jamstva: evaluacija bi trebala uključivati barem pregled tehničke dokumentacije IKT proizvoda, IKT usluge ili IKT procesa od strane tijela za ocjenjivanje sukladnosti. Ako certifikacija uključuje IKT procese, postupak koji se upotrebljava za oblikovanje, razvoj i održavanje IKT proizvoda, IKT usluge ili IKT procesa trebao bi također biti podložan tehničkom preispitivanju. U slučajevima kada se europskim programom kibersigurnosne certifikacije predviđa samoocjenjivanje sukladnosti, trebalo bi biti dovoljno da proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa provede samoocjenjivanje sukladnosti IKT proizvoda, IKT usluga ili IKT procesa s programom certifikacije.

(89) Kad je riječ o znatnoj jamstvenoj razini, evaluacija bi, uz zahtjeve za osnovnu jamstvenu razinu, trebala uključivati barem provjeru sukladnosti sigurnosnih funkcija IKT proizvoda, IKT usluge ili IKT procesa s njegovom tehničkom dokumentacijom.

(90) Kad je riječ o visokoj jamstvenoj razini, evaluacija bi, uz zahtjeve za znatnu jamstvenu razinu, trebala uključivati barem ispitivanje učinkovitosti kojim se procjenjuje otpornost sigurnosnih funkcija IKT proizvoda, IKT usluge ili IKT procesa na napredne kibernapade koje provode osobe koje posjeduju značajne vještine i resurse.

(91) Primjena europske kibersigurnosne certifikacije i EU izjava o sukladnosti trebala bi i dalje biti dobrovoljna, osim ako je u pravu Unije ili pravu država članica donesenom u skladu s pravom Unije predviđeno drugačije. U nedostatku usklađenog prava Unije, države članice mogu donijeti nacionalne tehničke propise kojima se predviđa obvezna certifikacija u okviru europskog programa kibersigurnosne certifikacije u skladu s Direktivom (EU) 2015/1535 Europskog parlamenta i Vijeća ([20]). Države članice također mogu upotrebljavati i europsku kibersigurnosnu certifikaciju u kontekstu javne nabave i Direktive 2014/24/EU Europskog parlamenta i Vijeća ([21]).

(92) U budućnosti bi u nekim područjima moglo biti potrebno odrediti da pojedini kibersigurnosni zahtjevi i njihova certifikacija budu obvezni za određene IKT proizvode, IKT usluge ili IKT procese kako bi se poboljšala razina kibersigurnosti u Uniji. Komisija bi trebala redovito pratiti učinak donesenih europskih programa kibersigurnosne certifikacije na dostupnost sigurnih IKT proizvoda, IKT usluga i IKT procesa na unutarnjem tržištu te bi trebala redovito procjenjivati koliko se proizvođači ili pružatelji IKT proizvoda, IKT usluga ili IKT procesa u Uniji koriste programima certifikacije. Učinkovitost europskih programa kibersigurnosne certifikacije i pitanje bi li određeni programi trebali biti obvezni trebalo bi procijeniti u svjetlu zakonodavstva Unije koje se odnosi na kibersigurnost, a posebno Direktive (EU) 2016/1148 vodeći računa o sigurnosti mrežnih i informacijskih sustava koje upotrebljavaju operatori ključnih usluga.

(93) Europski kibersigurnosni certifikati i EU izjava o sukladnosti trebali bi krajnjim korisnicima pomoći pri donošenju informiranih odluka. IKT proizvodi, IKT usluge i IKT procesi koji su certificirani ili za koje je izdana EU izjava o sukladnosti trebali bi stoga biti popraćeni strukturiranim informacijama koje su prilagođene očekivanoj tehničkoj razini predviđenog krajnjeg korisnika. Sve bi takve informacije trebale biti dostupne na internetu, a, gdje je to primjereno, i u fizičkom obliku. Krajnji korisnik trebao bi imati pristup informacijama o referentnom broju programa certifikacije, jamstvenoj razini, opisu rizikâ povezanih s IKT proizvodom, IKT uslugom ili IKT procesom te tijelu izdavatelja ili preslici europskog kibersigurnosnog certifikata. Osim toga, krajnjeg bi korisnika trebalo obavijestiti o politici kibersigurnosne podrške, odnosno o tome koliko dugo krajnji korisnik može očekivati primati kibersigurnosna ažuriranja ili zakrpe, o proizvođaču ili pružatelju IKT proizvoda, IKT usluga ili IKT procesa. Prema potrebi, trebalo bi pružiti i savjete o radnjama ili postavkama koje krajnji korisnik može provesti kako bi održao ili ojačao kibersigurnost IKT proizvoda ili IKT usluge te podatke za kontakt jedinstvene kontaktne točki za prijavu i potporu u slučaju kibernapada (uz automatsko izvješćivanje). Te bi informacije trebalo redovito ažurirati i trebale bi biti obznanjene na internetskim stranicama koje pružaju informacije o europskim programima kibersigurnosne certifikacije.

(94) Kako bi se ostvarili ciljevi ove Uredbe i izbjegla fragmentacija unutarnjeg tržišta, nacionalni programi kibersigurnosne certifikacije ili postupci za IKT proizvode, IKT usluge i IKT procese obuhvaćene europskim programom kibersigurnosne certifikacije trebali bi prestati biti valjani od datuma koji Komisija odredi provedbenim aktima. Štoviše, države članice ne bi trebale uvoditi nove nacionalne programe kibersigurnosne certifikacije IKT proizvoda, IKT usluga i IKT procesa koji su već obuhvaćeni postojećim europskim programom kibersigurnosne certifikacije. Međutim, države članice ne bi trebalo sprečavati da donesu ili zadrže nacionalne programe certifikacije za potrebe nacionalne sigurnosti.Države članice trebale bi priopćiti Komisiji i ECCG-u svaku namjeru izrade novog nacionalnog programa kibersigurnosne certifikacije. Komisija i ECCG trebali bi procijeniti učinke novog nacionalnog programa kibersigurnosne certifikacije na pravilno funkcioniranje unutarnjeg tržišta i s obzirom na strateški interes da se umjesto toga zatraži europski program kibersigurnosne certifikacije.

(95) Svrha europskih programa kibersigurnosne certifikacije jest da pomognu u usklađivanju kibersigurnosnih praksi u Uniji. Oni trebaju doprinijeti povećanju razine kibersigurnosti u Uniji. Pri osmišljavanju europskih programa kibersigurnosne certifikacije treba voditi računa o razvoju inovacija u području kibersigurnosti te ostaviti prostor za njih.

([20]) Direktiva (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva (SL L 241, 17.9.2015., str. 1.).

([21]) Direktiva 2014/24/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/18/EZ (SL L 94, 28.3.2014., str. 65.).

(96) U okviru europskih programa kibersigurnosne certifikacije trebalo bi uzeti u obzir postojeće metode razvoja softvera i hardvera, a posebno učinak čestih ažuriranja softvera ili ugrađenih programa na pojedinačne europske kibersigurnosne certifikate. U europskim programima kibersigurnosne certifikacije trebalo bi navesti uvjete pod kojima bi se zbog ažuriranja moglo zahtijevati da se IKT proizvod, IKT usluga ili IKT proces ponovno certificiraju ili da se područje primjene određenog europskog kibersigurnosnog certifikata smanji uzimajući u obzir sve moguće štetne učinke ažuriranja na sukladnost sa sigurnosnim zahtjevima tog certifikata.

(97) Nakon donošenja europskog programa kibersigurnosne certifikacije proizvođači ili pružatelji IKT proizvoda, IKT usluga ili IKT procesa trebali bi moći podnijeti zahtjev za certifikaciju svojih IKT proizvoda ili IKT usluga tijelu za ocjenjivanje sukladnosti po svojem izboru bilo gdje u Uniji. Tijela za ocjenjivanje sukladnosti trebalo bi akreditirati nacionalno akreditacijsko tijelo ako ispunjavaju određene zahtjeve propisane ovom Uredbom. Akreditacija bi se trebala izdavati na najviše pet godina i trebala bi se moći obnoviti pod istim uvjetima ako tijelo za ocjenjivanje sukladnosti i nadalje ispunjava zahtjeve. Nacionalna akreditacijska tijela trebala bi ograničiti, suspendirati ili ukinuti akreditaciju tijela za ocjenjivanje sukladnosti ako ono ne ispunjava uvjete za akreditaciju, ili ih je prestalo ispunjavati, ili ako se mjerama koje je poduzelo tijelo za ocjenjivanje sukladnosti krši ova Uredba.

(98) Upućivanja u nacionalnom zakonodavstvu na nacionalne norme koje su prestale proizvoditi učinke zbog stupanja na snagu europskog programa kibersigurnosne certifikacije mogu biti izvor zabune. Države članice trebale bi stoga u svojem nacionalnom zakonodavstvu odraziti donošenje europskog programa kibersigurnosne certifikacije.

(99) Kako bi se postigle istovjetne norme u cijeloj Uniji, olakšalo uzajamno priznavanje i promicalo opće prihvaćanje europskih kibersigurnosnih certifikata i EU izjava o sukladnosti, potrebno je uspostaviti sustav istorazinskog ocjenjivanja među nacionalnim tijelima za kibersigurnosnu certifikaciju. Istorazinsko ocjenjivanje trebalo bi obuhvatiti postupke za nadzor sukladnosti IKT proizvoda, IKT usluga i IKT procesa s europskim kibersigurnosnim certifikatima, za praćenje obveza proizvođača ili pružatelja IKT proizvoda, IKT usluga i IKT procesa koji provode samoocjenjivanje sukladnosti, za praćenje tijelâ za ocjenjivanje sukladnosti te primjerenost stručnog znanja osoblja tijela koja izdaju certifikate za visoku jamstvenu razinu. Komisija bi trebala provedbenim aktom moći utvrditi barem petogodišnji plan istorazinskog ocjenjivanja, kao i definirati kriterije i metodologije za rad sustava istorazinskog ocjenjivanja.

(100) Ne dovodeći u pitanje opći sustav istorazinskog ocjenjivanja koji treba uspostaviti u svim nacionalnim tijelima za kibersigurnosnu certifikaciju, unutar okvira za europsku kibersigurnosnu certifikaciju, određeni europski programi kibersigurnosne certifikacije mogu uključivati mehanizam istorazinske ocjene za tijela koja izdaju europske kibersigurnosne certifikate za IKT proizvode, IKT usluge i IKT procese za visoku jamstvenu razinu u okviru takvih programa.ECCG bi trebao podupirati provedbu takvih mehanizama istorazinske ocjene. Istorazinskim bi ocjenama trebalo konkretno ocijeniti obavljaju li dotična tijela svoje zadaće na usklađen način i one mogu uključivati mehanizme za žalbu. Rezultati istorazinskih ocjena trebali bi biti javno dostupni. Dotična bi tijela mogu donijeti odgovarajuće mjere za prilagodbu svojih praksi i stručnog znanja.

(101) Države članice trebale bi imenovati jedno ili više nacionalnih tijela za kibersigurnosnu certifikaciju u svrhu nadzora usklađenosti s obvezama koje proizlaze iz ove Uredbe. Nacionalno tijelo za kibersigurnosnu certifikaciju može biti novo ili već postojeće tijelo. Država članica također bi trebala moći imenovati, nakon dogovora s drugom državom članicom, jedno ili više nacionalnih tijela za kibersigurnosnu certifikaciju na državnom području te druge države članice.

(102) Nacionalna tijela za kibersigurnosnu certifikaciju posebno bi trebala pratiti i izvršavati obveze proizvođača ili pružatelja IKT proizvoda, IKT usluga i IKT procesa s poslovnim nastanom na njihovu državnom području u vezi s EU izjavom o sukladnosti, trebala bi pomagati nacionalnim tijelima za akreditaciju u praćenju i nadzoru aktivnosti tijela za ocjenjivanje sukladnosti tako što će im pružiti stručno znanje i relevantne informacije, trebala bi ovlastiti tijela za ocjenjivanje sukladnosti za izvršavanje svojih zadaća ako ta tijela ispunjavaju dodatne zahtjeve iz europskog programa kibersigurnosne certifikacije i trebala bi pratiti relevantne promjene u području kibersigurnosne certifikacije. Nacionalna tijela za kibersigurnosnu certifikaciju trebala bi također rješavati pritužbe fizičkih ili pravnih osoba u pogledu europskih kibersigurnosnih certifikata koje su sama izdala ili, u vezi s europskim kibersigurnosnim certifikatima koje su izdala tijela za ocjenjivanje sukladnosti, kada ti certifikati navode visoku

jamstvenu razinu, trebala bi u prikladnoj mjeri istražiti predmet pritužbe te bi u razumnom roku trebala obavijestiti podnositelja pritužbe o napretku i rezultatu istrage. Nadalje, nacionalna tijela za kibersigurnosnu certifikaciju trebala bi surađivati s drugim nacionalnim tijelima za kibersigurnosnu certifikaciju ili s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj neusklađenosti IKT proizvoda, IKT usluga i IKT procesa sa zahtjevima iz ove Uredbe ili s posebnim europskim programima kibersigurnosne certifikacije. Komisija bi trebala olakšati tu razmjenu informacija stavljanjem na raspolaganje općeg elektroničko-informacijskog sustava podrške, primjerice postojećeg Informacijskog i komunikacijskog sustava za tržišni nadzor (ICSMS) i sustava brzog uzbunjivanja za opasne neprehrambene proizvode (RAPEX) kojima se već koriste tijela za nadzor tržišta u skladu s Uredbom (EZ) br. 765/2008.

(103) Radi osiguranja dosljedne primjene europskog okvira za kibersigurnosnu certifikaciju trebalo bi osnovati ECCG koji se sastoji od predstavnika nacionalnih tijela za kibersigurnosnu certifikaciju ili drugih relevantnih nacionalnih tijela. Glavne bi zadaće ECCG-a trebale biti savjetovanje Komisije i pomoć Komisiji u njezinu radu prema osiguranju dosljedne provedbe i primjene europskog okvira za kibersigurnosnu certifikaciju, pomoć ENISA-i i bliska suradnja s njome u izradi prijedloga programâ certifikacije, u propisno opravdanim slučajevima, da od ENISA-e zatraži izradu prijedloga programa certifikacije i donošenje mišljenja upućenih ENISA-i o prijedlozima programa certifikacije te donošenje mišljenja upućenih Komisiji o održavanju i preispitivanju postojećih europskih programa kibersigurnosne certifikacije. ECCG bi trebao olakšati razmjenu dobre prakse i stručnog znanja između raznih nacionalnih tijela za kibersigurnosnu certifikaciju koja su odgovorna za ovlašćivanje tijela za ocjenjivanje sukladnosti i izdavanje europskih kibersigurnosnih certifikata.

(104) S ciljem podizanja svijesti i radi lakšeg prihvaćanja budućih europskih programa kibersigurnosne certifikacije Europska komisija može izdati opće ili sektorske smjernice u području kibersigurnosti, na primjer o dobroj praksi u području kibersigurnosti ili odgovornom ponašanju povezanom s kibersigurnošću, ističući pozitivan učinak uporabe certificiranih IKT proizvoda, IKT usluga i IKT procesa.

(105) Kako bi se dodatno olakšala trgovina i prepoznalo da su lanci opskrbe IKT-a globalni Unija može sklopiti sporazume o uzajamnom priznavanju europskih kibersigurnosnih certifikata u skladu s člankom 218. Ugovora o funkcioniranju Europske unije (UFEU). Komisija može, uzimajući u obzir savjete ENISA-e i Europske skupine za kibersigurnosnu certifikaciju, preporučiti pokretanje relevantnih pregovora. Svakim europskim programom kibersigurnosne certifikacije trebalo bi osigurati posebne uvjete za takve sporazume o uzajamnom priznavanju s trećim zemljama.

(106) Kako bi se osigurali ujednačeni uvjeti za provedbu ove Uredbe, Komisiji bi trebalo dodijeliti provedbene ovlasti. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća ([22]).

(107) Postupak ispitivanja trebao bi se upotrebljavati za donošenje provedbenih akata o europskim programima kibersigurnosne certifikacije za IKT proizvode, IKT usluge i IKT procese, za donošenje provedbenih akata o uređenju za provođenje istraga ENISA-e, za donošenje provedbenih akata o planu istorazinskog ocjenjivanja nacionalnih tijela za kibersigurnosnu certifikaciju te za donošenje provedbenih akata o okolnostima, formatima i postupcima u skladu s kojima nacionalna tijela za kibersigurnosnu certifikaciju Komisiji dostavljaju obavijesti o akreditiranim tijelima za ocjenjivanje sukladnosti.

(108) Rad ENISA-e trebao bi podlijegati redovitoj i neovisnoj evaluaciji. Tom bi evaluacijom trebalo uzeti u obzir ostvaruje li ENISA svoje ciljeve, njezin način rada i relevantnost njezinih zadaća, posebno njezine zadaće u vezi s operativnom suradnjom na razini Unije. Tom bi evaluacijom također trebalo procijeniti i učinak, djelotvornost i učinkovitost europskog okvira za kibersigurnosnu certifikaciju. U slučaju preispitivanja Komisija bi trebala ocijeniti kako se uloga ENISA-e kao referentne točke za savjetovanje i stručno znanje može ojačati te bi također trebala ocijeniti mogućnost za ulogu ENISA-e u podupiranju ocjene IKT proizvoda, IKT usluga i IKT procesa iz trećih zemalja koji nisu usklađeni s pravilima Unije, kada takvi proizvodi, usluge i procesi ulaze u Uniju.

([22]) Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.).

(109) S obzirom na to da ciljeve ove Uredbe ne mogu dostatno ostvariti države članice, nego se oni, zbog opsega ili učinaka djelovanja, na bolji način mogu ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji (UEU). U skladu s načelom proporcionalnosti utvrđenim u tom članku, ova Uredba ne prelazi ono što je potrebno za ostvarivanje tih ciljeva.

(110) Uredbu (EU) br. 526/2013 trebalo bi staviti izvan snage,

DONIJELI SU OVU UREDBU

GLAVA I.

OPĆE ODREDBE

Članak 1.

Predmet i područje primjene

1. S ciljem osiguravanja pravilnog funkcioniranja unutarnjeg tržišta uz istodobno postizanje visoke razine kibersigurnosti, kiberotpornosti i povjerenja u Uniji, ovom se Uredbom utvrđuju:

(a) ciljevi, zadaće i organizacijska pitanja ENISA-e (Agencija Europske unije za kibersigurnost), i

(b) okvir za uspostavu europskih programa kibersigurnosne certifikacije za potrebe osiguranja prikladne razine kibersigurnosti IKT proizvoda, IKT usluga i IKT procesa u Uniji kao i za potrebe izbjegavanja fragmentiranosti unutarnjeg tržišta u pogledu programâ kibersigurnosne certifikacije u Uniji.

Okvir iz prvog podstavka točke (b) primjenjuje se ne dovodeći u pitanje posebne odredbe u drugim pravnim aktima Unije o dobrovoljnoj ili obveznoj certifikaciji.

2. Ovom Uredbom ne dovode se u pitanje nadležnosti država članica u pogledu aktivnosti koje se odnose na javnu sigurnost, obranu, nacionalnu sigurnost i aktivnosti države u područjima kaznenog prava.

Članak 2.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „kibersigurnost” znači sve aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu;

2. „mrežni i informacijski sustav” znači mrežni i informacijski sustav kako je definirano u članku 4. točki 1. Direktive (EU) 2016/1148;

3. „nacionalna strategija za sigurnost mrežnih i informacijskih sustava” znači nacionalna strategija za sigurnost mrežnih i informacijskih sustava kako je definirano u članku 4. točki 3. Direktive (EU) 2016/1148;

4. „operator ključne usluge” znači operator ključne usluge kako je definirano u članku 4. točki 4. Direktive (EU) 2016/1148;

5. „pružatelj digitalnih usluga” znači pružatelj digitalnih usluga kako je definirano u članku 4. točki 6. Direktive (EU) 2016/1148;

6. „incident” znači incident kako je definirano u članku 4. točki 7. Direktive (EU) 2016/1148;

7. „rješavanje incidenta” znači rješavanje incidenta kako je definirano u članku 4. točki 8. Direktive (EU) 2016/1148;

8. „kiberprijetnja” znači svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno utjecati na mrežne i informacijske sustave, korisnike tih sustava i druge osobe.

9. „europski program kibersigurnosne certifikacije” znači sveobuhvatni skup pravila, tehničkih zahtjeva, normi i postupaka, koji su utvrđeni na razini Unije i koji se primjenjuju na certifikaciju ili ocjenjivanje sukladnosti određenih IKT proizvoda, IKT usluga i IKT procesa;

10. „nacionalni program kibersigurnosne certifikacije” znači sveobuhvatan skup pravila, tehničkih zahtjeva, normi i procedura koje je razvilo i donijelo nacionalno javno tijelo i koji se primjenjuju na certifikaciju ili ocjenjivanje sukladnosti IKT proizvoda, IKT usluga i IKT procesa obuhvaćenih područjem primjene tog konkretnog programa;

11. „europski kibersigurnosni certifikat” znači dokument koji je izdalo relevantno tijelo i kojim se potvrđuje da je određeni IKT proizvod, IKT usluga ili IKT proces evaluiran u pogledu toga je li skladu sa specifičnim sigurnosnim zahtjevima utvrđenima u europskom programu kibersigurnosne certifikacije;

12. „IKT proizvod” znači element ili skupina elemenata mrežnih i informacijskih sustava;

13. „IKT usluga” znači usluga koja se u cijelosti ili uglavnom sastoji od prijenosa, pohranjivanja, preuzimanja ili obrade informacija s pomoću mrežnih i informacijskih sustava;

14. „IKT proces” znači skup aktivnosti koje se provode radi oblikovanja, razvoja, ostvarivanja ili održavanja IKT proizvoda ili IKT usluge;

15. „akreditacija” znači akreditacija kako je definirana u članku 2. točki 10. Uredbe (EZ) br. 765/2008;

16. „nacionalno akreditacijsko tijelo” znači nacionalno akreditacijsko tijelo kako je definirano u članku 2. točki 11. Uredbe (EZ) br. 765/2008;

17. „ocjenjivanje sukladnosti” znači ocjenjivanje sukladnosti kako je definirano u članku 2. točki 12. Uredbe (EZ) br. 765/2008;

18. „tijelo za ocjenjivanje sukladnosti” znači tijelo koje obavlja poslove ocjenjivanja sukladnosti kako je definirano u članku 2. točki 13. Uredbe (EZ) br. 765/2008;

19. „norma” znači norma kako je definirana u članku 2. točki 1. Uredbe (EU) br. 1025/2012;

20. „tehnička specifikacija” znači dokument kojim se propisuju tehnički zahtjevi koje IKT proizvod, IKT usluga ili IKT proces trebaju ispunjavati ili postupci ocjenjivanja sukladnosti koji se na njih odnose;

21. „jamstvena razina” znači osnova za povjerenje u to da IKT proizvod, IKT usluga ili IKT proces zadovoljavaju sigurnosne zahtjeve određenog europskog programa kibersigurnosne certifikacije, navodi razinu na kojoj su IKT proizvod, IKT usluga ili IKT proces evaluirani, ali kao takav ne mjeri sigurnost dotičnog IKT proizvoda, IKT usluge ili IKT procesa;

22. „samoocjenjivanje sukladnosti” znači djelovanje koje provodi proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa kojim se evaluira ispunjenjava li taj IKT proizvoda, IKT usluga ili IKT proces zahtjeve utvrđene u određenom europskom programu kibersigurnosne certifikacije.

GLAVA II.

ENISA (AGENCIJA EUROPSKE UNIJE ZA KIBERSIGURNOST)

POGLAVLJE I.

Mandat i ciljevi

Članak 3.

Mandat

1. ENISA obavlja zadaće koje su joj dodijeljene ovom Uredbom u svrhu postizanja visoke zajedničke razine kibersigurnosti diljem Unije, među ostalim aktivnim podupiranjem država članica te institucija, tijela, ureda i agencija Unije u poboljšanju kibersigurnosti. ENISA djeluje kao referentna točka za pružanje savjeta i stručnog znanja o kibersigurnosti institucijama, tijelima, uredima i agencijama Unije te drugim relevantnim dionicima Unije.

ENISA obavljanjem zadaća koje su joj dodijeljene ovom Uredbom doprinosi smanjenju fragmentacije na unutarnjem tržištu.

2. ENISA obavlja zadaće koje su joj dodijeljene pravnim aktima Unije kojima su utvrđene mjere za usklađivanje zakona i drugih propisa država članica koji se odnose na kibersigurnost.

3. Pri obavljanju svojih zadaća ENISA djeluje neovisno te pritom izbjegava udvostručivanje aktivnosti države članice uzimajući u obzir već postojeća stručna znanja države članice.

4. ENISA razvija vlastite resurse, uključujući tehničke i ljudske sposobnosti i vještine koji su joj potrebni za obavljanje zadaća koje su joj dodijeljene ovom Uredbom.

Članak 4.

Ciljevi

1. ENISA djeluje kao centar za stručno znanje u području kibersigurnosti zahvaljujući svojoj neovisnosti, znanstvenoj i tehničkoj kvaliteti savjeta i pomoći koje pruža i informacija koje stavlja na raspolaganje, transparentnosti svojih operativnih postupaka i načina rada te revnosti u obavljanju zadaća.

2. ENISA pomaže institucijama, tijelima, uredima i agencijama Unije te državama članicama u razvoju i provedbi politika Unije povezanih s kibersigurnošću, uključujući sektorske politike o kibersigurnosti.

3. ENISA podupire jačanje kapaciteta i pripravnosti u cijeloj Uniji na način da institucijama, tijelima, uredima i agencijama Unije, kao i državama članicama te javnim i privatnim dionicima pomaže da povećaju zaštitu svojih mrežnih i informacijskih sustava, razviju i poboljšaju kiberotpornost i kapacitete za odgovor te razviju vještine i sposobnosti u području kibersigurnosti.

4. ENISA promiče suradnju, uključujući razmjenu informacija, i koordinaciju na razini Unije među državama članicama, institucijama, tijelima, uredima i agencijama Unije te relevantnim privatnim i javnim dionicima u pitanjima povezanima s kibersigurnošću.

5. ENISA doprinosi povećanju kibersigurnosne sposobnosti na razini Unije kako bi poduprla djelovanja država članica u sprečavanju kiberprijetnji i odgovoru na njih, posebno u slučaju prekograničnih incidenata.

6. ENISA promiče upotrebu europske kibersigurnosne certifikacije radi izbjegavanja fragmentacije unutarnjeg tržišta. ENISA doprinosi uspostavi i održavanju europskog okvira za kibersigurnosnu certifikaciju na razini Unije u skladu s glavom III. ove Uredbe s ciljem povećanja transparentnosti kibersigurnosti IKT proizvoda, IKT usluga i IKT procesa, jačajući time povjerenje u digitalno unutarnje tržište i njegovu konkurentnost.

7. ENISA promiče visoku razinu osviještenosti u pogledu kibersigurnosti, uključujući kiberhigijenu i kiberpismenost građana, organizacija i poduzeća.

POGLAVLJE II.

Zadaće

Članak 5.

Razvoj i provedba politike i prava Unije

ENISA doprinosi razvoju i provedbi politika i prava Unije na sljedeći način:

1. pružanjem pomoći i savjeta za razvoj i preispitivanje politike i prava Unije u području kibersigurnosti te sektorskih inicijativa politike i sektorskih zakonodavnih inicijativa koje uključuju pitanja povezana s kibersigurnošću, osobito pružanjem svojeg neovisnog mišljenja i analize te obavljanjem pripremih radnji;

2. pružanjem pomoći državama članicama u dosljednoj provedbi politika i prava Unije u području kibersigurnosti, posebno u vezi s Direktivom (EU) 2016/1148, među ostalim s pomoću izdavanja mišljenja, smjernica, pružanja savjeta i najbolje prakse o temama kao što su upravljanje rizikom, izvješćivanje o incidentima i razmjena informacija, te olakšavanjem razmjene najbolje prakse među nadležnim tijelima u tom pogledu;

3. pružanjem pomoći državama članicama te institucijama, tijelima, uredima i agencijama Unije u razvoju i promicanju politika kibersigurnosti povezanih s održavanjem općenite dostupnosti ili cjelovitosti javne jezgre otvorenog interneta;

4. doprinosom radu Skupine za suradnju u skladu s člankom 11. Direktive (EU) 2016/1148 pružanjem stručnih savjeta i pomoći;

5. podupiranjem:

   (a) razvoja i provedbe politike Unije u području elektroničkog identiteta i usluga povjerenja, posebno pružanjem savjeta i izdavanjem tehničkih smjernica te olakšavanjem razmjene najbolje prakse među nadležnim tijelima;

   (b) promicanja pojačane razine sigurnosti elektroničkih komunikacija, među ostalim pružanjem savjeta i stručnog znanja te olakšavanjem razmjene najbolje prakse među nadležnim tijelima;

   (c) država članica u provedbi posebnih kibersigurnosnih aspekata politike i prava Unije u vezi sa zaštitom podataka i privatnošću, među ostalim, pružanjem savjeta Europskom odboru za zaštitu podataka na zahtjev;

6. podupiranjem redovitog preispitivanja aktivnosti u okviru politika Unije pripremom godišnjeg izvješća o stanju provedbe pravnog okvira u pogledu sljedećeg:

   (a) informacija o obavijestima država članica o incidentima koje jedinstvene kontaktne točke dostavljaju Skupini za suradnju u skladu s člankom 10. stavkom 3. Direktive (EU) 2016/1148;

   (b) sažecima obavijesti o povredi sigurnosti ili gubitku cjelovitosti zaprimljenih od pružatelja usluga povjerenja koje nadzorna tijela dostavljaju ENISA-i na temelju članka 19. stavka 3. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća ([23]);

   (c) obavijesti o sigurnosnim incidentima koje dostavljaju pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga, a koje nadležna tijela dostavljaju Agenciji, na temelju članka 40. Direktive(EU) 2018/1972.

([23]) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).

Članak 6.

Izgradnja kapaciteta

1. ENISA pomaže:

(a) državama članicama u njihovim nastojanjima da poboljšaju sprečavanje, otkrivanje i analizu kiberprijetnji i kiberincidenata te sposobnost za odgovor na njih osiguravanjem potrebnih znanja i stručnjaka;

(b) državama članicama i institucijama, tijelima, uredima i agencijama Unije u uspostavi i provedbi politika otkrivanja ranjivosti na dobrovoljnoj osnovi;

(c) institucijama, tijelima, uredima i agencijama Unije u njihovim nastojanjima da poboljšaju sprečavanje, otkrivanje i analizu kiberprijetnji i kiberincidenata te da poboljšaju svoje sposobnosti za odgovor na te kiberprijetnje i kiberincidente, osobito pružanjem odgovarajuće potpore CERT- -EU-u;

(d) državama članicama u razvoju CSIRT-ova, ako to zatraže na temelju članka 9. stavka 5. Direktive (EU) 2016/1148;

(e) državama članicama u razvoju nacionalnih strategija za sigurnost mrežnih i informacijskih sustava, ako to zatraže na temelju članka 7. stavka 2. Direktive (EU) 2016/1148 te promiče širenje tih strategija i bilježi napredak njihove provedbe u cijeloj Uniji s ciljem promicanja najbolje prakse;

(f) institucijama Unije u razvoju i preispitivanju strategija Unije u pogledu kibersigurnosti promicanjem njihova širenja i praćenjem napretka u njihovoj provedbi;

(g) nacionalnim CSIRT-ovima i CSIRT-ovima Unije u podizanju njihove razine sposobnosti, među ostalim poticanjem dijaloga i razmjene informacija s ciljem osiguravanja da, s obzirom na najnovija tehnička dostignuća, svaki CSIRT zadovoljava zajednički skup minimalnih sposobnosti i djeluje u skladu s najboljim praksama;

(h) državama članicama redovitim organiziranjem vježbi u području kibersigurnosti na razini Unije iz članka 7. stavka 5. barem svake dvije godine i pružanjem preporuka politike na temelju postupka evaluacije vježbi i stečenog iskustva tijekom tih vježbi;

(i) relevantnim javnim tijelima pružanjem osposobljavanja u području kibersigurnosti, prema potrebi u suradnji s dionicima;

(j) Skupini za suradnju, pri razmjeni najbolje prakse posebno u pogledu identifikacije od strane država članica operatora ključnih usluga na temelju članka 11. stavka 3. točke 1. Direktive (EU) 2016/1148, među ostalim u vezi s prekograničnim ovisnostima u pogledu rizika i incidenata.

2. ENISA podupire razmjenu informacija u i među sektorima, posebno u sektorima navedenima u Prilogu II. Direktivi (EU) 2016/1148, pružanjem najbolje prakse i smjernica o dostupnim alatima, postupku i načinu rješavanja regulatornih pitanja povezanih s razmjenom informacija.

Članak 7.

Operativna suradnja na razini Unije

1. ENISA podupire operativnu suradnju među državama članicama, institucijama, tijelima, uredima i agencijama Unije te među dionicima.

2. ENISA surađuje na operativnoj razini i uspostavlja sinergije s institucijama, tijelima, uredima i agencijama Unije, uključujući CERT-EU, službama koje se bave kiberkriminalitetom i s nadzornim tijelima koja se bave zaštitom privatnosti i osobnih podataka, s ciljem rješavanja pitanja od zajedničkog interesa, među ostalim:

(a) razmjenom znanja i iskustava te najbolje prakse;

(b) pružanjem savjeta i izdavanjem smjernica o relevantnim pitanjima povezanima s kibersigurnošću;

(c) uspostavom praktičnih mehanizama za izvršenje određenih zadaća, nakon savjetovanja s Komisijom.

3. ENISA osigurava tajništvo mreže CSIRT-ova u skladu s člankom 12. stavkom 2. Direktive (EU) 2016/1148 i u tom svojstvu aktivno podupire razmjenu informacija i suradnju među njezinim članovima.

4. ENISA podupire države članice u pogledu operativne suradnje unutar mreže CSIRT-ova:

(a) savjetovanjem o tome kako poboljšati sposobnosti za sprečavanje i otkrivanje incidenata i odgovor na njih te, na zahtjev jedne ili više država članica, pružanjem savjetovanja u vezi s određenom kiberprijetnjom;

(b) pružanjem pomoći, na zahtjev jedne ili više država članica, pri ocjeni incidenata sa značajnim ili bitnim učinkom pružanjem stručnog znanja i olakšavanjem tehničkog rješavanja takvih incidenata, među ostalim posebice podupiranjem dobrovoljne razmjene relevantnih informacija i tehničkih rješenja među državama članicama;

(c) analiziranjem ranjivosti i incidenata na temelju javno dostupnih informacija ili informacija koje su države članice dobrovoljno dostavile u tu svrhu; i

(d) na zahtjev jedne ili više država članica, pružanjem potpore u vezi s ex post tehničkim istragama u pogledu incidenata sa značajnim ili bitnim učinkom u smislu Direktive (EU) 2016/1148.

Pri obavljaju tih zadaća ENISA i CERT-EU uspostavljaju strukturiranu suradnju kako bi ostvarili koristi od sinergija i izbjegli udvostručavanje aktivnosti.

5. ENISA redovito organizira vježbe u području kibersigurnosti na razini Unije i, na njihov zahtjev, podupire države članice i institucije, tijela, ureda i agencije Unije pri organizaciji tih vježbi. Takve vježbe u području kibersigurnosti na razini Unije mogu uključivati tehničke, operativne ili strateške elemente. Jednom u dvije godine ENISA organizira sveobuhvatnu vježba velikog opsega.

Kada je to prikladno, ENISA doprinosi i pomaže u organizaciji sektorskih vježbi u području kibersigurnosti u suradnji s relevantnim organizacijama koje mogu i sudjelovati u vježbama u području kibersigurnosti na razini Unije.

6. ENISA u bliskoj suradnji s državama članicama sastavlja redovito detaljno tehničko izvješće o stanju kibersigurnosti u EU-u u pogledu incidenata i kiberprijetnji na temelju javno dostupnih informacija, vlastite analize i izvješća koje dostavljaju, među ostalim, CSIRT-ovi država članica ili jedinstvene kontaktne točke iz Direktive (EU) 2016/1148, u oba slučaja na dobrovoljnoj osnovi, EC3 te CERT-EU.

7. ENISA doprinosi razvoju zajedničkog odgovora na razini Unije i država članica na prekogranične incidente ili krize velikih razmjera povezane s kibersigurnošću, posebno na sljedeće načine:

(a) objedinjavanjem i analiziranjem izvješća iz nacionalnih izvora koja su dostupna javnosti ili se razmjenjuju na dobrovoljnoj osnovi radi doprinosa zajedničkoj informiranosti o stanju;

(b) osiguravanjem učinkovitog protoka informacija i osiguravanjem mehanizama eskalacije između mreže CSIRT-ova i oblikovatelja tehničkih i političkih odluka na razini Unije;

(c) na zahtjev, olakšavanjem tehničkog rješavanja takvih incidenta ili kriza, uključujući, osobito, podupiranjem dobrovoljne razmjene tehničkih rješenja među državama članicama;

(d) potporom institucijama, tijelima, uredima i agencijama Unije te, na njihov zahtjev, državama članicama u javnoj komunikaciji u vezi s takvim incidentom ili krizom;

(e) ispitivanjem planova suradnje za odgovor na takve incidente i krize na razini Unije i, na njihov zahtjev, podupiranjem država članica u ispitivanju takvih planova na nacionalnoj razini.

Članak 8.

Tržište, kibersigurnosna certifikacija i normizacija

1. ENISA podupire i promiče razvoj i provedbu politike Unije o kibersigurnosnoj certifikaciji IKT proizvoda, IKT usluga i IKT procesa, kako je utvrđeno u glavi III. ove Uredbe na sljedeće načine:

(a) stalnim praćenjem razvoja u povezanim područjima normizacije i preporukom odgovarajućih tehničkih specifikacija za uporabu pri razvoju europskih programa kibersigurnosne certifikacije na temelju članka 54. stavka 1. točke (c)ako norme nisu dostupne;

(b) izradom prijedloga europskih programa kibersigurnosne certifikacije („prijedlozi programa certifikacije") za IKT proizvode, IKT usluge i IKT procese u skladu s člankom 49.;

(c) evaluacijom donesenih europskih programa kibersigurnosne certifikacije u skladu s člankom 49. stavkom 8.;

(d) sudjelovanjem u istorazinskim ocjenjivanjima na temelju članka 59. stavka 4.;

(e) pomaganjem Komisiji u osiguravanju tajništva ECCG-a na temelju članka 62. stavka 5. ove Uredbe.

2. ENISA osigurava tajništvo interesne skupine za kibersigurnosnu certifikaciju na temelju članka 22. stavka 4.

3. ENISA sastavlja i objavljuje smjernice i razvija dobru praksu u pogledu kibersigurnosnih zahtjeva za IKT proizvode, IKT usluge i IKT procese, u suradnji s nacionalnim tijelima za kibersigurnosnu certifikaciju i industrijom na formalan, strukturiran i transparentan način.

4. ENISA doprinosi izgradnji kapaciteta u vezi s postupcima evaluacije i certifikacije sastavljanjem i izdavanjem smjernica te pružanjem potpore državama članicama na njihov zahtjev.

5. ENISA olakšava uspostavu i prihvaćanje europskih i međunarodnih normi za upravljanje rizikom i za sigurnost IKT proizvoda, IKT usluga i IKT procesa.

6. ENISA izrađuje, u suradnji s državama članicama i industrijom, savjeta i smjernica o tehničkim područjima povezanima sa sigurnosnim zahtjevima za operatore ključnih usluga i pružatelje digitalnih usluga, te u pogledu već postojećih normi, uključujući nacionalne norme država članica, u skladu s člankom 19. stavkom 2. Direktive (EU) 2016/1148.

7. ENISA provodi i distribuira redovite analize glavnih trendova na kibersigurnosnom tržištu i na strani ponude i na strani potražnje s ciljem poticanja kibersigurnosnog tržišta u Uniji.

Članak 9.

Znanje i informiranje

ENISA:

(a) provodi analize novih tehnologija i daje tematske procjene očekivanog društvenog, pravnog, gospodarskog i regulatornog učinka tehnoloških inovacija na kibersigurnost;

(b) provodi dugoročne strateške analize kiberprijetnji i incidenata kako bi utvrdila nove trendove i pomogla spriječiti incidente;

(c) u suradnji sa stručnjacima iz tijela država članica i relevantnim dionicima, pruža savjete, smjernice i najbolju praksu za sigurnost mrežnih i informacijskih sustava, posebno za sigurnost infrastruktura kojima se podupiru sektori navedeni u Prilogu II. Direktivi (EU) 2016/1148 te onih kojima se koriste pružatelji digitalnih usluga iz Priloga III. toj Direktivi;

(d) putem posebnog portala objedinjuje, organizira i stavlja na raspolaganje javnosti koje su dostavile institucije, tijela, uredi i agencije Unije te informacije o kibersigurnosti koje su dobrovoljno na raspolaganje stavile države članice i javni i privatni dionici;

(e) prikuplja i analizira javno dostupne informacije o značajnim incidentima i sastavlja izvješća s ciljem pružanja smjernica građanima, organizacijama i poduzećima u cijeloj Uniji.

Članak 10.

Podizanje razine osviještenosti i obrazovanje

ENISA:

(a) podiže razinu osviještenosti javnosti o rizicima povezanima s kibersigurnošću i daje smjernice o dobroj praksi za pojedinačne korisnike usmjerene na građane, organizacije i poduzeća, uključujući kiberhigijenu i kiberpismenost;

(b) u suradnji s državama članicama i institucijama, tijelima, uredima i agencijama Unije te industrijom, organizira redovite informativne kampanje s ciljem povećanja kibersigurnosti i svoje vidljivosti u Uniji te potiče široku javnu raspravu;

(c) pomaže državama članicama u njihovim naporima za podizanje razine osviještenosti o kibersigurnosti i promicanje obrazovanja u području kibersigurnosti;

(d) podupire bliskiju koordinaciju i razmjenu najbolje prakse među državama članicama u pogledu podizanja razine osviještenosti i obrazovanja u vezi s kibersigurnošću.

Članak 11.

Istraživanja i inovacije

U pogledu istraživanja i inovacija, ENISA:

(a) savjetuje institucije, tijela, urede i agencije Unije i države članice o istraživačkim potrebama i prioritetima u području kibersigurnosti kako bi se omogućili učinkoviti odgovori na postojeće i nove rizike i kiberprijetnje, među ostalim i u pogledu novih informacijskih i komunikacijskih tehnologija te onih u nastajanju, te kako bi se učinkovito upotrebljavale tehnologije za sprečavanje rizika;

(b) ako joj je Komisija prenijela relevantne ovlasti, sudjeluje u fazi provedbe programa za financiranje istraživanja i inovacija ili kao korisnik;

(c) doprinosi strateškoj agendi za istraživanja i inovacije na razini Unije u području kibersigurnosti.

Članak 12.

Međunarodna suradnja

ENISA doprinosi nastojanjima Unije da uspostavi suradnju s trećim zemljama i međunarodnim organizacijama kao i u relevantnim okvirima međunarodne suradnje s ciljem promicanja međunarodne suradnje u području kibersigurnosti:

(a) sudjelovanjem, prema potrebi, u ulozi promatrača u organizaciji međunarodnih vježbi, analiziranjem ishoda takvih vježbi i izvješćivanjem Upravljačkog odbora o njihovu ishodu;

(b) na zahtjev Komisije, olakšavanjem razmjene najbolje prakse;

(c) na zahtjev Komisije, pružanjem stručnih savjeta Komisiji;

(d) pružanjem savjeta i potpore Komisiji o pitanjima koja se odnose na sporazume o uzajamnom priznavanju kibersigurnosnih certifikata s trećim zemljama u suradnji sa ECCG-om uspostavljenom na temelju članka 62.

POGLAVLJE III.

Organizacija ENISA-e

Članak 13.

Struktura ENISA-e

Administrativna i upravljačka struktura ENISA-e sastoji se od sljedećeg:

(a) Upravljačkog odbora;

(b) Izvršnog odbora;

(c) izvršnog direktora;

(d) Savjetodavne skupine ENISA-e;

(e) Mreže nacionalnih časnika za vezu.

Odjeljak 1.

Upravljački Odbor

Članak 14.

Sastav Upravljačkog odbora

1. Upravljački odbor sastoji se od po jednog člana imenovanog od strane svake države članice te dva člana koje imenuje Komisija. Svi članovi imaju pravo glasa.

2. Svaki član Upravljačkog odbora ima zamjenika. Taj zamjenik predstavlja člana u slučaju odsutnosti člana.

3. Članove Upravljačkog odbora i njihove zamjenike imenuje se na temelju njihovog znanja u području kibersigurnosti i relevantnih upravljačkih i administrativnih vještina te vještina upravljanja proračunom. Komisija i države članice nastoje ograničiti fluktuaciju svojih predstavnika u Upravljačkom odboru kako bi se osigurao kontinuitet njegova rada. Komisija i države članice nastoje postići rodnu ravnoteža u Upravljačkom odboru.

4. Mandat članova Upravljačkog odbora i njihovih zamjenika traje četiri godine. Taj se mandat može produljiti.

Članak 15.

Funkcije Upravljačkog odbora

1. Upravljački odbor obavlja sljedeće:

(a) utvrđuje opći smjer djelovanja ENISA-e i osigurava da ENISA djeluje u skladu s pravilima i načelima iz ove Uredbe; također osigurava usklađenost rada ENISA-e s aktivnostima koje provode države članice i s onima koje se provode na razini Unije;

(b) donosi nacrt jedinstvenog programskog dokumenta ENISA-e iz članka 24. prije nego što ga podnese Komisiji radi dobivanja mišljenja;

(c) donosi jedinstveni programski dokument ENISA-e, uzimajući u obzir mišljenje Komisije;

(d) nadzire provedbu višegodišnjih i godišnjih programa sadržanih u jedinstvenom programskom dokumentu;

(e) donosi godišnji proračun ENISA-e i izvršava druge funkcije povezane s proračunom ENISA-e u skladu s poglavljem IV.;

(f) ocjenjuje i donosi konsolidirano godišnje izvješće o aktivnostima ENISA-e, u što je uključena računovodstvena dokumentacija i opis ENISA-inog ostvarenja pokazatelja uspješnosti, i do 1. srpnja sljedeće godine dostavlja godišnje izvješće i njegovu ocjenu Europskom parlamentu, Vijeću, Komisiji i Revizorskom sudu te ga objavljuje;

(g) donosi financijska pravila koja se primjenjuju na ENISA-u u skladu s člankom 32.;

(h) donosi strategiju za suzbijanje prijevara koja je razmjerna rizicima od prijevare, uzimajući u obzir analizu troškova i koristi mjera koje će se provoditi;

(i) donosi pravila o sprečavanju sukoba interesa u pogledu svojih članova i o postupanju u slučaju sukoba interesa;

(j) osigurava odgovarajuće daljnje postupanje u vezi s nalazima i preporukama proizišlim iz istraga Europskog ureda za borbu protiv prijevara (OLAF) i različitih unutarnjih ili vanjskih izvješća o reviziji i evaluacija;

(k) donosi svoj poslovnik, uključujući pravila za privremene odluke o delegiranju posebnih zadaća na temelju članka 19. stavka 7.;

(l) u odnosu na osoblje ENISA-e izvršava ovlasti koje su Pravilnikom o osoblju za dužnosnike („Pravilnik o osoblju za dužnosnike") i Uvjetima zaposlenja ostalih službenika Europske unije („Uvjeti zaposlenja ostalih službenika") utvrđenima Uredbom Vijeća (EEZ, Euratom, EZUČ) br. 259/68 ([24]) dodijeljene tijelu nadležnom za imenovanja i tijelu ovlaštenom za sklapanje ugovora o radu („ovlasti tijela nadležnog za imenovanja") u skladu sa stavkom 2. ovog članka;

(m) donosi pravila za provedbu Pravilnika o osoblju za dužnosnike i Uvjeta zaposlenja ostalih službenika u skladu s postupkom iz članka 110. Pravilnika o osoblju za dužnosnike;

(n) imenuje izvršnog direktora i, po potrebi, produljuje njegov mandat ili ga razrješava dužnosti u skladu s člankom 36.;

(o) imenuje računovodstvenog službenika, koji može biti računovodstveni službenik Komisije, koji svoje dužnosti obavlja potpuno neovisno;

(p) donosi sve odluke koje se tiču unutarnjeg ustrojstva ENISA-e te, prema potrebi, o izmjenama tog unutarnjeg ustrojstva, uzimajući u obzir potrebe ENISA-e u pogledu aktivnosti te razumno financijsko upravljanje;

(q) odobrava uspostavu radnih aranžmana u odnosu na Članak 7.;

(r) odobrava uspostavu ili sklapanje radnih aranžmana u skladu s člankom 42.

2. U skladu s člankom 110. Pravilnika o osoblju, upravljački odbor donosi odluku na temelju članka 2. stavka 1. Pravilnika o osoblju za dužnosnike i članka 6. Uvjeta zaposlenja ostalih službenika kojom se odgovarajuće ovlasti tijela nadležnog za imenovanja delegiraju izvršnom direktoru i utvrđuju uvjeti pod kojima se to delegiranje ovlasti može suspendirati. Izvršni direktor ovlašten je dalje delegirati te ovlasti.

([24]) SL L 56, 4.3.1968., str. 1.

3. U iznimnim okolnostima Upravljački odbor može donijeti odluku o privremenoj suspenziji delegiranja ovlasti tijela nadležnog za imenovanja na izvršnog direktora i svih ovlasti i tijela nadležnog za imenovanja koje je izvršni direktor dalje delegirao te ih umjesto toga izvršavati sam ili ih delegirati jednom od svojih članova ili zaposlenika koji nije izvršni direktor.

Članak 16.

Predsjednik Upravljačkog odbora

Upravljački odbor bira svojeg predsjednika i zamjenika predsjednika iz redova svojih članova dvotrećinskom većinom glasova. Njihov mandat traje četiri godine s mogućnošću jednog produljenja. Međutim, ako njihovo članstvo u Upravljačkom odboru prestane u bilo kojem trenutku trajanja njihova mandata, toga datuma automatski prestaje i njihov mandat. Zamjenik predsjednika po službenoj dužnosti zamjenjuje predsjednika ako predsjednik nije u mogućnosti obavljati svoje zadaće.

Članak 17.

Sastanci Upravljačkog odbora

1. Sastanke Upravljačkog odbora saziva njegov predsjednik.

2. Upravljački odbor održava najmanje dva redovita sastanka godišnje. Održava i izvanredne sastanke na zahtjev predsjednika, Komisije ili najmanje jedne trećine svojih članova.

3. Izvršni direktor sudjeluje na sastancima Upravljačkog odbora ali nema pravo glasa.

4. Članovi Savjetodavne skupine ENISA-e mogu na poziv predsjednika sudjelovati na sastancima Upravljačkog odbora, ali nemaju pravo glasa.

5. Članovima Upravljačkog odbora i njihovim zamjenicima na sastancima Upravljačkog odbora mogu pomagati savjetnici ili stručnjaci, podložno Poslovniku Upravljačkog odbora,.

6. ENISA Upravljačkom odboru osigurava tajništvo.

Članak 18.

Pravila o glasovanju Upravljačkog odbora

1. Upravljački odbor donosi svoje odluke većinom glasova svojih članova.

2. Dvotrećinska većina glasova članova Upravljačkog odbora potrebna je za donošenje jedinstvenog programskog dokumenta, godišnjeg proračuna, imenovanje izvršnog direktora te za produljenje njegova mandata ili njegovo razrješenje s dužnosti.

3. Svaki član ima jedan glas. U odsutnosti člana pravo glasa izvršava zamjenik člana.

4. Predsjednik Upravljačkog odbora sudjeluje u glasovanju.

5. Izvršni direktor ne sudjeluje u glasovanju.

6. Poslovnikom Upravljačkog odbora utvrđuju se detaljnija pravila glasovanja, osobito okolnosti u kojima jedan član može djelovati u ime drugog člana.

Odjeljak 2.

Izvršni Odbore

Članak 19.

Izvršni odbor

1. Izvršni odbor pomaže Upravljačkom odboru.

2. Izvršni odbor obavlja sljedeće:

(a) priprema odluke koje donosi Upravljački odbor;

(b) zajedno s Upravljačkim odborom osigurava prikladno daljnje postupanje u vezi s nalazima i preporukama proizišlim iz istraga OLAF-a i različitih unutarnjih ili vanjskih izvješća o reviziji i evaluacija;

(c) ne dovodeći u pitanje odgovornosti izvršnog direktora utvrđene u članku 20., pruža pomoć i savjete izvršnom direktoru u provedbi odluka Upravljačkog odbora o upravnim i proračunskim pitanjima, u skladu s člankom 20.

3. Izvršni odbor sastavljen je od pet članova. Članovi Izvršnog odbora imenuju se iz redova članova Upravljačkog odbora. Jedan od članova je predsjednik Upravljačkog odbora, a može predsjedati i Izvršnim odborom, jedan od članova je predstavnik Komisije. Pri imenovanjima članova Izvršnog odbora nastoji se postići rodna ravnoteža u Izvršnom odboru. Izvršni direktor sudjeluje na sastancima Izvršnog odbora, ali nema pravo glasa.

4. Mandat članova Izvršnog odbora traje četiri godine. Taj se mandat može produljiti.

5. Izvršni se odbor sastaje najmanje jednom u tri mjeseca. Predsjednik Izvršnog odbora saziva dodatne sastanke na zahtjev članova Izvršnog odbora.

6. Upravljački odbor donosi poslovnik Izvršnog odbora.

7. Prema potrebi, Izvršni odbor može u slučaju hitnosti donijeti određene privremene odluke u ime Upravljačkog odbora, osobito o pitanjima povezanima s administrativnim upravljanjem, uključujući suspenziju delegiranja ovlasti tijela nadležnog za imenovanja, i o proračunskim pitanjima. O svim se takvim privremenim odlukama bez nepotrebne odgode obavješćuje Upravljački odbor. Upravljački odbor zatim, najkasnije tri mjeseca nakon njezina donošenja, odlučuje treba li privremenu odluku odobriti ili odbiti. Izvršni odbor ne može u ime Upravljačkog odbora donositi odluke za koje je potrebna dvotrećinska većina članova Upravljačkog odbora.

Odjeljak 3.

Izvršni Direktor

Članak 20.

Dužnosti izvršnog direktora

1. ENISA-om upravlja izvršni direktor koji je neovisan u obavljanju svojih dužnosti. Izvršni direktor odgovara Upravljačkom odboru.

2. Izvršni direktor izvješćuje Europski parlament o izvršavanju svojih dužnosti kada ga se pozove da to učini. Vijeće može pozvati izvršnog direktora da ga izvijesti o izvršavanju svojih dužnosti.

3. Izvršni direktor odgovoran je za sljedeće:

(a) svakodnevno upravljanje ENISA-om;

(b) provedbu odluka koje je donio Upravljački odbor;

(c) izradu nacrta jedinstvenog programskog dokumenta i njegovo podnošenje Upravljačkom odboru na odobrenje prije podnošenja Komisiji;

(d) provedbu jedinstvenog programskog dokumenta i izvješćivanje Upravljačkog odbora o njegovoj provedbi;

(e) izradu konsolidiranog godišnjeg izvješća o aktivnostima ENISA-e uključujući provedbu godišnjeg programa rada ENISA-e i njegovo dostavljanje Upravljačkom odboru na ocjenjivanje i donošenje;

(f) izradu akcijskog plana koji se nadovezuje na zaključke naknadnih evaluacija i izvješćivanje Komisije o napretku svake dvije godine;

(g) izradu akcijskog plana koji se nadovezuje na zaključke iz izvješća o unutarnjoj ili vanjskoj reviziji i istraga OLAF-a i izvješćivanje Komisije o napretku dva puta godišnje te redovito izvješćivanje Upravljačkog odbora;

(h) izradu nacrta financijskih pravila iz članka 32. koja se primjenjuju na ENISA-u;

(i) izradu nacrta izvješća ENISA-e o procjeni prihoda i rashoda i izvršavanje njezina proračuna;

(j) zaštitu financijskih interesa Unije primjenom preventivnih mjera za borbu protiv prijevara, korupcije i drugih nezakonitih aktivnosti, izvršavanjem djelotvornih provjera i, ako se otkriju nepravilnosti, povratom nepropisno isplaćenih iznosa i, prema potrebi, izricanjem učinkovitih, proporcionalnih i odvraćajućih administrativnih i novčanih kazni;

(k) izradu strategije ENISA-e za borbu protiv prijevara i njezino podnošenje Upravljačkom odboru na odobrenje;

(l) uspostavljanje i održavanje kontakta s poslovnom zajednicom i organizacijama potrošača radi osiguravanja redovitog dijaloga s relevantnim dionicima;

(m) redovitu razmjenu informacija s institucijama, tijelima, uredima i agencijama Unije u pogledu svojih aktivnosti povezanih sa kibersigurnošću kako bi se osigurala usklađenost u razvoju i provedbi politike Unije;

(n) obavljanje drugih zadaća dodijeljenih izvršnom direktoru ovom Uredbom.

4. Prema potrebi i u okviru mandata ENISA-e te u skladu s ciljevima i zadaćama ENISA-e, izvršni direktor može osnovati ad hoc radne skupine sastavljene od stručnjaka, uključujući stručnjake iz nadležnih tijela država članica. Izvršni direktor o tome unaprijed obavješćuje Upravljački odbor. Postupci koji se odnose posebno na sastav radnih skupina, imenovanje stručnjaka u radne skupine koje obavlja izvršni direktor i rad radnih skupina utvrđuju se unutarnjim pravilnikom o radu ENISA-e.

5. Prema potrebi, u svrhu obavljanja zadaća ENISA-e na učinkovit i djelotvoran način i na temelju odgovarajuće analize troškova i koristi, izvršni direktor može odlučiti osnovati jedan ili više lokalnih ureda u jednoj ili više država članica. Prije odluke o osnivanju lokalnog ureda izvršni direktor traži mišljenje dotične države članice ili više njih, uključujući državu članicu u kojoj se nalazi sjedište ENISA-e te mora dobiti prethodnu suglasnost Komisije i Upravljačkog odbora. U slučaju neslaganja tijekom postupka savjetovanja između izvršnog direktora i dotičnih država članica to se pitanje podnosi Vijeću na raspravu. Ukupan broj osoblja u svim lokalnim uredima svodi se na najmanju moguću mjeru i ne smije prelaziti 40 % ukupnog broja osoblja ENISA-e koje se nalazi u državi članici u kojoj se nalazi sjedište ENISA-e. Broj osoblja u svakom lokalnom uredu ne prelazi 10 % ukupnog broja osoblja ENISA-e koje se nalazi u državi članici u kojoj se nalazi sjedište ENISA-e.

U odluci o osnivanju lokalnog ureda utvrđuje se opseg aktivnosti koje će obavljati taj lokalni ured na način da se izbjegnu nepotrebni troškovi i udvostručavanje administrativnih zadaća ENISA-e.

Odjeljak 4.

Savjetodavna Skupina ENISA-e, Interesna Skupina za Kibersigurnosnu Certifikaciju i Mreža Nacionalnih Časnika za Vezu

Članak 21.

Savjetodavna skupina ENISA-e

1. Upravljački odbor, djelujući na prijedlog izvršnog direktora, na transparentan način osniva Savjetodavnu skupinu ENISA-e sastavljenu od priznatih stručnjaka koji zastupaju relevantne interesne skupine, kao što su IKT industrija, pružatelji elektroničkih komunikacijskih mreža ili usluga dostupnih javnosti, MSP-ovi, operatori ključnih usluga, skupine potrošača, akademski stručnjaci za kibersigurnost i predstavnici nadležnih tijela prijavljenih u skladu s Direktivom (EU) 2018/1972 i europskih organizacija za normizaciju te od tijela za izvršavanje zakonodavstva i tijela za nadzor zaštite podataka. Upravljački odbor nastoji osigurati odgovarajuću rodnu i geografsku ravnotežu te ravnotežu među različitim interesnim skupinama.

2. Postupci koji se odnose na Savjetodavnu skupinu ENISA-e, posebno u pogledu njezina sastava, prijedloga izvršnog direktora iz stavka 1., broja i imenovanja njezinih članova i rada Savjetodavne skupine ENISA-e utvrđuju se u unutarnjem pravilniku o radu ENISA-e te se objavljuju.

3. Savjetodavnom skupinom ENISA-e predsjeda izvršni direktor ili bilo koja osoba koju, zasebno za svaki slučaj, imenuje izvršni direktor.

4. Mandat članova Savjetodavne skupine ENISA-e traje dvije i pol godine. Članovi Upravljačkog odbora ne mogu biti članovi Savjetodavne skupine ENISA-e. Stručnjaci Komisije i država članica imaju pravo nazočiti sjednicama Savjetodavne skupine ENISA-e i sudjelovati u njezinu radu. Na sastanke Savjetodavne skupine ENISA-e i sudjelovanje u njezinu radu mogu se pozvati predstavnici drugih tijela koja izvršni direktor smatra relevantnima i koji nisu članovi Savjetodavne skupine ENISA-e.

5. Savjetodavna skupina ENISA-e savjetuje Agenciju u vezi s obavljanjem aktivnosti ENISA-e, osim u pogledu primjene odredbi glave III. ove Uredbe. Ona posebno savjetuje izvršnog direktora u vezi s izradom prijedloga godišnjeg programa rada ENISA-e i osiguravanjem komunikacije s relevantnim interesnim skupinama o pitanjima koja se odnose na godišnji program rada.

6. Savjetodavna skupina ENISA-e redovito obavještava Upravljački odbor o svojim aktivnostima.

Članak 22.

Interesna skupina za kibersigurnosnu certifikaciju

1. Osniva se interesna skupina za kibersigurnosnu certifikaciju.

2. Interesna skupina za kibersigurnosnu certifikaciju sastoji se od članova odabranih među priznatim stručnjacima koji predstavljaju relevantne dionike. Komisija nakon transparentnog i otvorenog poziva, na prijedlog ENISA-a odabire članove Interesne skupine za kibersigurnosnu certifikaciju osiguravajući ravnotežu među različitim interesnim skupinama kao i odgovarajuću rodnu i geografsku ravnotežu.

3. Interesna skupina za kibersigurnosnu certifikaciju:

(a) pruža savjete Komisiji o strateškim pitanjima u vezi s europskim okvirom za kibersigurnosnu certifikaciju;

(b) na zahtjev, pruža savjete Agenciji o općim i strateškim pitanjima koja se odnose na zadaće ENISA-e u vezi s tržištem, kibersigurnosnom certifikacijom i normizacijom;

(c) pruža pomoć Komisiji u pripremi kontinuiranog programa rada Unije iz članka 47.;

(d) izdaje mišljenja o kontinuiranom programu rada Unije na temelju članka 47. stavka 4. i

(e) u hitnim slučajevima, daje savjete Komisiji i ECCG-u o potrebi za dodatnim programima certifikacije koji nisu uključeni u kontinuirani program rada Unije, kako je navedeno u člancima 47. i 48.

4. Interesnom skupinom za kibersigurnosnu certifikaciju supredsjedaju Komisija i ENISA, a tajništvo joj osigurava ENISA.

Članak 23.

Mreža nacionalnih časnika za vezu

1. Upravljački odbor, odlučujući na prijedlog izvršnog direktora, uspostavlja mrežu nacionalnih časnika za vezu sastavljenu od svih država članica (nacionalni časnici za vezu). Svaka država članica imenuje jednog predstavnika u mrežu nacionalnih časnika za vezu. Sastanci mreže nacionalnih časnika za vezu mogu se održavati u različitim sastavima stručnjaka.

2. Mreža nacionalnih časnika za vezu posebice olakšava razmjenu informacija između ENISA-e i država članica te podržava ENISA-u u širenju njezinih aktivnosti, nalaza i preporuka relevantnim dionicima diljem Unije.

3. Nacionalni časnici za vezu djeluju kao kontaktna točka na nacionalnoj razini kako bi se olakšala suradnja između ENISA-e i nacionalnih stručnjaka u kontekstu provedbe godišnjeg programa rada ENISA-e.

4. Iako nacionalni časnici za vezu usko surađuju s predstavnicima svojih država članica u Upravljačkom odboru, radom mreže nacionalnih časnika za vezu ne udvostručuje se rad Upravljačkog odbora ni drugih foruma Unije.

5. Funkcije i postupci za mrežu nacionalnih časnika za vezu utvrđuju se u unutarnjem pravilniku o radu ENISA-e i javno obznanjuju.

Odjeljak 5.

Djelovanje

Članak 24.

Jedinstveni programski dokument

1. ENISA djeluje u skladu s jedinstvenim programskim dokumentom koji sadržava njezine godišnje i višegodišnje programe koji uključuju sve njezine planirane aktivnosti.

2. Izvršni direktor svake godine izrađuje nacrt jedinstvenog programskog dokumenta koji sadržava godišnje i višegodišnje programe s odgovarajućim planovima u pogledu financijskih i ljudskih resursa u skladu s člankom 32. Delegirane uredbe Komisije (EU) br. 1271/2013 ([25]) i uzimajući u obzir smjernice koje je utvrdila Komisija.

3. Do 30. studenoga svake godine Upravljački odbor donosi jedinstveni programski dokument iz stavka 1. te ga do 31. siječnja sljedeće godine šalje Europskom parlamentu, Vijeću i Komisiji, kao i sve naknadne ažurirane verzije tog dokumenta.

4. Jedinstveni programski dokument postaje konačan nakon konačnog donošenja općeg proračuna Unije te se odgovarajuće prilagođava.

([25]) Delegirana uredba Komisije (EU) br. 1271/2013 od 30. rujna 2013. o Okvirnoj financijskoj uredbi za tijela iz članka 208. Uredbe (EU, Euratom) br. 966/2012 Europskog parlamenta i Vijeća (SL L 328, 7.12.2013., str. 42.).

5. Godišnji program rada obuhvaća detaljne ciljeve i očekivane rezultate, uključujući pokazatelje uspješnosti. Sadržava i opis aktivnosti koje je potrebno financirati i podatke o financijskim i ljudskim resursima dodijeljenima svakoj aktivnosti, u skladu s načelima pripreme proračuna i upravljanja na temelju aktivnosti. Godišnji program rada usklađen je s višegodišnjim programom rada iz stavka 7. U njemu su jasno navedene zadaće koje su dodane, izmijenjene ili izbrisane u odnosu na prethodnu financijsku godinu.

6. Upravljački odbor mijenja doneseni godišnji program rada ako je ENISA-i dodijeljena nova zadaća. Sve znatne izmjene godišnjeg programa rada donose se po istom postupku kao i početni godišnji program rada. Upravljački odbor može ovlast za donošenje manjih izmjena godišnjeg programa rada delegirati izvršnom direktoru.

7. U višegodišnjem programu rada utvrđuje se opći strateški program, među ostalim i ciljevi, očekivani rezultati i pokazatelji uspješnosti. Sadržava i programiranje resursa, uključujući višegodišnji proračun i osoblje.

8. Programiranje resursa ažurira se svake godine. Strateški program ažurira se prema potrebi, a posebno kada je to nužno kako bi se uzeo u obzir ishod evaluacije iz članka 67.

Članak 25.

Izjava o interesu

1. Članovi Upravljačkog odbora, izvršni direktor i službenici koje su države članice privremeno uputile daju izjavu o obvezama i izjavu o nepostojanju ili postojanju bilo kakvog izravnog ili neizravnog interesa za koji bi se moglo smatrati da dovodi u pitanje njihovu neovisnost. Izjave su točne i potpune, daju se svake godine u pisanom obliku i ažuriraju se prema potrebi.

2. Članovi Upravljačkog odbora, izvršni direktor i vanjski stručnjaci koji sudjeluju u ad hoc radnim skupinama daju, najkasnije na početku svakog sastanka, točnu i potpunu izjavu o svim interesima za koje bi se moglo smatrati da dovode u pitanje njihovu neovisnost u pogledu točaka dnevnog reda i suzdržavaju se od sudjelovanja u raspravi i glasovanja o takvim točkama.

3. ENISA u svojem unutarnjem pravilniku o radu utvrđuje praktična rješenja za pravila o izjavama o interesima iz stavaka 1. i 2.

Članak 26.

Transparentnost

1. ENISA obavlja svoje aktivnosti uz visok stupanj transparentnosti i u skladu s člankom 28.

2. ENISA osigurava da javnost i sve zainteresirane strane dobiju odgovarajuće, objektivne, pouzdane i lako dostupne informacije, posebno u pogledu rezultata njezina rada. Ona javno obznanjuje i izjave o interesima dane u skladu s člankom 25.

3. Upravljački odbor na prijedlog izvršnog direktora može zainteresiranim stranama odobriti da u svojstvu promatrača sudjeluju u određenim aktivnostima ENISA-e.

4. ENISA u svojem unutarnjem pravilniku o radu utvrđuje praktična rješenja za provedbu pravila o transparentnosti iz stavaka 1. i 2.

Članak 27.

Povjerljivost

1. Ne dovodeći u pitanje Članak 28., ENISA trećim stranama ne otkriva informacije koje obrađuje ili prima, a za koje je podnesen opravdan zahtjev da s njima postupa kao s povjerljivim informacijama.

2. Članovi Upravljačkog odbora, izvršni direktor, članovi Savjetodavne skupine ENISA-e, vanjski stručnjaci koji sudjeluju u radu ad hoc radnih skupina i članovi osoblja ENISA-e, uključujući službenike koje privremeno upućuju države članice, poštuju zahtjeve u pogledu povjerljivosti iz članka 339. UFEU-a čak i nakon prestanka njihovih dužnosti.

3. ENISA u svojem unutarnjem pravilniku o radu utvrđuje praktična rješenja za provedbu pravila o povjerljivosti iz stavaka 1. i 2.

4. Ako je to potrebno za obavljanje zadaća ENISA-e, Upravljački odbor donosi odluku kojom ENISA-i dopušta obradu klasificiranih podataka. U tom slučaju ENISA u dogovoru sa službama Komisije donosi sigurnosna pravila primjenjujući načela sigurnosti utvrđena odlukama Komisije (EU, Euratom) 2015/443 ([26]) i 2015/444 ([27]). Ta sigurnosna pravila uključuju odredbe o razmjeni, obradi i pohrani klasificiranih podataka.

Članak 28.

Pristup dokumentima

1. Na dokumente koje posjeduje ENISA primjenjuje se Uredba (EZ) br. 1049/2001.

2. Upravljački odbor donosi pravila za provedbu Uredbe (EZ) br. 1049/2001 do 28. prosinca 2019.

3. Odluke koje ENISA donosi u skladu s člankom 8. Uredbe (EZ) br. 1049/2001 mogu biti predmetom pritužbe Europskom ombudsmanu u skladu s člankom 228. UFEU-a ili tužbe pred Sudom Europske unije u skladu s člankom 263. UFEU-a.

POGLAVLJE IV.

Donošenje i struktura proračuna ENISA-e

Članak 29.

Donošenje proračuna ENISA-e

1. Izvršni direktor svake godine izrađuje nacrt izvješća o procjenama prihoda i rashoda ENISA-e za sljedeću financijsku godinu te ga prosljeđuje Upravljačkom odboru zajedno s nacrtom plana radnih mjesta. Prihodi i rashodi moraju biti u ravnoteži.

2. Upravljački odbor svake godine, na temelju nacrta izvješća o procjenama, sastavlja izvješće o procjenama prihoda i rashoda ENISA-e za sljedeću financijsku godinu.

3. Upravljački odbor svake godine do 31. siječnja Komisiji i trećim zemljama s kojima je Unija sklopila sporazume u skladu s člankom 42. stavkom 2. šalje izvješće o procjenama koje je dio nacrta jedinstvenog programskog dokumenta.

4. Na temelju navedenog izvješća o procjenama Komisija procjene koje smatra potrebnima za plan radnih mjesta i iznos doprinosa na teret općeg proračuna Unije unosi u nacrt općeg proračuna Unije, koji podnosi Europskom parlamentu i Vijeću u skladu s člankom 314. UFEU-a.

5. Europski parlament i Vijeće odobravaju dodjelu sredstava za doprinose Unije ENISA-i.

6. Europski parlament i Vijeće donose plan radnih mjesta ENISA-e.

([26]) Odluka Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji (SL L 72, 17.3.2015., str. 41.).
([27]) Odluka Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 72, 17.3.2015., str. 53.).

7. Upravljački odbor donosi proračun ENISA-e zajedno s jedinstvenim programskim dokumentom. Proračun ENISA-e postaje konačan nakon konačnog donošenja općeg proračuna Unije. Upravljački odbor prema potrebi prilagođava proračun i jedinstveni programski dokument ENISA-e u skladu s općim proračunom Unije.

Članak 30.

Struktura proračuna ENISA-e

1. Ne dovodeći u pitanje druge izvore, prihodi ENISA-e uključuju sljedeće:

(a) doprinos iz općeg proračuna Unije;

(b) namjenske prihode za određene stavke rashoda u skladu s financijskim pravilima iz članka 32.;

(c) financijska sredstva Unije u obliku sporazuma o delegiranju ili ad hoc bespovratnih sredstava u skladu s njezinim financijskim pravilima iz članka 32. i u skladu s odredbama relevantnih instrumenata kojima se podupiru politike Unije;

(d) doprinose trećih zemalja koje sudjeluju u radu ENISA-e kako je predviđeno u članku 42.;

(e) sve dobrovoljne doprinose država članica u novcu ili naravi.

Države članice koje daju dobrovoljne doprinose iz prvog podstavka točke (e) ne mogu na temelju toga zahtijevati nikakva posebna prava ili usluge.

2. Rashodi ENISA-e uključuju troškove osoblja, troškove administrativne i tehničke podrške, infrastrukturne i operativne troškove te troškove proizišle iz ugovora s trećim stranama.

Članak 31.

Izvršenje proračuna ENISA-e

1. Izvršni direktor odgovoran je za izvršenje proračuna ENISA-e.

2. Unutarnji revizor Komisije ima iste ovlasti u odnosu na ENISA-u kao i u odnosu na službe Komisije.

3. Računovodstveni službenik ENISA-e dostavlja privremenu računovodstvenu dokumentaciju za financijsku godinu (godina N) računovodstvenom službeniku Komisije i Revizorskom sudu do 1. ožujka sljedeće financijske godine (godina N + 1).

4. Po primitku opažanja Revizorskog suda o privremenoj računovodstvenoj dokumentaciji ENISA-e na temelju članka 246. Uredbe (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća ([28]), računovodstveni službenik ENISA-e izrađuje završnu računovodstvenu dokumentaciju ENISA-e pod vlastitom odgovornošću i šalje je Upravljačkom odboru radi mišljenja.

5. Upravljački odbor donosi mišljenje o završnoj računovodstvenoj dokumentaciji ENISA-e.

6. Do 31. ožujka godine N + 1, izvršni direktor prosljeđuje izvješće o proračunskom i financijskom upravljanju Europskom parlamentu, Vijeću, Komisiji i Revizorskom sudu.

7. Do 1. srpnja godine N + 1 računovodstveni službenik ENISA-e podnosi završnu računovodstvenu dokumentaciju ENISA-e zajedno s mišljenjem Upravljačkog odbora Europskom parlamentu, Vijeću, računovodstvenom službeniku Komisije i Revizorskom sudu.

([28]) Uredba (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o financijskim pravilima koja se primjenjuju na opći proračun Unije, o izmjeni uredaba (EU) br. 1296/2013, (EU) br. 1301/2013, (EU) br. 1303/2013, (EU) br. 1304/2013, (EU) br. 1309/2013, (EU) br. 1316/2013, (EU) br. 223/2014, (EU) br. 283/2014 i Odluke br. 541/2014/EU te o stavljanju izvan snage Uredbe (EU, Euratom) br. 966/2012 (SL L 193, 30.7.2018., str. 1.).

8. Na dan slanja završne računovodstvene dokumentacije ENISA-e računovodstveni službenik ENISA-e Revizorskom sudu šalje i izjavu povezanu s tom završnom računovodstvenom dokumentacijom, a presliku šalje i računovodstvenom službeniku Komisije.

9. Do 15. studenoga godine N + 1 izvršni direktor objavljuje završnu računovodstvenu dokumentaciju ENISA-e u *Službenom listu Europske unije.*

10. Do 30. rujna godine N + 1 izvršni direktor Revizorskom sudu šalje odgovor na njegova opažanja, a presliku tog odgovora šalje i Upravljačkom odboru i Komisiji.

11. Izvršni direktor dostavlja Europskom parlamentu, na njegov zahtjev, sve informacije potrebne za nesmetanu primjenu postupka davanja razrješnice za dotičnu financijsku godinu u skladu s člankom 261. stavkom 3. Uredbe (EU, Euratom) 2018/1046.

12. Na preporuku Vijeća Europski parlament prije 15. svibnja godine N + 2 daje razrješnicu izvršnom direktoru u vezi s izvršenjem proračuna za godinu N.

Članak 32.

Financijska pravila

Financijska pravila koja se primjenjuju na ENISA-u donosi Upravljački odbor nakon savjetovanja s Komisijom. Ona ne odstupaju od Delegirane uredbe (EU) br. 1271/2013, osim ako je to odstupanje posebno potrebno za rad ENISA-e i ako je Komisija prethodno dala suglasnost.

Članak 33.

Borba protiv prijevara

1. Kako bi se olakšala borba protiv prijevara, korupcije i drugih nezakonitih aktivnosti u skladu s Uredbom (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća ([29]), ENISA do 28. prosinca 2019. pristupa Međuinstitucionalnom sporazumu od 25. svibnja 1999. između Europskog parlamenta, Vijeća Europske unije i Komisije Europskih zajednica u vezi s internim istragama koje provodi Europski ured za borbu protiv prijevara (OLAF) ([30]). ENISA donosi odgovarajuće odredbe primjenjive na sve zaposlenike ENISA-e, koristeći se obrascem utvrđenim u prilogu tom Sporazumu.

2. Revizorski sud ovlašten je provoditi reviziju, na temelju dokumenata i inspekcija na terenu, svih korisnika bespovratnih sredstava, ugovaratelja i podugovaratelja koji su primili sredstva Unije od ENISA-e.

3. OLAF može provoditi istrage, među ostalim provjere i inspekcije na terenu, u skladu s odredbama i postupcima propisanima Uredbom (EU, Euratom) br. 883/2013 i Uredbom Vijeća (Euratom, EZ) br. 2185/96 ([31]), kako bi utvrdio je li došlo do prijevare, korupcije ili bilo koje druge nezakonite aktivnosti koja utječe na financijske interese Unije u vezi s bespovratnim sredstvima ili ugovorom koji financira ENISA.

4. Ne dovodeći u pitanje stavke 1., 2. i 3., sporazumi o suradnji s trećim zemljama i međunarodnim organizacijama, ugovori, sporazumi o bespovratnim sredstvima i odluke ENISA-e o bespovratnim sredstvima sadržavaju odredbe kojima se Revizorskom sudu i OLAF-u daje izričita ovlast za provođenje tih revizija i istraga u skladu s njihovim nadležnostima.

([29]) Uredba (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća od 11. rujna 2013. o istragama koje provodi Europski ured za borbu protiv prijevara (OLAF) i stavljanju izvan snage Uredbe (EZ) br. 1073/1999 Europskog parlamenta i Vijeća te Uredbe Vijeća (Euratom) br. 1074/1999 (SL L 248, 18.9.2013., str. 1.).

([30]) SL L 136, 31.5.1999., str. 15.

([31]) Uredba Vijeća (Euratom, EZ) br. 2185/96 od 11. studenoga 1996. o provjerama i inspekcijama na terenu koje provodi Komisija s ciljem zaštite financijskih interesa Europskih zajednica od prijevara i ostalih nepravilnosti (SL L 292, 15.11.1996., str. 2.).

POGLAVLJE V.

Osoblje

Članak 34.

Opće odredbe

Na osoblje ENISE-e primjenjuju se Pravilnik o osoblju za dužnosnike i Uvjeti zaposlenja ostalih službenika te pravila koja su na temelju zajedničkog dogovora donijele institucije Unije radi primjene Pravilnika o osoblju za dužnosnike i Uvjeta zaposlenja ostalih službenika.

Članak 35.

Povlastice i imuniteti

Na ENISA-u i njezino osoblje primjenjuje se Protokol br. 7 o povlasticama i imunitetima Europske unije, koji je priložen UEU-u i UFEU-u.

Članak 36.

Izvršni direktor

1. Izvršni direktor zapošljava se kao privremeni djelatnik ENISA-e u skladu s člankom 2. točkom (a) Uvjeta zaposlenja ostalih službenika.

2. Izvršnog direktora imenuje Upravljački odbor nakon otvorenog i transparentnog postupka odabira s popisa kandidata koje je predložila Komisija.

3. Za potrebe sklapanja ugovora o radu s izvršnim direktorom ENISA-u zastupa predsjednik Upravljačkog odbora.

4. Kandidat kojeg je odabrao Upravljački odbor poziva se prije imenovanja da pred relevantnim odborom Europskog parlamenta da izjavu i odgovori na pitanja njegovih članova.

5. Mandat izvršnoga direktora traje pet godina. Do kraja tog razdoblja Komisija provodi procjenu uspješnosti izvršnog direktora te budućih izazova i zadaća ENISA-e.

6. Upravljački odbor donosi odluku o imenovanju, produljenju mandata ili razrješenju dužnosti izvršnoga direktora u skladu s člankom 18. stavkom 2.

7. Upravljački odbor, na prijedlog Komisije kojim se uzima u obzir procjena iz stavka 5., može jedanput produljiti mandat izvršnoga direktora za razdoblje od pet godina.

8. Upravljački odbor obavješćuje Europski parlament o svojoj namjeri da produlji mandat izvršnoga direktora. U roku od tri mjeseca prije takvog produljenja izvršni direktor, ako ga se na to pozove, daje izjavu pred relevantnim odborom Europskog parlamenta i odgovara na pitanja njegovih članova.

9. Izvršni direktor čiji je mandat produljen ne smije sudjelovati u još jednom postupku odabira za isto radno mjesto.

10. Izvršni direktor može biti razriješen dužnosti samo na temelju odluke Upravljačkog odbora, koji djeluje na prijedlog Komisije.

Članak 37.

Upućeni nacionalni stručnjaci i ostalo osoblje

1. ENISA može angažirati upućene nacionalne stručnjake ili drugo osoblje koje nije zaposleno u ENISA-i. Na to se osoblje ne primjenjuju Pravilnik o osoblju za dužnosnike i Uvjeti zaposlenja ostalih službenika.

2. Upravljački odbor donosi odluku o utvrđivanju pravila za upućivanje nacionalnih stručnjaka u ENISA-u.

POGLAVLJE VI.

Opće odredbe o ENISA-i

Članak 38.

Pravni status ENISA-e

1. ENISA je tijelo Unije i ima pravnu osobnost.

2. ENISA u svakoj državi članici ima najširu pravnu sposobnost koja se pravnim osobama priznaje nacionalnim pravom. ENISA konkretno može stjecati ili otuđivati pokretnu i nepokretnu imovinu te biti stranka u sudskom postupku.

3. ENISA-u zastupa izvršni direktor.

Članak 39.

Odgovornost ENISA-e

1. Ugovorna odgovornost ENISA-e uređena je pravom koje se primjenjuje na dotični ugovor.

2. Sud Europske unije nadležan je za donošenje presuda na temelju bilo koje odredbe o arbitraži sadržane u ugovoru koji je sklopila ENISA.

3. U slučaju izvanugovorne odgovornosti ENISA je dužna nadoknaditi svaku štetu koju ENISA ili njezini službenici prouzroče pri obavljanju svojih dužnosti, u skladu s općim načelima koja su zajednička zakonodavstvima država članica.

4. Sud Europske unije nadležan je za sve sporove o naknadi štete iz stavka 3.

5. Osobna odgovornost službenika prema ENISA-i podliježe odgovarajućim uvjetima koji se primjenjuju na osoblje ENISA-e.

Članak 40.

Pravila o jezicima

1. Uredba Vijeća br. 1 ([32]) primjenjuje se na ENISA-u. Države članice i druga tijela koja su imenovale države članice mogu se obratiti ENISA-i i dobiti odgovor na službenom jeziku institucija Unije po svom izboru.

2. Prevoditeljske usluge potrebne za funkcioniranje ENISA-e pruža Prevoditeljski centar za tijela Europske unije.

Članak 41.

Zaštita osobnih podataka

1. ENISA obrađuje osobne podatke u skladu s Uredbom (EU) 2018/1725.

2. Upravljački odbor donosi provedbena pravila iz članka 45. stavka 3. Uredbe (EU) 2018/1725. Upravljački odbor može donijeti dodatne mjere koje su potrebne kako bi ENISA primjenjivala Uredbu (EU) 2018/1725.

([32]) Uredba br. 1 o utvrđivanju jezika koji se koriste u Europskoj ekonomskoj zajednici (SL 17, 6.10.1958., str. 385.).

Članak 42.

Suradnja s trećim zemljama i međunarodnim organizacijama

1. U mjeri u kojoj je to nužno za ostvarivanje ciljeva utvrđenih u ovoj Uredbi, ENISA može surađivati s nadležnim tijelima trećih zemalja ili s međunarodnim organizacijama ili i s jedinima i s drugima. U tu svrhu ENISA može, uz prethodno odobrenje Komisije, utvrditi radne aranžmane s tijelima trećih zemalja i međunarodnim organizacijama. Tim se radnim aranžmanima ne stvaraju pravne obveze za Uniju i njezine države članice.

2. ENISA je otvorena za sudjelovanje trećih zemalja koje su u tu svrhu s Unijom sklopile sporazume. U skladu s relevantnim odredbama tih sporazuma utvrđuju se radni aranžmani kojima se posebno određuju priroda, opseg i način sudjelovanja tih trećih zemalja u radu ENISA-e te oni uključuju odredbe koje se odnose na sudjelovanje u inicijativama koje poduzima ENISA, na financijske doprinose i na osoblje. U pogledu pitanja koja se odnose na osoblje, ti radni aranžmani u svakom slučaju moraju biti u skladu s Pravilnikom o osoblju za dužnosnike i Uvjetima zaposlenja ostalih službenika.

3. Upravljački odbor donosi strategiju za odnose s trećim zemljama i međunarodnim organizacijama u pogledu pitanja za koja je ENISA nadležna. Komisija osigurava da ENISA djeluje u okviru svojeg mandata i postojećeg institucijskog okvira sklapanjem odgovarajućih radnih aranžmana s izvršnim direktorom ENISA-e.

Članak 43.

Sigurnosna pravila za zaštitu osjetljivih neklasificiranih podataka i klasificiranih podataka

ENISA nakon savjetovanja s Komisijom donosi sigurnosna pravila primjenjujući sigurnosna načela iz sigurnosnih pravila Komisije za zaštitu osjetljivih neklasificiranih podataka i klasificiranih podataka Europske unije, kako je utvrđeno u odlukama (EU, Euratom) 2015/443 i 2015/444. Sigurnosna pravila ENISA-e uključuju i odredbe o razmjeni, obradi i pohrani takvih podataka.

Članak 44.

Sporazum o sjedištu i uvjeti rada

1. Potrebni dogovori o smještaju ENISA-e u državi članici domaćinu i objektima koje ta država članica daje na raspolaganje, zajedno s posebnim pravilima koja se u državi članici domaćinu primjenjuju na izvršnog direktora, članove Upravljačkog odbora, osoblje ENISA-e i članove njihovih obitelji, utvrđuju se sporazumom o sjedištu između ENISA-e i države članice domaćina, koji se sklapa nakon dobivanja odobrenja Upravljačkog odbora.

2. Država članica domaćin ENISA-e osigurava najbolje moguće uvjete za osiguravanje pravilnog funkcioniranja ENISA-e, vodeći računa o dostupnosti lokacije, postojanju odgovarajućih obrazovnih objekata za djecu članova osoblja, odgovarajućem pristupu tržištu rada, socijalnoj sigurnosti i zdravstvenoj zaštiti za djecu i supružnike članova osoblja.

Članak 45.

Upravna kontrola

Rad ENISA-e nadzire Europski ombudsman u skladu s člankom 228. UFEU-a.

GLAVA III.

OKVIR ZA KIBERSIGURNOSNU CERTIFIKACIJU

Članak 46.

Europski okvir za kibersigurnosnu certifikaciju

1. Europski okvir za kibersigurnosnu certifikaciju uspostavlja se kako bi se poboljšali uvjeti za funkcioniranje unutarnjeg tržišta povećanjem razine kibersigurnosti u Uniji i omogućavanjem usklađenog pristupa na razini Unije za europske programe kibersigurnosne certifikacije s ciljem stvaranja jedinstvenog digitalnog tržišta IKT proizvoda, IKT usluga i IKT procesa.

2. Europskim okvirom za kibersigurnosnu certifikaciju pruža se mehanizam za uspostavu europskih programa kibersigurnosne certifikacije i potvrđivanje toga da IKT proizvodi, IKT usluge i IKT procesi koji su evaluirani u skladu s takvim programima ispunjavaju utvrđene sigurnosne zahtjeve za potrebe zaštite dostupnosti, izvornosti, cjelovitosti i povjerljivosti pohranjenih, poslanih ili obrađenih podataka ili funkcija ili usluga koje se nude s pomoću tih proizvoda, usluga i procesa ili kojima se s pomoću njih može pristupiti tijekom njihova cijelog životnog ciklusa.

Članak 47.

Kontinuirani program rada Unije za europsku kibersigurnosnu certifikaciju

1. Komisija objavljuje kontinuirani program rada Unije za europsku kibersigurnosnu certifikaciju („kontinuirani program rada Unije"), kojim se utvrđuju strateški prioriteti za buduće europske programe kibersigurnosne certifikacije.

2. Kontinuirani program rada Unije konkretno uključuje popis IKT proizvoda, IKT usluga i IKT procesa ili njihovih kategorija koji mogu imati koristi od uključivanja u područje primjene europskog programa kibersigurnosne certifikacije.

3. Uključivanje određenih IKT proizvoda, IKT usluga i IKT procesa ili njihovih kategorija u kontinuirani program rada Unije opravdano je na temelju jednog ili više od sljedećih razloga:

(a) dostupnosti i razvoja nacionalnih programa kibersigurnosne certifikacije koji obuhvaćaju određene kategorije IKT proizvoda, IKT usluga ili IKT procesa, a posebno u pogledu rizika od fragmentacije;

(b) relevantno pravo ili politike Unije ili država članica;

(c) tržišne potražnje;

(d) razvoja kiberprijetnji;

(e) zahtjeva za pripremu posebnog prijedloga programa certifikacije koji je predložio ECCG.

4. Komisija uzima u obzir mišljenja ECCG-a i Interesne skupine za certifikaciju o nacrtu kontinuiranog programa rada Unije.

5. Prvi kontinuirani program rada Unije objavljuje se do 28. lipnja 2020. Kontinuirani program rada Unije ažurira se najmanje svake tri godine, a po potrebi i češće.

Članak 48.

Zahtjev za europski program kibersigurnosne certifikacije

1. Komisija može zatražiti od ENISA-e da izradi prijedlog programa certifikacije ili da preispita postojeći program na temelju kontinuiranog programa rada Unije.

2. U propisno opravdanim slučajevima Komisija ili ECCG mogu zatražiti od ENISA-e da pripremi prijedlog programa certifikacije ili da preispita postojeći europski program programa kibersigurnosne certifikacije koji nije uključen u kontinuirani program rada Unije. Kontinuirani program rada Unije ažurirat će se u skladu s time.

Članak 49.

Izrada, donošenje i preispitivanje europskih programa kibersigurnosne certifikacije

1. Na temelju zahtjeva Komisije u skladu s člankom 48. ENISA izrađuje prijedlog programa certifikacije koji je u skladu sa zahtjevima iz Članaka 51., 52. i 54.

2. Na temelju zahtjeva ECCG-a u skladu s člankom 48. stavkom 2., ENISA može izraditi prijedlog programa certifikacije koji ispunjava zahtjeve iz Članaka 51., 52. i 54. Ako ENISA odbije takav zahtjev, dužna je dati obrazloženje. Svaku odluku o odbijanju takva zahtjeva donosi Upravljački odbor.

3. Pri izradi prijedloga programa certifikacije ENISA se savjetuje sa svim relevantnim dionicima putem formalnih, otvorenih, transparentnih i uključivih postupaka savjetovanja.

4. Za svaki prijedlog programa certifikacije ENISA uspostavlja ad hoc radnu skupinu u skladu s člankom 20. stavkom 4. radi pružanja posebnih savjeta i stručnog znanja ENISA-i.

5. ENISA blisko surađuje s ECCG-om. ECCG pruža ENISA-i pomoć i stručne savjete u vezi s izradom prijedloga programa certifikacije i donosi mišljenje o prijedlogu programa certifikacije.

6. ENISA u najvećoj mogućoj mjeri uzima u obzir mišljenje ECCG-a prije nego što Komisiji podnese prijedlog programa izrađen u skladu sa stavcima 3., 4. i 5. Mišljenje ECCG-a nije obvezujuće za ENISA-u niti njegov izostanak sprečava ENISA-u da proslijedi prijedlog programa certifikacije Komisiji.

7. Komisija, na temelju prijedloga programa certifikacije koji je izradila ENISA, može donositi provedbene akte kojima se predviđaju europski programi kibersigurnosne certifikacije za IKT proizvode, IKT usluge i IKT procese koji ispunjavaju zahtjeve određene u člancima 51., 52. i 54. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 66. stavka 2.

8. ENISA najmanje svakih pet godina evaluira svaki doneseni europski program kibersigurnosne certifikacije, uzimajući u obzir povratne informacije primljene od zainteresiranih strana. Prema potrebi, Komisija ili ECCG mogu od ENISA-e zatražiti da pokrene postupak izrade revidiranog prijedloga programa certifikacije u skladu s člankom 48. i ovim člankom.

Članak 50.

Internetske stranice o europskim programima kibersigurnosne certifikacije

1. ENISA održava posebne internetske stranice na kojima se pružaju informacije i daje vidljivost europskim programima kibersigurnosne certifikacije, europskim kibersigurnosnim certifikatima i EU izjavama o sukladnosti, uključujući informacije u pogledu programa kibersigurnosne certifikacije koji više nisu važeći, u pogledu povučenih i isteklih europskih kibersigurnosnih certifikata i EU izjava o sukladnosti te u pogledu repozitorija poveznica na informacije o kibersigurnosti koje se pružaju u skladu s člankom 55.

2. Kada je to primjenjivo, na internetskim stranicama iz stavka 1. navode se i oni nacionalni programi kibersigurnosne certifikacije koji su zamijenjeni europskim programom kibersigurnosne certifikacije.

Članak 51.

Sigurnosni ciljevi europskih programa kibersigurnosne certifikacije

Europski program kibersigurnosne certifikacije osmišljava se kako bi se postigli, prema potrebi, barem sljedeći sigurnosni ciljevi:

(a) zaštita pohranjenih, poslanih ili na drugačiji način obrađenih podataka od slučajnog ili neovlaštenog pohranjivanja, obrade, pristupa ili objave tijekom cijelog životnog ciklusa IKT proizvoda, IKT usluge ili IKT procesa;

(b) zaštita pohranjenih, poslanih ili na drugačiji način obrađenih podataka od slučajnog ili neovlaštenog uništavanja, gubitka ili izmjene ili nedostatka dostupnosti tijekom cijelog životnog ciklusa IKT proizvoda, IKT usluge ili IKT procesa;

(c) da ovlaštene osobe, programi ili strojevi mogu pristupiti isključivo podacima, uslugama ili funkcijama na koje se odnose njihova prava pristupa;

(d) utvrđivanje i dokumentacija poznatih ovisnosti i ranjivosti;

(e) evidentiranje kojim se podacima, uslugama ili funkcijama pristupilo i koji su podaci, usluge ili funkcije upotrijebljeni ili na drugi način obrađeni, kada i tko je to učinio;

(f) da je moguće provjeriti kojim se podacima, uslugama ili funkcijama pristupilo i koji su podaci, usluge ili funkcije upotrijebljeni ili na drugi način obrađeni, kada i tko je to učinio;

(g) provjera toga da IKT proizvodi, IKT usluge i IKT procesi ne sadrže poznate ranjivosti;

(h) pravodobno osiguravanje ponovne dostupnosti podataka i pristup podacima, uslugama i funkcijama u slučaju fizičkog ili tehničkog incidenta;

(i) da su IKT proizvodi, IKT usluge i IKT procesi zadanim postavkama i dizajnom sigurni;

(j) da IKT proizvodi, IKT usluge i IKT procesi imaju osiguran ažuriran softver i hardver koji ne sadrže javno poznate ranjivosti te imaju osigurane mehanizme za sigurno ažuriranje.

Članak 52.

Jamstvene razine europskih programa kibersigurnosne certifikacije

1. Europskim programom kibersigurnosne certifikacije može se za IKT proizvode, IKT usluge i IKT procese utvrditi jedna od sljedećih jamstvenih razina ili više njih: osnovna, znatna ili visoka. Jamstvena razina razmjerna je razini rizika povezanog s predviđenom uporabom IKT proizvoda, IKT usluge ili IKT procesa, u smislu vjerojatnosti i učinka incidenta.

2. U europskim kibersigurnosnim certifikatima i EU izjavama o sukladnosti navodi se jamstvena razina određena u europskom programu kibersigurnosne certifikacije u okviru kojeg je izdan Europski kibersigurnosni certifikat lii EU izjava o sukladnosti.

3. Sigurnosni zahtjevi koji odgovaraju svakoj jamstvenoj razini moraju biti predviđeni u relevantnom europskom programu kibersigurnosne certifikacije uključujući odgovarajuće sigurnosne funkcionalnosti i odgovarajuću razinu strogoće i opsežnosti evaluacije kojoj IKT proizvod, IKT usluga ili IKT proces mora biti podvrgnut.

4. Certifikat ili EU izjava o sukladnosti mora upućivati na odgovarajuće, s njime povezane, tehničke specifikacije, norme i procedure, uključujući tehničke kontrole, čija je svrha smanjiti rizik od kibersigurnosnih incidenata ili ih spriječiti.

5. Europskim kibersigurnosnim certifikatom ili EU izjavom o sukladnosti koji se odnosi na osnovnu jamstvenu razinu pruža se jamstvo da IKT proizvodi, IKT usluge i IKT procesi za koje su taj certifikat ili ta EU izjava o sukladnosti izdani, ispunjavaju odgovarajuće sigurnosne zahtjeve, uključujući sigurnosne funkcionalnosti, te da su bili podvrgnuti evaluaciji na razini čija je svrha svođenje na najmanju moguću mjeru poznatih osnovnih rizika za incidente i kibernapade. Aktivnosti evaluacije koje treba poduzeti obuhvaćaju barem preispitivanje tehničke dokumentacije. Ako takvo preispitivanje nije odgovarajuće, poduzimaju se zamjenske aktivnosti evaluacije s istovjetnim učinkom.

6. Europskim kibersigurnosnim certifikatom koji se odnosi na znatnu jamstvenu razinu pruža se jamstvo da IKT proizvodi, IKT usluge i IKT procesi za koje su taj certifikat ili ta EU izjava o sukladnosti izdani, ispunjavaju odgovarajuće sigurnosne zahtjeve, uključujući sigurnosne funkcionalnosti, te da su bili podvrgnuti evaluaciji na razini čija je svrha svođenje na najmanju moguću mjeru poznatih kibersigurnosnih rizika te rizika od incidenata i kibernapada koje provode subjekti ograničenih vještina i resursa. Aktivnosti evaluacije koje treba poduzeti obuhvaćaju barem sljedeće: preispitivanje radi dokazivanja nepostojanja javno poznatih ranjivosti i testiranje radi dokazivanja da IKT proizvodi, IKT usluge ili IKT procesi na ispravan način primjenjuju potrebne sigurnosne funkcionalnosti. Ako bilo koja od tih aktivnosti evaluacije nije odgovarajuća, poduzimaju se zamjenske aktivnosti evaluacije s istovjetnim učinkom.

7. Europskim kibersigurnosnim certifikatom koji se odnosi na visoku jamstvenu razinu pruža se jamstvo da IKT proizvodi, IKT usluge i IKT procesi za koje su taj certifikat ili ta EU izjava o sukladnosti izdani, ispunjavaju odgovarajuće sigurnosne zahtjeve, uključujući sigurnosne funkcionalnosti, te da su bili podvrgnuti evaluaciji na razini čija je svrha svođenje na najmanju moguću mjeru rizika od najsuvremenijih kibernapada koje provode subjekti znatnih vještina i resursa. Aktivnosti evaluacije koje treba poduzeti obuhvaća barem sljedeće: preispitivanje radi dokazivanja nepostojanja javno poznatih ranjivosti; testiranje radi dokazivanja da IKT proizvodi, IKT usluge ili IKT procesi na ispravan način i na najsuvremenijoj razini primjenjuju potrebne sigurnosne funkcionalnosti; procjenu njihove otpornosti na napad vještih napadača, koristeći se penetracijskim testiranjem. Ako bilo koja od tih aktivnosti evaluacije nije odgovarajuća, poduzimaju se zamjenske aktivnosti s istovjetnim učinkom.

8. U okviru europskog programa kibersigurnosne certifikacije može se utvrditi nekoliko razina evaluacije ovisno o strogoći i opsežnosti upotrijebljene metodologije evaluacije. Svaka od razina evaluacije odgovara jednoj od jamstvenih razina i definira se odgovarajućom kombinacijom sastavnica jamstva.

Članak 53.

Samoocjenjivanje sukladnosti

1. Europskim programom kibersigurnosne certifikacije može se omogućiti da se samoocjenjivanje sukladnosti provodi pod isključivom odgovornošću proizvođača ili pružatelja IKT proizvoda, IKT usluga ili IKT procesa. Takvo samoocjenjivanje sukladnosti primjenjuje se samo na IKT proizvode, IKT usluge i IKT procese koji predstavljaju niski rizik koji odgovara osnovnoj jamstvenoj razini.

2. Proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa može izdati EU izjavu o sukladnosti u kojoj se navodi da je dokazano ispunjenje zahtjeva utvrđenih u programu. Izdavanjem takve izjave proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa preuzima odgovornost za sukladnost IKT proizvoda, IKT usluge ili IKT procesa sa zahtjevima utvrđenima u tom programu.

3. Proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa EU izjavu o sukladnosti, tehničku dokumentaciju i sve druge relevantne informacije o sukladnosti IKT proizvoda ili IKT usluga s programom treba staviti na raspolaganje nacionalnom tijelu za kibersigurnosnu certifikaciju iz članka 58. stavka 1. u razdoblju utvrđenom u odgovarajućem europskom programu kibersigurnosne certifikacije. Preslika EU izjave o sukladnosti podnosi se nacionalnom tijelu za kibersigurnosnu certifikaciju i ENISA-i.

4. Izdavanje EU izjave o sukladnosti dobrovoljno je, osim ako nije drukčije navedeno u pravu Unije ili u pravu država članica.

5. EU izjave o sukladnosti izdane u skladu s ovim člankom priznaju se u svim državama članicama.

Članak 54.

Elementi europskih programa kibersigurnosne certifikacije

1. Europski program kibersigurnosne certifikacije uključuje barem sljedeće elemente:

(a) predmet i opseg programa certifikacije, uključujući vrstu ili kategorije obuhvaćenih IKT proizvoda, IKT usluga ili IKT procesa;

(b) jasan opis svrhe programa i način na koji odabrane norme, metode evaluacije i jamstvene razine odgovaraju potrebama predviđenih korisnika programa;

(c) upućivanje na međunarodne, europske ili nacionalne norme koje se primjenjuju pri evaluaciji ili, ako te norme nisu dostupne ili odgovarajuće, upućivanje na tehničke specifikacije koje ispunjavaju zahtjeve određene u Prilogu II. Uredbi (EU) br. 1025/2012 ili, ako te specifikacije nisu dostupne, na tehničke specifikacije ili druge kibersigurnosne zahtjeve definirane u europskom programm kibersigurnosne certifikacije;

(d) jednu ili više jamstvenih razina, ako je primjenjivo;

(e) naznaku o tome je li samoocjenjivanje sukladnosti dopušteno u okviru programa;

(f) ako je primjenjivo, posebne ili dodatne zahtjeve kojima podliježu tijela za ocjenjivanje sukladnosti s ciljem jamčenja njihove tehničke stručnosti za evaluaciju kibersigurnosnih zahtjeva;

(g) posebne kriterije i metode evaluacije, uključujući vrste evaluacije, koje treba upotrijebiti za dokazivanje da su ostvareni sigurnosni ciljevi iz članka 51.;

(h) ako je primjenjivo, informacije koje su potrebne za certifikaciju i koje podnositelj zahtjeva treba dostaviti ili na drugi način staviti na raspolaganje tijelima za ocjenjivanje sukladnosti;

(i) ako su programom predviđeni oznake ili znakovi, uvjete pod kojim se te oznake ili znakovi mogu upotrebljavati;

(j) pravila za praćenje sukladnosti IKT proizvoda, IKT usluga i IKT procesa sa zahtjevima europskih kibersigurnosnih certifikata ili EU izjava o sukladnosti, uključujući mehanizme za dokazivanje trajne sukladnosti s navedenim kibersigurnosnim zahtjevima;

(k) ako je primjenjivo, uvjete za izdavanje, održavanje, nastavak i obnavljanje europskih kibersigurnosnih certifikata, kao i uvjete za proširenje ili smanjenje opsega certifikacije;

(l) pravila u vezi s posljedicama nesukladnosti IKT proizvoda, IKT usluga i IKT procesa koji su certificirani ili za koje je izdana EU izjava o sukladnosti, ali koji ne ispunjavaju zahtjeve programa;

(m) pravila o tome kako prijaviti prethodno neotkrivene kibersigurnosne ranjivosti IKT proizvoda, IKT usluga i IKT procesa i postupiti u slučaju njihova otkrivanja;

(n) ako je primjenjivo, pravila o čuvanju evidencije tijelâ za ocjenjivanje sukladnosti;

(o) utvrđivanje nacionalnih ili međunarodnih programa kibersigurnosne certifikacije koji obuhvaćaju iste vrste ili kategorije IKT proizvoda, IKT usluga i IKT procesa, sigurnosne zahtjeve, kriterije i metode evaluacije te jamstvene razine;

(p) sadržaj i format europskih kibersigurnosnih certifikata i EU izjava o sukladnosti koje treba izdati;

(q) razdoblje u kojem proizvođač ili pružatelj IKT proizvoda, IKT usluga ili IKT procesa treba staviti na raspolaganje EU izjavu o sukladnosti, tehničku dokumentaciju i sve relevantne informacije;

(r) maksimalno razdoblje valjanosti europskih kibersigurnosnih certifikata koji se izdaju u okviru programa;

(s) politiku objavljivanja za europske kibersigurnosne certifikate koji su dodijeljeni, izmijenjeni ili povučeni u okviru programa;

(t) uvjete za uzajamno priznavanje programa certifikacije s trećim zemljama;

(u) ako je primjenjivo, pravila koja se odnose na mehanizam istorazinske ocjene utvrđen u programu za tijela koja izdaju europske kibersigurnosne certifikate za visoku jamstvenu razinu na temelju članka 56. stavka 6. Takvim se mehanizmom ne dovodi u pitanje istorazinsko ocjenjivanje iz članka 59.;

(v) format i procedure kojih se proizvođači ili pružatelji IKT proizvoda, IKT usluga i IKT procesa moraju pridržavati pri dostavljanju i ažuriranju dodatnih informacija o kibersigurnosti u skladu s člankom 55. (EP).

2. Navedeni zahtjevi europskog programa kibersigurnosne certifikacije moraju biti usklađeni sa svim primjenjivim pravnim zahtjevima, posebno zahtjevima koji proizlaze iz usklađenog prava Unije.

3. Ako je tako predviđeno posebnim pravnim aktom Unije, certifikat ili EU izjava o sukladnosti koji se izdaje uokviru europskog programa kibersigurnosne certifikacije može se upotrijebiti za dokazivanje pretpostavke sukladnosti sa zahtjevima tog pravnog akta.

4. U slučaju nepostojanja usklađenog prava Unije i prava država članica može se predvidjeti da se europski program kibersigurnosne certifikacije može upotrijebiti za utvrđivanje pretpostavke sukladnosti s pravnim zahtjevima.

Članak 55.

Dodatne informacije o kibersigurnosti za certificirane IKT proizvode, IKT usluge i IKT procese

1. Proizvođač ili pružatelj certificiranih IKT proizvoda, IKT usluga ili IKT procesa ili IKT proizvoda, IKT usluga ili IKT procesa za koje je izdana EU izjava o sukladnosti stavlja na raspolaganje javnosti sljedeće dopunske informacije o kibersigurnosti:

(a) smjernice i preporuke za pomoć krajnjim korisnicima pri sigurnoj konfiguraciji, instalaciji, uvođenju, upotrebi i održavanju IKT proizvoda ili IKT usluga;

(b) razdoblje tijekom kojeg će se pružati sigurnosna potpora krajnjim korisnicima, posebno kad je riječ o dostupnosti ažuriranja povezanih s kibersigurnošću;

(c) informacije za kontakt proizvođača ili pružatelja i prihvaćene metode za primanje informacija o ranjivostima od krajnjih korisnika i istraživača u području sigurnosti;

(d) upućivanje na popis internetskih repozitorija s popisom javno obznanjenih ranjivosti povezanih s IKT proizvodom, IKT uslugom ili IKT procesom i na sve relevantne kibersigurnosne preporuke.

2. Informacije iz stavka 1. dostupne su u elektroničkom obliku te bivaju dostupne i ažuriraju se prema potrebi barem do isteka odgovarajućeg europskog kibersigurnosnog certifikata ili EU izjave o sukladnosti.

Članak 56.

Kibersigurnosna certifikacija

1. Smatra se da su IKT proizvodi, IKT usluge i IKT procesi koji su certificirani u okviru europskog programa kibersigurnosne certifikacije donesenog u skladu s člankom 49. sukladni sa zahtjevima tog programa.

2. Kibersigurnosna certifikacija je dobrovoljna, osim ako je drugačije određeno pravom Unije ili pravom država članica.

3. Komisija redovito ocjenjuje učinkovitost i upotrebu donesenih europskih programa kibersigurnosne certifikacije te treba li određeni europski program kibersigurnosne certifikacije učiniti obveznim putem relevantnog prava Unije kako bi se osigurala odgovarajuća razina kibersigurnosti IKT proizvoda, IKT usluga i IKT procesa u Uniji i poboljšalo funkcioniranje unutarnjeg tržišta. Prva takva ocjena provodi se najkasnije do 31. prosinca 2023., a daljnje ocjene provode se najmanje svake dvije godine.Komisija na temelju rezultata tog ocjenjivanja određuje IKT proizvode, IKT usluge i IKT procese obuhvaćene postojećim programom certifikacije koji trebaju biti obuhvaćeni obveznim programom certifikacije.

Komisija se u prvom redu usredotočuje na sektore navedene u Prilogu II. Direktivi (EU) 2016/1148, koji se ocjenjuju najkasnije dvije godine nakon donošenja prvog europskog programa kibersigurnosne certifikacije.

Prilikom pripreme ocjenjivanja Komisija:

(a) uzima u obzir utjecaj mjera na proizvođače ili pružatelje takvih IKT proizvoda, IKT usluga i IKT procesa te na korisnike u smislu troška tih mjera, kao i društvenih ili gospodarskih koristi koje proizlaze iz očekivane poboljšane razine sigurnosti ciljanih IKT proizvoda, IKT usluga ili IKT procesa;

(b) uzima u obzir postojanje i provedbu relevantnog prava u državama članicama i trećim zemljama;

(c) provodi otvoren, transparentan i uključiv postupak savjetovanja sa svim relevantnim dionicima i državama članicama;

(d) uzima u obzir sve rokove za provedbu, prijelazne mjere i razdoblja, posebno vodeći računa o mogućem učinku mjere na proizvođače ili pružatelje IKT proizvoda, IKT usluga ili IKT procesa, uključujući mala i srednja poduzeća;

(e) predlaže najbrži i najučinkovitiji način provedbe prelaska s dobrovoljnih programa certifikacije na one obvezne.

4. Tijela za ocjenjivanje sukladnosti iz članka 60. europski kibersigurnosni certifikat koji se odnosi na osnovnu ili znatnu jamstvenu razinu izdaju u skladu s ovim člankom na temelju kriterija uključenih u europski program kibersigurnosne certifikacije koji je Komisija donijela u skladu s člankom 49.

5. Odstupajući od stavka 4., u propisno opravdanim slučajevima u europskom programu kibersigurnosne certifikacije može se predvidjeti da europske kibersigurnosne certifikate koji proizlaze iz tog programa može izdati samo javno tijelo. To tijelo može biti:

(a) nacionalno tijelo za kibersigurnosnu certifikaciju iz članka 58. stavka 1.; ili

(b) javno tijelo koje je akreditirano kao tijelo za ocjenjivanje sukladnosti u skladu s člankom 60. stavkom 1..

6. Kada europski program kibersigurnosne certifikacije donesen na temelju članka 49. zahtijeva visoku jamstvenu razinu, europski kibersigurnosni certifikat može izdati samo nacionalno tijelo za kibersigurnosnu certifikaciju ili, u sljedećim slučajevima, tijelo za ocjenjivanje sukladnosti:

(a) uz prethodno odobrenje nacionalnog tijela za kibersigurnosnu certifikaciju za svaki pojedini europski kibersigurnosni certifikat koji izdaje tijelo za ocjenjivanje sukladnosti; ili

(b) na temelju općeg delegiranja zadaće izdavanja tih europskih kibersigurnosnih certifikata tijelu za ocjenjivanje sukladnosti od strane nacionalnog tijela za kibersigurnosnu certifikaciju.

7. Fizička ili pravna osoba koja podnosi IKT proizvode, IKT usluge i IKT procese na certifikaciju stavlja na raspolaganje sve informacije nužne za provođenje certifikacije nacionalnom tijelu za kibersigurnosnu certifikaciju iz članka 58., ako je to tijelo ono koje izdaje europski kibersigurnosni certifikat ili tijelu za ocjenjivanje sukladnosti iz članka 60.

8. Nositelj europskog kibersigurnosnog certifikata obavješćuje tijelo iz stavka 7. o svim naknadno otkrivenim ranjivostima ili nepravilnostima koje se odnose na sigurnost certificiranog IKT proizvoda, IKT usluge ili IKT procesa koje bi mogle imati učinak na njegovu usklađenost sa zahtjevima u vezi s certifikacijom. To tijelo bez nepotrebne odgode prosljeđuje te informacije dotičnom nacionalnom tijelu za kibersigurnosnu certifikaciju.

9. Europski kibersigurnosni certifikati izdaju se na razdoblje predviđeno europskim programom kibersigurnosne certifikacije te se mogu obnoviti pod uvjetom da su i dalje ispunjeni relevantni zahtjevi.

10. Europski kibersigurnosni certifikat izdan u skladu s ovim člankom priznaje se u svim državama članicama.

Članak 57.

Nacionalni programi kibersigurnosne certifikacije i certifikati

1. Ne dovodeći u pitanje stavak 3. ovog članka, nacionalni programi kibersigurnosne certifikacije i povezani postupci za IKT proizvode, IKT usluge i IKT procese koji su obuhvaćeni europskim programom kibersigurnosne certifikacije prestaju proizvoditi učinke od datuma utvrđenog u provedbenom aktu donesenom u skladu s člankom 49. stavkom 7. Nacionalni programi kibersigurnosne certifikacije i povezani postupci za IKT proizvode, IKT usluge i IKT procese koji nisu obuhvaćeni europskim programom kibersigurnosne certifikacije i dalje postoje.

2. Države članice ne uvode nove nacionalne programe kibersigurnosne certifikacije IKT proizvoda, IKT usluga i IKT procesa koji su već obuhvaćeni europskim programom kibersigurnosne certifikacije koji je na snazi.

3. Postojeći certifikati koji su bili izdani u okviru nacionalnih programa kibersigurnosne certifikacije, a obuhvaćeni su europskim programom kibersigurnosne certifikacije ostaju na snazi do svojeg datuma isteka.

4. S ciljem izbjegavanja fragmentacije unutarnjeg tržišta države članice obavješćuju Komisiju i ECCG o svakoj namjeri izrade novih nacionalnih programa kibersigurnosne certifikacije.

Članak 58.

Nacionalna tijela za kibersigurnosnu certifikaciju

1. Svaka država članica imenuje jedno ili više nacionalnih tijela za kibersigurnosnu certifikaciju na svojem državnom području ili, uz pristanak druge države članice, određuje da jedno ili više nacionalnih tijela za kibersigurnosnu certifikaciju s poslovnim nastanom u toj drugoj državi članici bude odgovorno za zadaće nadzora u državi članici koja ga imenuje.

2. Svaka država članica obavješćuje Komisiju o imenovanim nacionalnim tijelima za kibersigurnosnu certifikaciju. Ako država članica imenuje više od jednog tijela, također obavješćuje Komisiju o zadaćama koje su dodijeljene svakome od tih tijela.

3. Ne dovodeći u pitanje Članak 56. stavak 5. točku (a) i Članak 56. stavak 6., svako nacionalno tijelo za kibersigurnosnu certifikaciju neovisno je od subjekata koje nadzire u pogledu svojeg ustrojstva, odluka o financiranju, pravne strukture i odlučivanja.

4. Države članice osiguravaju da aktivnosti nacionalnih tijela za kibersigurnosnu certifikaciju koje se odnose na izdavanje europskih kibersigurnosnih certifikata iz s članka 56. stavka 5. točke (a) i članka 56. stavka 6. budu strogo razdvojene od njihovih nadzornih aktivnosti određenih u ovom članku i da se te aktivnosti provode neovisno jedne o drugima.

5. Države članice osiguravaju da nacionalna tijela za kibersigurnosnu certifikaciju imaju odgovarajuće resurse za djelotvorno i učinkovito izvršavanje svojih ovlasti i provođenje svojih.

6. Kako bi se ova Uredba mogla djelotvorno provoditi, primjereno je da tijela za kibersigurnosnu certifikaciju bi na aktivan, djelotvoran, učinkovit i siguran način sudjeluju u ECCG-u.

7. Nacionalna tijela za kibersigurnosnu certifikaciju:

(a) nadziru i zahtijevaju ispunjavanje pravila iz europskih programa kibersigurnosne certifikacije u skladu s člankom 54. stavkom 1. točkom (j) za praćenje sukladnosti IKT proizvoda, IKT usluga i IKT procesa sa zahtjevima iz europksih kibersigurnosnih certifikata izdanih na njihovim državnim područjima, u suradnji s drugim relevantnim tijelima za nadzor tržišta;

(b) prate usklađenost i zahtijevaju ispunjavanje obveza proizvođača ili proizvođača ili pružatelja IKT proizvoda, IKT usluga i IKT procesa koji imaju poslovni nastan na njihovim državnim područjima i koji provode samoprocjenu sukladnosti, te posebno prate usklađenost i zahtijevaju ispunjavanje obveza tih proizvođača ili pružatelja iz članka 53. stavaka 2. i 3. te odgovarajućeg europskog programa kibersigurnosne certifikacije;

(c) ne dovodeći u pitanje Članak 60. stavak 3., aktivno pomažu nacionalnim akreditacijskim tijelima i podupiru ih u praćenju i nadzoru aktivnosti tijela za ocjenjivanje sukladnosti za potrebe ove Uredbe;

(d) prate i nadziru aktivnosti javnih tijela iz članka 56. stavka 5.;

(e) ako je primjenjivo, ovlašćuju tijela za ocjenjivanje sukladnosti u skladu s člankom 60. stavkom 3. i ograničavaju, suspendiraju ili povlače postojeće odobrenje kada tijela za ocjenjivanje sukladnosti krše zahtjeve iz ove Uredbe;

(f) obrađuju pritužbe fizičkih ili pravnih osoba u pogledu europskih kibersigurnosnih certifikata koje su izdala nacionalna tijela za kibersigurnosnu certifikaciju ili u pogledu europskih kibersigurnosnih certifikata koje su izdala tijela za ocjenjivanje sukladnosti izdanih u skladu s člankom 56. stavkom 6. ili u pogledu EU izjava o sukladnosti izdanih na temelju članka 53. te u odgovarajućoj mjeri istražuju predmet tih pritužbi i u razumnom roku obavješćuju podnositelja pritužbe o napretku i rezultatu istrage;

(g) ENISA-i i ECCG-u dostavljaju godišnje sažeto izvješće o provedenim aktivnostima u skladu s točkama (b), (c) i (d) ovog stavka ili sa stavkom 8.;

(h) surađuju s drugim nacionalnim tijelima za kibersigurnosnu certifikaciju ili s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj neusklađenosti IKT proizvoda, IKT usluga i IKT procesa sa zahtjevima iz ove Uredbe ili sa zahtjevima pojedinih europskih programa kibersigurnosne certifikacije; i

(i) prate relevantne promjene u području kibersigurnosne certifikacije.

8. Svako nacionalno tijelo za kibersigurnosnu certifikaciju ima barem sljedeće ovlasti:

(a) zatražiti od tijelâ za ocjenjivanje sukladnosti, nositeljâ europskog kibersigurnosnog certifikata i izdavateljâ EU izjave o sukladnosti da dostave sve informacije koje su mu potrebne za obavljanje njegovih zadaća;

(b) provoditi istrage, u obliku revizija, tijelâ za ocjenjivanje sukladnosti, nositeljâ europskog kibersigurnosnog certifikata i izdavateljâ EU izjave o sukladnosti za potrebe provjere njihove usklađenosti s ovom glaveom;

(c) poduzimati odgovarajuće mjere, u skladu s nacionalnim pravom, radi osiguranja usklađenosti tijelâ za ocjenjivanje sukladnosti, nositeljâ europskog kibersigurnosnog certifikata i izdavateljâ EU izjave o sukladnosti s ovom Uredbom ili europskim programom kibersigurnosne certifikacije;

(d) osigurati pristup prostorijama svakog tijela za ocjenjivanje sukladnosti ili nositelja europskog kibersigurnosnog certifikata za potrebe provedbe istraga u skladu s postupovnim pravom Unije ili države članice;

(e) povući, u skladu s nacionalnim pravom, europske kibersigurnosne certifikate koje su izdala nacionalna tijela za kibersigurnosnu certifikaciju ili europske kibersigurnosne certifikate koje su izdala tijela za ocjenjivanje sukladnosti, u skladu s člankom 56. stavkom 6. ako ti certifikati nisu u skladu s ovom Uredbom ili s europskim programom kibersigurnosne certifikacije;

(f) izreći sankcije, kako je predviđeno člankom 65., u skladu s nacionalnim pravom i zatražiti hitan prestanak kršenja obveza koje su određene ovom Uredbom.

9. Nacionalna tijela za kibersigurnosnu certifikaciju surađuju međusobno i s Komisijom, osobito razmjenom informacija, iskustava i dobre prakse u području kibersigurnosne certifikacije i tehničkih pitanja povezanih s kibersigurnošću IKT proizvoda, IKT usluga i IKT procesa.

Članak 59.

Istorazinsko ocjenjivanje

1. S ciljem postizanja istovjetnih normi u cijeloj Uniji u pogledu izdanih europskih kibersigurnosnih certifikata i EU izjava o sukladnosti, nacionalna tijela za kibersigurnosnu certifikaciju podliježu istorazinskom ocjenjivanju.

2. Istorazinsko ocjenjivanje provodi se na temelju dobrih i jasnih kriterija i postupaka evaluacije, posebno što se tiče zahtjeva u pogledu strukture, ljudskih resursa i postupaka, povjerljivosti i pritužbi.

3. Istorazinsko ocjenjivanje obuhvaća procjene:

(a) ako je primjenjivo, toga jesu li aktivnosti nacionalnih tijela za kibersigurnosnu certifikaciju koje su povezane s izdavanjem certifikata iz članka 56. stavka 5. točke (a) i članka 56. stavka 6. strogo razdvojene odnjihovih nadzornih aktivnosti određenih u članku 58. i toga provode li se te aktivnosti neovisno jedne o drugima;

(b) postupaka za nadzor i provedbu pravila o praćenju sukladnosti IKT proizvoda, IKT usluga i IKT procesa s europskim kibersigurnosnim certifikatima na temelju članka 58. stavka 7. točke (a);

(c) postupaka za praćenje i izvršenje obveza proizvođača ili pružatelja IKT proizvoda, IKT usluga ili IKT procesa u skladu s člankom 58. stavkom 7. točkom (b);

(d) postupaka za praćenje, odobravanje i nadzor aktivnosti tijela za ocjenjivanje sukladnosti;

(e) ako je primjenjivo, toga posjeduje li osoblje tijela koja izdaju certifikate za visoku jamstvenu razinu u skladu s člankom 56. stavkom 6. odgovarajuće stručno znanje.

4. Istorazinsko ocjenjivanje provode najmanje dva nacionalna tijela za kibersigurnosnu certifikaciju iz drugih država članica i Komisija te se ona provodi najmanje jednom svakih pet godina. ENISA može sudjelovati u istorazinskom ocjenjivanju.

5. Komisija može donijeti provedbene akte kojima se utvrđuje plan za istorazinsko ocjenjivanje kojim se obuhvaća razdoblje od najmanje pet godina, definiraju kriteriji za sastav tima za istorazinsko ocjenjivanje, metodologija koja se primjenjuje za istorazinsko ocjenjivanje te raspored, učestalost i druge zadaće povezane s njime. Pri donošenju tih provedbenih akata Komisija u obzir uzima mišljenja ECCG-a. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 66. stavka 2.

6. Rezultate istorazinskih ocjenjivanja ispituje ECCG te izrađuje sažetke koji mogu biti javno dostupni i, prema potrebi, izdaje smjernice ili preporuke o djelovanjima ili mjerama koje subjekti o kojima je riječ trebaju poduzeti.

Članak 60.

Tijela za ocjenjivanje sukladnosti

1. Tijela za ocjenjivanje sukladnosti moraju imati akreditaciju nacionalnih akreditacijskih tijela u skladu s Uredbom (EZ) br. 765/2008. Takva se akreditacija izdaje samo ako tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve utvrđene u Prilogu ovoj Uredbi.

2. Ako je europski kibersigurnosni certifikat izdalo nacionalno tijelo za kibersigurnosnu certifikaciju u skladu s člankom 56. stavkom 5. točkom (a) i člankom 56. stavkom 6., tijelo za izdavanje certifikata nacionalnog tijela za kibersigurnosnu certifikaciju akreditira se kao tijelo za ocjenjivanje sukladnosti u skladu sa stavkom 1. ovog članka.

3. Ako su europskim programima kibersigurnosne certifikacije utvrđeni posebni ili dodatni zahtjevi u skladu s člankom 54. stavkom 1. točkom (f), za obavljanje zadaća u okviru tih programa nacionalno tijelo za kibersigurnosnu certifikaciju ovlašćuje samo tijela za ocjenjivanje sukladnosti koja ispunjavaju te zahtjeve.

4. Akreditacija iz stavka 1. tijelima za ocjenjivanje sukladnosti izdaje se na najviše pet godina i može se obnoviti pod istim uvjetima ako tijelo za ocjenjivanje sukladnosti i dalje ispunjava zahtjeve iz ovog članka. Nacionalna akreditacijska tijela poduzimaju sve odgovarajuće mjere u razumnom roku kako bi ograničila, suspendirala ili povukla akreditaciju tijela za ocjenjivanje sukladnosti izdanu u skladu sa stavkom 1. ako uvjeti za akreditaciju nisu ili više nisu ispunjeni ili ako tijelo za ocjenjivanje sukladnosti krši ovu Uredbu.

Članak 61.

Prijavljivanje

1. Za svaki europski program kibersigurnosne certifikacije nacionalna tijela za kibersigurnosnu certifikaciju Komisiji prijavljuju tijela za ocjenjivanje sukladnosti koja su akreditirana i, ako je primjenjivo, ovlaštena u skladu s člankom 60. stavkom 3. za izdavanje europskih kibersigurnosnih certifikata određene jamstvene razine iz članka 52. Nacionalna tijela za kibersigurnosnu certifikaciju bez nepotrebne odgode prijavljuju Komisiji sve naknadne promjene u vezi s tim tijelima.

2. Godinu dana nakon stupanja na snagu europskog programa kibersigurnosne certifikacije Komisija u *Službenom listu Europske unije* objavljuje popis tijela za ocjenjivanje sukladnosti prijavljenih u okviru programa.

3. Ako Komisija zaprimi prijavu nakon isteka razdoblja iz stavka 2., ona u *Službenom listu Europske unije* objavljuje izmjene popisa prijavljenih tijela za ocjenjivanje sukladnosti u roku od dva mjeseca od datuma primitka te prijave.

4. Nacionalno tijelo za kibersigurnosnu certifikaciju može Komisiji podnijeti zahtjev da se tijelo za ocjenjivanje sukladnosti koje je to nacionalno tijelo prijavilo ukloni s popisa iz stavka 2. Komisija objavljuje odgovarajuće izmjene tog popisa u *Službenom listu Europske unije* u roku od jednog mjeseca od primitka zahtjeva nacionalnog tijela za kibersigurnosnu certifikaciju.

5. Komisija može donijeti provedbene akte kojima utvrđuje okolnosti, formate i postupke za prijave iz stavka 1. ovog članka. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 66. stavka 2.

Članak 62.

Europska skupina za kibersigurnosnu certifikaciju

1. Osniva se Europska skupina za kibersigurnosnu certifikaciju („ECCG”).

2. ECCG se sastoji od predstavnika nacionalnih tijela za kibersigurnosnu certifikaciju ili predstavnika drugih relevantnih nacionalnih tijela.Član ECCG-a ne može predstavljati više od dvije države članice.

3. Dionici i relevantne treće strane mogu biti pozvani da prisustvuju sastancima ECCG-a i sudjelovati u njezinu radu.

4. ECCG ima sljedeće zadaće:

(a) savjetovati Komisiju i pomagati joj u radu s ciljem osiguravanja usklađene provedbe i primjene ove glave, posebno u pogledu kontinuiranog programa rada Unije, pitanja politike kibersigurnosne certifikacije, koordinacije pristupa politike i izrade europskih programa kibersigurnosne certifikacije;

(b) pomagati ENISA-i, savjetovati je i surađivati s njome u pogledu izrade prijedloga programa certifikacije na temelju članka 49. ove Uredbe;

(c) donijeti mišljenje o prijedlogu programa certifikacije koji je pripremila ENISA u skladu s člankom 49. ove Uredbe;

(d) zatražiti od ENISA-e da izradi prijedlog programa certifikacije na temelju članka 48. stavka 2.;

(e) donositi mišljenja upućena Komisiji koja se odnose na održavanje i preispitivanje postojećih europskih programa kibersigurnosne certifikacije;

(f) analizirati relevantne promjene u području kibersigurnosne certifikacije i razmjenjivati informacije i dobru praksu o programima kibersigurnosne certifikacije;

(g) olakšavati suradnju između nacionalnih tijela za kibersigurnosnu certifikaciju iz ove glave izgradnjom kapaciteta i razmjenom informacija, posebno uspostavom načina za učinkovitu razmjenu informacija povezanih sa svim pitanjima koja se odnose na kibersigurnosnu certifikaciju;

(h) pružati potporu provedbi mehanizama istorazinske ocjene u skladu s pravilima utvrđenima u europskom programu kibersigurnosne certifikacije u skladu s člankom 54. stavkom 1. točkom (u);

(i) olakšavati usklađivanje europskih programa kibersigurnosne certifikacije s međunarodno priznatim normama, uključujući preispitivanjem postojećih europskih programa kibersigurnosne certifikacije te, prema potrebi, davanjem preporuka ENISA-i u pogledu suradnje s relevantnim međunarodnim organizacijama za normizacijuradi rješavanja nedostatakaili manjkavosti u dostupnim međunarodno priznatim normama.

5. Uz pomoć ENISA-e Komisija predsjeda ECCG-om i osigurava mu tajništvo u skladu s člankom 8. stavkom 1. točki (e).

Članak 63.

Pravo na podnošenje pritužbe

1. Fizičke i pravne osobe imaju pravo podnijeti pritužbu izdavatelju europskog kibersigurnosnog certifikata ili, ako se pritužba odnosi na europski kibersigurnosni certifikat koji je izdalo tijelo za ocjenjivanje sukladnosti djelujući u skladu s člankom 56. stavkom 6., relevantnom nacionalnom tijelu za kibersigurnosnu certifikaciju.

2. Tijelo kojem je podnesena pritužba obavješćuje podnositelja pritužbe o napretku postupka i donesenoj odluci te obavješćuje podnositelja o pravu na učinkovit pravni lijek iz članka 64.

Članak 64.

Pravo na učinkovit pravni lijek

1. Neovisno o bilo kakvim administrativnim ili drugim izvansudskim pravnim lijekovima, fizičke i pravne osobe imaju pravo na učinkovit pravni lijek u pogledu:

(a) odluka koje donesu tijela iz članka 63. stavka 1., među ostalim prema potrebi u vezi s nepravilnim izdavanjem, neizdavanjem ili priznavanjem europskog kibersigurnosnog certifikata koji imaju te fizičke i pravne osobe;

(b) propuštanja postupanja u vezi s pritužbom podnesenom tijelu iz članka 63. stavka 1.

2. Postupci na temelju ovog članka pokreću se pred sudovima države članice u kojoj se nalazi tijelo protiv kojeg je pravni lijek upućen.

Članak 65.

Sankcije

Države članice utvrđuju pravila o sankcijama koje se primjenjuju na povrede ove glave i povrede europskih programa kibersigurnosne certifikacije te poduzimaju sve potrebne mjere kako bi osigurale njihovo izvršenje. Predviđene kazne moraju biti učinkovite, proporcionalne i odvraćajuće. Države članice bez odgode obavješćuju Komisiju o tim pravilima i mjerama te o svim njihovim naknadnim izmjenama.

GLAVA IV.

ZAVRŠNE ODREDBE

Članak 66.

Postupak odbora

1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.

2. Pri upućivanju na ovaj stavak primjenjuje se Članak 5. stavak 4. točka (b) Uredbe (EU) br. 182/2011.

Članak 67.

Ocjenjivanje i revizija

1. Do 28. lipnja 2024., a nakon toga svakih pet godina Komisija ocjenjuje učinak, djelotvornost i učinkovitost ENISA-e i njezina načina rada kao i moguću potrebu za izmjenom mandata ENISA-e te financijske posljedice takve izmjene. Ocjenjivanjem se uzimaju u obzir sve povratne informacije pružene ENISA-i kao odgovor na njezine aktivnosti. Ako Komisija smatra da daljnje postojanje ENISA-e više nije opravdano u svijetlu dodijeljenih joj ciljeva, mandata i zadaća, ona može predložiti izmjenu odredaba ove Uredbe koje se odnose na ENISA-u.

2. Ocjenjivanjem se procjenjuje i učinak, djelotvornost i učinkovitost odredaba iz glave III. ove Uredbe u pogledu ciljeva osiguranja prikladne razine kibersigurnosti IKT proizvoda, IKT usluga i IKT procesa u Uniji i poboljšanja funkcioniranja unutarnjeg tržišta.

3. Ocjenjivanjem se procjenjuje jesu li ključni zahtjevi kibersigurnosti za pristup unutarnjem tržištu potrebni kako bi se spriječilo da IKT proizvodi, IKT usluge i IKT procesi koji ne ispunjavaju temeljne zahtjeve u pogledu kibersigurnosti uđu na tržište Unije.

4. Do 28. lipnja 2024. i svakih pet godina nakon toga Komisija prosljeđuje izvješće o ocjenjivanju zajedno sa svojim zaključcima Europskom parlamentu, Vijeću i Upravljačkom odboru. Nalazi tog izvješća javno se obznanjuju.

Članak 68.

Stavljanje izvan snage i sljedništvo

1. Uredba (EU) br. 526/2013 stavlja se izvan snage od 27. lipnja 2019.

2. Upućivanja na Uredbu (EU) br. 526/2013 i na ENISA-u osnovanu tom uredbom smatraju se upućivanjima na ovu Uredbu i na ENISA-u osnovanu ovom Uredbom.

3. ENISA osnovana ovom Uredbom pravni je sljednik ENISA-e osnovane Uredbom (EU) br. 526/2013 u pogledu cjelokupnog vlasništva, svih sporazuma, pravnih obveza, ugovora o radu, financijskih obveza i odgovornosti. Sve odluke Upravljačkog odbora i Izvršnog odbora donesene u skladu s Uredbom (EU) br. 526/2013 ostaju na snazi ako su u skladu s ovom Uredbom.

4. ENISA se osniva na neodređeno razdoblje počevši od 27. lipnja 2019.

5. Izvršni direktor imenovan u skladu s člankom 24. stavkom 4. Uredbe (EU) br. 526/2013 ostaje na dužnosti i djeluje kao izvršni direktor iz članka 20. ove Uredbe za preostalo razdoblje mandata izvršnog direktora. Ostali uvjeti njegovog ugovora ostaju neizmijenjeni.

6. Članovi Upravljačkog odbora i njihovi zamjenici imenovani u skladu s člankom 6. Uredbe (EU) br. 526/2013 ostaju na dužnosti i djeluju u Upravljačkom odboru u skladu s člankom 15. ove Uredbe za preostalo razdoblje svojeg mandata.

Članak 69.

Stupanje na snagu

1. Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

2. Članci 58., 60., 61., 63., 64. i 65. primjenjuju se od 28. lipnja 2021.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Strasbourgu 17. travnja 2019.

Za Europski parlament	*Za Vijeće*
Predsjednik	*Predsjednik*
A. TAJANI	G. CIAMBA

PRILOG

ZAHTJEVI KOJE MORAJU ISPUNITI TIJELA ZA OCJENJIVANJE SUKLADNOSTI

Tijela za ocjenjivanje sukladnosti koja žele biti akreditirana moraju ispuniti sljedeće zahtjeve:

1. Tijelo za ocjenjivanje sukladnosti osniva se u skladu s nacionalnim pravom i ima pravnu osobnost.

2. Tijelo za ocjenjivanje sukladnosti tijelo je koje ima svojstvo treće strane neovisne o organizaciji ili IKT proizvodima, IKT uslugama ili IKT procesima koje ocjenjuje.

3. Tijelo koje je dio poslovnog udruženja ili strukovnog saveza koji zastupaju poduzeća uključena u projektiranje, proizvodnju, nabavu, sastavljanje, uporabu ili održavanje IKT proizvoda, IKT usluga ili IKT procesa koje ono ocjenjuje može se smatrati tijelom za ocjenjivanje sukladnosti pod uvjetom da je dokazana njegova neovisnost i nepostojanje svakog oblika sukoba interesa.

4. Tijela za ocjenjivanje sukladnosti, njihovo visoko rukovodstvo i osoblje zaduženo za provedbu zadaća ocjenjivanja sukladnosti ne smiju biti projektant, proizvođač, dobavljač, ugraditelj, kupac, vlasnik, korisnik ili održavatelj IKT proizvoda, IKT usluge ili IKT procesa koje ocjenjuju, ili ovlašteni zastupnik bilo koje od tih strana. Tom se zabranom ne isključuje upotreba ocijenjenih IKT proizvoda koji su potrebni za rad tijela za ocjenjivanje sukladnosti ili upotrebu takvih IKT proizvoda u osobne svrhe.

5. Tijela za ocjenjivanje sukladnosti, njihovo visoko rukovodstvo i osoblje zaduženo za provedbu zadaća ocjenjivanja sukladnosti ne smiju izravno sudjelovati u projektiranju, proizvodnji ili izradi, stavljanju na tržište, ugradnji, uporabi ili održavanju IKT proizvoda, IKT usluga ili IKT procesa koji se ocjenjuju ni zastupati strane uključene u te djelatnosti. Tijela za ocjenjivanje sukladnosti, njihovo visoko rukovodstvo i osoblje zaduženo za provedbu zadaća ocjenjivanja sukladnosti ne smiju sudjelovati ni u kakvoj djelatnosti koja može ugroziti neovisnost njihove prosudbe ili integritet u odnosu na njihove aktivnosti ocjenjivanja sukladnosti. Ta se zabrana posebno odnosi na usluge savjetovanja.

6. Ako je tijelo za ocjenjivanje sukladnosti u vlasništvu javnog subjekta ili institucije ili takav subjekt ili institucija njime upravljaju, osigurava se neovisnost i nepostojanje sukoba interesa između nacionalnog tijela za kibersigurnosnu certifikaciju i tijela za ocjenjivanje sukladnosti te se dokumentira.

7. Tijela za ocjenjivanje sukladnosti osiguravaju da djelatnosti njihovih društava kćeri i podizvođača ne utječu na povjerljivost, objektivnost ili nepristranost njihovih aktivnosti ocjenjivanja sukladnosti.

8. Tijela za ocjenjivanje sukladnosti i njihovo osoblje provode aktivnosti ocjenjivanja sukladnosti na najvišem stupnju profesionalnog integriteta i potrebne tehničke stručnosti u određenom području, bez pritisaka i poticaja koji bi mogli utjecati na njihovu prosudbu ili rezultate njihovih aktivnosti ocjenjivanja sukladnosti, uključujući pritiske i poticaje financijske prirode, posebno u vezi s osobama ili skupinama osoba kojima su rezultati tih aktivnosti važni.

9. Tijelo za ocjenjivanje sukladnosti u stanju je obavljati sve zadaće ocjenjivanja sukladnosti koje su mu dodijeljene u skladu s ovom Uredbom, bez obzira na to obavlja li te zadaće samo ili se one obavljaju u njegovo ime i pod njegovom odgovornošću. Svako podugovaranje ili savjetovanje s vanjskim osobljem uredno se dokumentira, ne uključuje nikakve posrednike, i predmetom je pisanog sporazuma kojim su obuhvaćeni, među ostalim, povjerljivost i sukobi interesa. Dotično tijelo za ocjenjivanje sukladnosti preuzima punu odgovornost za zadaće koje obavlja.

10. U bilo kojem trenutku i za bilo koji postupak ocjenjivanja sukladnosti te za svaku vrstu, kategoriju ili potkategoriju IKT proizvoda, IKT usluga ili IKT procesa tijelo za ocjenjivanje sukladnosti raspolaže potrebnim:

    (a) osobljem koje posjeduje tehničko znanje te dostatno i primjereno iskustvo za obavljanje zadaća ocjenjivanja sukladnosti;

    (b) opisima postupaka u skladu s kojima se provodi ocjenjivanje sukladnosti, radi osiguranja transparentnost tih postupaka i mogućnost njihova ponavljanja. Ima i uspostavljenu primjerenu politiku i postupke za razlikovanje između zadaća koje provodi kao tijelo prijavljeno u skladu s člankom 61. i svojih drugih aktivnosti;

(c) postupcima za obavljanje aktivnosti kojima se vodi računa o veličini poduzeća, sektoru u kojemu ono djeluje, njegovoj strukturi, stupnju složenosti tehnologije dotičnog IKT proizvoda, IKT usluge ili IKT procesa te masovnom ili serijskom karakteru proizvodnog procesa.

11. Tijelo za ocjenjivanje sukladnosti raspolaže potrebnim sredstvima za primjereno obavljanje tehničkih i administrativnih zadaća povezanih s aktivnostima ocjenjivanja sukladnosti te ima pristup svoj potrebnoj opremi i objektima.

12. Osobe zadužene za aktivnosti ocjenjivanja sukladnosti imaju:

(a) dobru tehničku i strukovnu osposobljenost za sve aktivnosti ocjenjivanja sukladnosti;

(b) dostatno znanje o zahtjevima koji se odnose na ocjenjivanja sukladnosti koja provode i odgovarajuće ovlaštenje za provedbu tih ocjenjivanja;

(c) primjereno poznavanje i razumijevanje primjenjivih zahtjeva i ispitnih normi;

(d) sposobnost za sastavljanje certifikata, vođenje evidencije i pripremu izvješća kojima se dokazuje da su ocjenjivanja sukladnosti provedena.

13. Nepristranost tijela za ocjenjivanje sukladnosti, njihova visokog rukovodstva i osoba zaduženih za aktivnosti ocjenjivanja sukladnosti te podugovaratelja, ako ih ima, mora biti zajamčena.

14. Naknada za rad visokog rukovodstva i osoba zaduženih za aktivnosti ocjenjivanja sukladnosti ne ovisi o broju provedenih ocjenjivanja sukladnosti ni o rezultatima tih ocjenjivanja.

15. Tijela za ocjenjivanje sukladnosti sklapaju osiguranje od odgovornosti osim ako je odgovornost preuzela država članica u skladu sa svojim nacionalnim pravom ili je sama država članica izravno odgovorna za ocjenjivanje sukladnosti.

16. Tijelo za ocjenjivanje sukladnosti i njegovo osoblje, odbori, ovisni subjekti, podugovoratelji i sva povezana tijela ili osoblje vanjskih tijela postupaju u skladu s načelima povjerljivosti i čuvaju poslovnu tajnu koja se odnosi na sve informacije prikupljene pri obavljanju zadaća ocjenjivanja sukladnosti u skladu s ovom Uredbom ili na temelju bilo koje odredbe nacionalnoga prava kojom se ova Direktiva provodi, osim u slučajevima kada se otkrivanje informacija zahtijeva pravom Unije ili države članice koje je mjerodavno za te osobe i osim u pogledu nadležnih tijela država članica u kojoj se provode njegove aktivnosti. Prava intelektualnog vlasništva zaštićena su. Tijelo za ocjenjivanje sukladnosti ima uspostavljene dokumentirane postupke u pogledu zahtjeva iz ove točke.

17. Uz iznimku točke 16., zahtjevi iz ovog Priloga ni na koji način ne isključuju razmjenu tehničkih informacija i regulatornih smjernica između tijela za ocjenjivanje sukladnosti i osobe koja podnosi zahtjev za certifikaciju ili koja razmatra mogućnost podnošenja zahtjeva.

18. Tijela za ocjenjivanje sukladnosti djeluju u skladu s nizom dosljednih, pravednih i razumnih uvjeta, uzimajući u vezi s naknadama u obzir interese MSP-ova.

19. Tijela za ocjenjivanje sukladnosti ispunjavaju zahtjeve relevantne norme usklađene na temelju Uredbe (EZ) br. 765/2008 za akreditaciju tijela za ocjenjivanje sukladnosti koja obavljaju certifikaciju IKT proizvoda, IKT usluga ili IKT procesa.

20. Tijela za ocjenjivanje sukladnosti osiguravaju da ispitni laboratoriji koji se upotrebljavaju za potrebe ocjenjivanja sukladnosti ispunjavaju zahtjeve relevantne norme usklađene na temelju Uredbe (EZ) br. 765/2008 za akreditaciju laboratorija koji obavljaju ispitivanje.