Vijeće
Europske unije

Bruxelles, 29. svibnja 2018.
(OR. en)

9350/18

Međuinstitucijski predmet:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NAPOMENA

Od:	Predsjedništvo
Za:	Vijeće
Br. preth. dok.:	8834/18
Br. dok. Kom.:	12183/17
Predmet:	Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o ENISA-i, Agenciji EU-a za kibersigurnost, i stavljanju izvan snage Uredbe (EU) 526/2013 te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt o kibersigurnosti”) – općí pristup

I. UVOD

1. Komisija je, u okviru svoje strategije jedinstvenog digitalnog tržišta, 13. rujna 2017. donijela i proslijedila Vijeću i Europskom parlamentu navedeni prijedlog[1] na temelju članka 114. UFEU-a kao pravne osnove. U okviru takozvanog „paketa za kibersigurnost" ovim se prijedlogom nastoji ostvariti visoka razina kibersigurnosti, kiberotpornosti i povjerenja u Uniju kako bi se osiguralo pravilno funkcioniranje unutarnjeg tržišta.

2. Predloženom uredbom utvrđuju se ciljevi, zadaće i organizacijski aspekti ENISA-e, Agencije EU-a za kibersigurnost, i stvara se okvir za uspostavu europskih programa kibersigurnosne certifikacije za potrebe osiguravanja odgovarajuće razine kibersigurnosti IKT proizvoda i usluga u Uniji. Uz Komisijin prijedlog priložena je procjena učinka u kojoj se istražuje konkretan niz od osam političkih opcija kojima je obuhvaćeno preispitivanje ENISA-e i kibersigurnosne certifikacije IKT-a.

3. Predložena uredba sadržava dvije glavne komponente:

   - trajni mandat Agencije s određenim područjem primjene s obzirom na potrebe u skladu s novim političkim prioritetima i instrumentima te obnovljeni skup zadaća i funkcija Agencije kako bi se omogućila učinkovita i djelotvorna potpora državama članicama, institucijama EU-a i naporima drugih dionika u cilju osiguravanja sigurnog kiberprostora;

   - Europski okvir za kibersigurnosnu certifikaciju IKT proizvoda i usluga te pravila o europskim programima kibersigurnosne certifikacije kojima se omogućuje valjanost i priznavanje certifikata izdanih u okviru tih programa u svim državama članicama i kojima se nastoji uhvatiti ukoštac s trenutačnom fragmentacijom tržišta.

[1] Dok. 12183/17. 12183/1/17 REV 1; 12183/2/17 REV 2.

4. U listopadu 2017. Europsko vijeće[2] pozvalo je na to da se Komisijini prijedlozi za kibersigurnost izrade na cjelovit način, pravovremeno dostave i bez odgađanja razmotre na temelju akcijskog plana koji Vijeće treba uspostaviti.

5. Vijeće za opće poslove 12. prosinca 2017. donijelo je Akcijski plan[3] za provedbu Zaključaka Vijeća[4] o Zajedničkoj komunikaciji[5] Europskom parlamentu i Vijeću pod nazivom „Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a". U Akcijskom planu odražava se ambicija Vijeća da do lipnja 2018. postigne opći pristup u vezi s prijedlogom.

6. U Europskom parlamentu gđa Angelika NIEBLER (ITRE, EPP) imenovana je izvjestiteljicom. Glasovanje Odbora ITRE o svojem izvješću zakazano je za 19. lipnja 2018.

7. Europski gospodarski i socijalni odbor donio je svoje mišljenje 14. veljače 2018.

II. RAD U OKVIRU VIJEĆA

8. Komisija je predstavila ovaj prijedlog i njegovu procjenu učinka Horizontalnoj radnoj skupini za kiberpitanja (dalje u tekstu „Radna skupina") 26. rujna 2017., a zatim je Radna skupina 20. listopada 2017. razmotrila procjenu učinka. Naknadne rasprave bile su usmjerene na operativni kapacitet Agencije i opseg interakcije s nacionalnim nadležnim tijelima, kao i na učinak okvira za certifikaciju na tržište i poslovnu konkurentnost. Delegacije su u načelu dale pozitivno mišljenje i o procjeni učinka i o prijedlogu.

---

2 EUCO 14/17, točka 11.
3 Dok. 15748/17.
4 Dok. 14435/17.
5 Dok. 12211/17.

9. Raspravu o samom prijedlogu Radna skupina započela je u studenome 2017. u okviru estonskog predsjedništva te je nastavila s njome tijekom bugarskog predsjedanja. O tom prijedlogu održano je 12 sastanaka, iz kojih je proizašlo osam uzastopnih revidiranih verzija prijedloga s ciljem dogovora o općem pristupu na predstojećem sastanku Vijeća TTE (telekomunikacije) 8. lipnja 2018.

10. U Prilogu ovoj napomeni nalazi se rezultat rasprava u Radnoj skupini održanih 14. i 15. svibnja 2018, kao i revidirani kompromisni tekst predsjedništva. Uvodne izjave prilagođene su kako bi se odrazile promjene u materijalnim odredbama. Sve promjene u odnosu na Komisijin prijedlog označene su **podebljanim slovima** ili oznakom [...]. Promjene u odnosu na najnoviji dokument Radne skupine (8834/18) označene su **podebljanim i podcrtanim slovima**, a sva brisanja oznakom **[...]**.

III. ZAKLJUČAK

11. Kompromisni tekst predsjedništva , kako je utvrđen u Prilogu, odražava napore predsjedništva i država članica da u tekstu postignu odgovarajuću ravnotežu.

12. Odbor stalnih predstavnika postigao je 25. svibnja 2018. dogovor o kompromisnom tekstu predsjedništva podložno izmjenama članka 19. stavka 5. i članka 48. stavka 5. kako je utvrđeno u Prilogu.

13. Vijeće se stoga poziva da na svojem sastanku 8. lipnja 2018. donese opći pristup i predsjedništvu dodijeli mandat za početak pregovora o tom predmetu s predstavnicima Europskog parlamenta i Europske komisije.

PRILOG

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o ENISA-i, „*Agenciji [...] Europske unije za kibersigurnost*”, i stavljanju izvan snage Uredbe (EU) 526/2013 te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („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[6],

uzimajući u obzir mišljenje Odbora regija[7],

u skladu s redovnim zakonodavnim postupkom,

[6] SL C , , str. .
[7] SL C , , str. .

budući da:

(1) Mrežni i informacijski sustavi i telekomunikacijske mreže i usluge imaju ključnu ulogu u društvu i postali su okosnica gospodarskog rasta. Informacijska i komunikacijska tehnologija podupire složene sustave kojima se podupiru 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, poduzeća i javna tijela u cijeloj Uniji sada se koriste mrežnim i informacijskim sustavima. Digitalizacija i povezivost postaju ključne značajke sve većeg broja proizvoda i usluga, a uvođenjem interneta stvari očekuje se da će se u EU-u tijekom sljedećeg desetljeća upotrebljavati milijuni, ako ne i milijarde, povezanih digitalnih uređaja. Iako se na internet povezuje sve veći broj uređaja, sigurnost i otpornost nisu dostatno ugrađeni u dizajn, što dovodi do nedostatne kibersigurnosti. U tom kontekstu, zbog ograničene uporabe certifikacije, organizacije i pojedinačni korisnici nemaju dovoljno informacija o kibersigurnosnim značajkama IKT proizvoda i usluga, što smanjuje povjerenje u digitalna rješenja.

(3) Rast digitalizacije i povezivosti donosi veće kibersigurnosne rizike zbog čega je društvo u cjelini osjetljivije na prijetnje kibersigurnosti, a građani se suočavaju sa sve većim opasnostima, uključujući ranjive osobe kao što su djeca. Kako bi se ublažio taj rizik za društvo, treba poduzeti sve nužne mjere za poboljšanje kibersigurnosti u EU-u u cilju bolje zaštite mrežnih i informacijskih sustava, telekomunikacijskih mreža, digitalnih proizvoda, usluga i uređaja kojima se koriste građani, vlade i poduzeća, od MSP-ova do operatora ključnih infrastruktura, od kiberprijetnji.

(4) Kibernapadi su sve češći te je potrebna snažnija obrana povezanog gospodarstva i društva koje je osjetljivije na kiberprijetnje i napade. Međutim, iako su kibernapadi često prekogranični, politički odgovori nadležnih tijela za kibersigurnost i nadležnosti u području izvršavanja zakonodavstva uglavnom su nacionalne. Veliki kiberincidenti mogli bi uzrokovati prekid u opskrbi ključnim uslugama u cijelom EU-u. Zbog toga su potrebni učinkovit odgovor i upravljanje krizama na razini EU-a, koji se temelje na ciljanim politikama i opsežnijim instrumentima za europsku solidarnost i uzajamnu pomoć. Nadalje, za kreatore politike, industriju i korisnike stoga je važno 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.

(5) 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. One uključuju potrebu za daljnjim povećanjem sposobnosti i spremnosti država članica i poduzeća te za poboljšanjem suradnje i koordinacija u državama članicama i institucijama, agencijama i tijelima EU-a. Nadalje, s obzirom na to da kiberprijetnje ne poznaju granica, trebalo bi povećati sposobnosti na razini Unije kojima bi se mogla dopuniti djelovanja država članica, posebno u slučaju velikih prekograničnih kiberincidenata i kriza. Potrebno je uložiti dodatne napore u podizanje razine osviještenosti građana i poduzeća u području kibersigurnosti. Nadalje, povjerenje u jedinstveno digitalno tržište trebalo bi dodatno poboljšati ponudom transparentnih informacija o razini sigurnosti IKT proizvoda i usluga. To se može olakšati certificiranjem na razini EU-a kojim će se osigurati zajednički kibersigurnosni zahtjevi i kriteriji za evaluaciju na svim nacionalnim tržištima i u svim sektorima.

(6) Europski parlament i Vijeće donijeli su 2004. Uredbu (EZ) br. 460/2004[8] o osnivanju ENISA-e kako bi doprinijeli ciljevima osiguravanja visoke razine mrežne i informacijske sigurnosti u Uniji te razvoja kulture mrežne i informacijske sigurnosti u korist građana, potrošača, poduzeća i javnih uprava. Europski parlament i Vijeće donijeli su 2008. Uredbu (EZ) br. 1007/2008[9] o produljenju mandata Agencije do ožujka 2012. Uredbom (EZ) br. 580/2011[10] produljen je mandat Agencije do 13. rujna 2013. Europski parlament i Vijeće donijeli su 2013. Uredbu (EU) br. 526/2013[11] o ENISA-i i stavljanju izvan snage Uredbe (EZ) br. 460/2004, kojom je mandat Agencije proširen do lipnja 2020.

---

[8] 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.).

[9] 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.).

[10] 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.).

[11] 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.).

(7) Unija je već poduzela važne korake kako bi osigurala kibersigurnost i povećala povjerenje u digitalne tehnologije. Tijekom 2013. donesena je Strategija EU-a za kibersigurnost kako bi se usmjerio politički odgovor Unije na kibersigurnosne prijetnje i rizike. U cilju bolje zaštite Europljana na internetu Unija je 2016. donijela prvi zakonodavni akt u području kibersigurnosti, Direktivu (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije („Direktiva NIS"). Direktivom NIS 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, vodoopskrba, 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 pridonosi općem cilju postizanja visoke razine kibersigurnosti.

(8) Priznaje se da se od donošenja strategije EU-a o kibersigurnosti iz 2013. i posljednje revizije mandata Agencije znatno promijenio opći kontekst politike, među ostalim u pogledu nesigurnijeg globalnog okruženja. U tom kontekstu i 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 pridonosi odgovoru Unije na kiberizazove koji proizlaze iz bitno preobraženog okruženja prijetnji na koje Agencija, u okviru svojeg trenutačnog mandata, ne može odgovoriti.

(9) Agencija osnovana ovom Uredbom trebala bi naslijediti ENISA-u osnovanu Uredbom (EZ) br. 526/2013. Agencija bi trebala izvršavati zadaće koje su joj povjerene ovom Uredbom i pravnim aktima Unije u području kibersigurnosti pružanjem, među ostalim, stručnih savjeta i djelujući kao centar za informacije i znanje u Uniji. Ona bi trebala promicati razmjenu najbolje prakse među državama članicama i privatnim dionicima, Europskoj komisiji i državama članicama trebala bi davati prijedloge o politici, djelujući kao referentna točka za sektorske inicijative politike Unije u području kibersigurnosti i potičući operativnu suradnju među državama članicama i između država članica i europskih institucija, agencija i tijela.

(10) Odlukom 2004/97/EZ, Euratom, koja je donesena na sastanku Europskog vijeća od 13. prosinca 2003., predstavnici država članica odlučili su da će sjedište ENISA-e biti u Grčkoj u gradu koji odredi grčka vlada. Država članica domaćin Agencije 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 Agencija nalazi na odgovarajućoj lokaciji na kojoj su, među ostalim, osigurani odgovarajuća prometna povezanost te prostori za supružnike i djecu koji prate članove osoblja Agencije. Potrebne aranžmane trebalo bi utvrditi u sporazumu između Agencije i države članice domaćina koji se sklapa nakon dobivanja suglasnosti Upravljačkog odbora Agencije.

(11) S obzirom na sve veće izazove kibersigurnosti s kojima se Unija suočava, trebalo bi povećati financijske i ljudske resurse dodijeljene Agenciji u skladu s njezinom pojačanom ulogom i zadaćama i njezinom ključnom ulogom u ekosustavu organizacija koje brane europski digitalni ekosustav.

(12) Agencija bi trebala razviti i održavati visoku razinu stručnosti i djelovati kao referentna točka te bi svojom neovisnošću, kvalitetom savjeta i informacija koje pruža, transparentnošću postupaka i metoda rada te marljivošću u obavljanju svojih zadaća trebala uspostaviti povjerenje u jedinstveno tržište. Agencija bi trebala **podupirati** [...] nacionalne napore i **proaktivno doprinositi** naporima Unije pri obavljanju svojih zadaća u potpunoj suradnji s institucijama, [...] agencijama **i tijelima** Unije te državama članicama. Nadalje, rad Agencije trebao bi se temeljiti na informacijama dobivenima od privatnog sektora i suradnji s njim i drugim relevantnim dionicima. Skupom zadaća trebao bi se utvrditi način na koji će Agencija ostvariti svoje ciljeve, pri čemu joj se treba omogućiti fleksibilnost u radu.

(13) Agencija bi trebala pomagati Komisiji davanjem savjeta, mišljenja i analiza u vezi sa svim pitanjima Unije koja se odnose na razvoj, ažuriranje i preispitivanje politike i prava u području kibersigurnosti **te njezinih sektorskih aspekata radi jačanja relevantnosti politika i prava EU-a s dimenzijom kibersigurnosti i omogućavanja dosljednosti u njihovoj provedbi na nacionalnoj razini** [...]. Agencija bi trebala djelovati kao referentna točka za pružanje savjeta i stručnog znanja o sektorskoj politici i zakonodavnim inicijativama Unije kada je riječ o pitanjima kibersigurnosti.

(14) Osnovna je zadaća Agencije promicati dosljednu provedbu odgovarajućeg pravnog okvira, posebno učinkovitu provedbu Direktive NIS, što je od ključne važnosti za povećanje kiberotpornosti. S obzirom na okruženje prijetnji kibersigurnosti koje se brzo razvija, državama članicama treba pružiti potporu s pomoću sveobuhvatnijeg, horizontalnog pristupa izgradnji kiberotpornosti.

(15) Agencija bi trebala pomagati državama članicama i institucijama, [...] agencijama **i tijelima** Unije u njihovim naporima usmjerenima na izgradnju i jačanje sposobnosti i pripravnosti u cilju sprječavanja i otkrivanja [...] **prijetnji** i incidenata u području kibersigurnosti i odgovora na njih te u vezi sa sigurnošću mrežnih i informacijskih sustava. Agencija bi posebno trebala poduprijeti razvoj i jačanje nacionalnih CSIRT-ova u cilju postizanja visoke zajedničke razine njihove zrelosti u Uniji. **Aktivnosti ENISA-e koje se odnose na operativne kapacitete država članica trebale bi isključivo biti dopuna vlastitim aktivnostima država članica koje poduzimaju radi ispunjenja svojih obveza proizašlih iz Direktive NIS te ih stoga ne bi trebale nadomjestiti** [...].

(15a) Agencija bi usto trebala pomagati u razvoju i ažuriranju strategija Unije i, na zahtjev, strategija država članica o sigurnosti mrežnih i informacijskih sustava, osobito o kibersigurnosti, te promicati njihovo širenje i pratiti njihovu provedbu. Agencija bi trebala nuditi i osposobljavanja i obrazovne materijale javnim tijelima i, prema potrebi „osposobljavati voditelje osposobljavanja" kako bi pomogla državama članicama da razviju vlastite sposobnosti za osposobljavanje.

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

(17) U cilju poticanja suradnje između javnog i privatnog sektora i unutar privatnog sektora [...] **Agencija 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 procedurama, kao i smjernica za rješavanje regulatornih pitanja povezanih s razmjenom informacija, primjerice olakšavanjem** [...] uspostave sektorskih centara za razmjenu i analizu informacija (ISAC) [...].

(18) Agencija bi trebala objedinjavati i analizirati **dobrovoljna zajednička** nacionalna izvješća CSIRT-ova i CERT-EU-a **s ciljem pomaganja državama članicama** pri uspostavi zajedničkih [...] **procedura**, jezika i terminologije za razmjenu informacija. Agencija bi trebala uključiti i privatni sektor, u okviru Direktive NIS kojom je utvrđena osnova za dobrovoljnu razmjenu tehničkih informacija na operativnoj razini [...] **u okviru** mreže CSIRT-ova.

(19) Agencija bi trebala doprinijeti odgovoru na razini EU-a u slučaju prekograničnih kibersigurnosnih incidenata i kiberkriza velikih razmjera. Tu funkciju trebala bi **obavljati sukladno svojem mandatu u skladu s ovom Uredbom i pristupom koji trebaju dogovoriti države članice u kontekstu Preporuke Komisije o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera. Mogla bi** uključivati prikupljanje relevantnih informacija i posredovanje između mreže CSIRT-ova i tehničke zajednice te donositelja odluka koji su odgovorni za upravljanje krizom. Nadalje, Agencija bi mogla pružati tehničku pomoć u slučaju incidenata olakšavanjem odgovarajuće tehničke razmjene rješenja među državama članicama i obavješćivanjem javnosti. Agencija bi trebala poduprijeti taj postupak ispitivanjem načina takve suradnje s pomoću [...] **redovnih** vježbi u području kibersigurnosti.

(20) [...] Agencija bi **pri podupiranju** operativne **suradnje** [...] trebala iskoristiti dostupnu **tehničku i operativnu** stručnost CERT-EU-a u okviru strukturirane suradnje [...]. [...] Prema potrebi trebalo bi uspostaviti posebne aranžmane između te dvije organizacije radi definiranja praktične provedbe takve suradnje **i izbjegavanja udvostručavanja aktivnosti.**

(21) U skladu sa svojim [...] zadaćama **za pružanje potpore operativnoj suradnji u okviru mreže CSIRT-ova** Agencija 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 analiza prijetnji i incidenata. **U okviru olakšavanja tehničkog postupanja u slučaju incidenata sa značajnim ili bitnim učinkom ENISA bi osobito trebala podupirati dobrovoljnu razmjenu tehničkih rješenja među državama članicama ili kombinirati tehničke informacije kao što su tehnička rješenja koja države članice dobrovoljno razmjenjuju.** U Preporuci Komisije o koordiniranom odgovoru na velike kiberincidente i kiberprijetnje preporučuje se da države članice surađuju u dobroj vjeri te da uzajamno i s ENISA-om bez nepotrebnog odlaganja razmjenjuju informacije o velikim incidentima i krizama u području kibersigurnosti. Takvim informacijama trebalo bi se dodatno pomoći ENISA-i pri [...] **podupiranju operativne suradnje**.

(22) U okviru redovne suradnje na tehničkoj razini u cilju podupiranja informiranosti o stanju u Uniji, Agencija bi trebala redovito **i u bliskoj suradnji s državama članicama** izrađivati tehničko izvješće o stanju kibersigurnosti EU-a u pogledu incidenata i prijetnji, na temelju javno dostupnih informacija, vlastite analize i izvješća koje s njom dijele CSIRT-ovi država članica [...] ili jedinstvene kontaktne točke iz Direktive NIS **(u oba slučaja na dobrovoljnoj osnovi)**, Europski centar za kiberkriminalitet (EC3) pri Europolu, CERT-EU i, prema potrebi, Obavještajni i situacijski centar EU-a (INTCEN) pri Europskoj službi za vanjsko djelovanje (ESVD). Izvješće bi trebalo stavljati na raspolaganje relevantnim instancama pri Vijeću, Komisiji, Visokom predstavniku Unije za vanjske poslove i sigurnosnu politiku i mreži CSIRT-ova.

(23) **Potpora Agencije *e***[...]*x-post* tehničkim **istragama** [...] incidenata sa značajnim učinkom [...] na zahtjev [...] **pogođenih** država članica [...] trebala bi biti usmjerena na sprečavanje budućih incidenata [...]. **Dotične države članice trebale bi pružiti potrebne informacije kako bi Agencija mogla učinkovito podupirati tehničku istragu.**

(24) [...]

(25) Države članice mogu pozvati poduzeća pogođena incidentom da surađuju pružanjem potrebnih informacija i pomoći Agenciji ne dovodeći u pitanje njihovo pravo na zaštitu poslovno osjetljivih informacija.

(26) Kako bi bolje razumjela izazove u području kibersigurnosti i u cilju pružanja strateških dugoročnih savjeta državama članicama i institucijama Unije, Agencija mora analizirati postojeće i nove rizike. U tu svrhu Agencija 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 tehničkih inovacija na mrežnu i informacijsku sigurnost, posebno na kibersigurnost. Nadalje, Agencija bi analizom prijetnji i incidenata trebala pomagati državama članicama i institucijama, agencijama i tijelima Unije u prepoznavanju novih prijetnji i sprečavanju [...] kibersigurnosnih **incidenata**.

(27) U cilju povećanja otpornosti Unije Agencija bi trebala razvijati izvrsnost u području **kiber**sigurnosti **infrastruktura koje posebno podupiru sektore iz Priloga II. Direktivi NIS i onih koje upotrebljavaju pružatelji digitalnih usluga navedeni u Prilogu III. toj Direktivi** [...] pružanjem savjeta, smjernica i najboljih praksi. Kako bi osigurala lakši pristup bolje strukturiranim informacijama o kibersigurnosnim rizicima i mogućim lijekovima, Agencija 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, agencija i tijela na razini EU-a i nacionalnoj razini.

(28) Agencija bi trebala doprinijeti podizanju razine osviještenosti javnosti o rizicima povezanima s kibersigurnošću i davati smjernice o dobroj praksi za pojedinačne korisnike koje su usmjerene na građane i organizacije. Agencija bi trebala doprinositi i promicanju najbolje prakse i rješenja na razini pojedinaca i organizacija prikupljanjem i analizom javno dostupnih informacija o znatnim incidentima i sastavljanjem izvješća u cilju pružanja smjernica poduzećima i građanima i poboljšanja opće razine pripravnosti i otpornosti. Nadalje, Agencija bi u suradnji s državama članicama i institucijama, [...] agencijama **i tijelima** Unije trebala organizirati redovite kampanje informiranja i obrazovanja javnosti namijenjene krajnjim korisnicima s ciljem poticanja sigurnijeg ponašanja pojedinaca na internetu, podizanja razine osviještenosti o potencijalnim opasnostima u kiberprostoru, uključujući oblike kiberkriminaliteta kao što su *phishing* napadi, mreže zaraženih računala (*botnet*) te financijske i bankovne prijevare, i poticanja osnovnog savjetovanja o autentikaciji i zaštiti podataka. Agencija bi trebala imati glavnu ulogu u bržem osvješćivanju krajnjih korisnika o sigurnosti uređaja.

(29) Kako bi pružala potporu poduzećima koja djeluju u sektoru kibersigurnosti i korisnicima kibersigurnosnih rješenja, Agencija bi trebala razviti i održavati „opservatorij tržišta" provođenjem redovitih analiza i širenjem glavnih kretanja na kibersigurnosnom tržištu na strani ponude i potražnje.

(30) Kako bi u potpunosti ostvarila svoje ciljeve. Agencija bi se trebala povezati s relevantnim institucijama, agencijama i tijelima, među ostalim s CERT-EU-om, Europskim centrom za kiberkriminalitet (EC3) pri Europolu, Europskom obrambenom agencijom (EDA), Europskom agencijom za operativno upravljanje opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde (eu-LISA), Europskom agencijom za sigurnost zračnog prometa (EASA)**, Agencijom za europski GNSS (Agencija za GNSS)** i s drugim agencijama EU-a koje djeluju u području kibersigurnosti. Ona bi se trebala povezati i s nadležnim tijelima za zaštitu podataka u cilju razmjene znanja i najbolje prakse i u cilju davanja savjeta o aspektima kibersigurnosti koji bi mogli utjecati na njihov rad. Predstavnici nacionalnih tijela kaznenog progona i tijela kaznenog progona na razini Unije te nacionalnih tijela i tijela Unije za zaštitu privatnosti trebali bi imati pravo da budu zastupljeni u Stalnoj interesnoj skupini Agencije. Pri povezivanju s tijelima kaznenog progona u vezi s aspektima mrežne i informacijske sigurnosti koji mogu utjecati na njihov rad, Agencija bi trebala poštovati postojeće informacijske kanale i uspostavljene mreže.

(31) Agencija, **u ulozi** [...] tajništva mreže CSIRT-ova, trebala bi podupirati CSIRT-ove u državama članicama i CERT-EU u operativnoj suradnji kao i u svim relevantnim zadaćama mreže CSIRT-ova kako su definirane u Direktivi NIS. Nadalje, Agencija 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 mogu uključivati najmanje dva CERT-a uzimajući u obzir standardne operativne postupke mreže CSIRT-ova.

(32) U cilju povećanja pripravnosti Unije za odgovor na kiberincidente Agencija bi trebala organizirati [...] **redovne** vježbe u području kibersigurnosti na razini Unije te državama članicama, institucijama, agencijama i tijelima EU-a na njihov zahtjev pomagati pri organizaciji vježbi.

(33) Agencija bi trebala dalje razvijati i održavati svoje stručno znanje u području kibersigurnosne certifikacije radi potpore politici Unije u tom području. Agencija bi trebala promicati prihvaćanje kibersigurnosne certifikacije u Uniji, među ostalim pridonošenjem uspostavi okvira za kibersigurnosnu certifikaciju na razini Unije i njegovu održavanju, u cilju povećanja transparentnosti kibersigurnosnog jamstva za IKT proizvode i usluge i jačanja povjerenja u jedinstveno digitalno tržište.

(34) Učinkovitu kibersigurnosnu politiku trebalo bi temeljiti na dobro razrađenim metodama procjene rizika, kako u javnom tako 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 svrhu Agencija bi trebala podupirati suradnju između dionika na razini Unije i time olakšati 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.

(35) Agencija bi trebala poticati države članice i pružatelje usluga da povećaju svoje opće sigurnosne standarde kako bi svi korisnici interneta mogli poduzeti potrebne korake za osiguranje svoje osobne kibersigurnosti. Konkretno, pružatelji usluga i proizvođači proizvoda trebali bi povući ili reciklirati proizvode i usluge koji ne zadovoljavaju standarde kibersigurnosti. ENISA, u suradnji s nadležnim tijelima, može širiti informacije o razini kibersigurnosti proizvoda i usluga koje se nude na unutarnjem tržištu te pružateljima i proizvođačima izdavati upozorenja u kojima od njih traži da poboljšaju sigurnost, uključujući kibersigurnost, svojih proizvoda i usluga.

(36) Agencija bi trebala u potpunosti uzeti u obzir aktualne aktivnosti istraživanja, razvoja i tehnoloških ocjena, osobito one aktivnosti koje se provode u okviru različitih istraživačkih inicijativa Unije kako bi institucijama, [...] agencijama **i tijelima** Unije te, kada je to relevantno, državama članicama na njihov zahtjev pružala savjete o istraživačkim potrebama u području [...] kibersigurnosti. **U cilju utvrđivanja istraživačkih potreba i prioriteta Agencija bi se također trebala savjetovati s relevantnim skupinama korisnika.**

(37) **Prijetnje** [...] kibersigurnosti globalni su problemi. Potrebna je bliža međunarodna suradnja radi unaprjeđenja **kiber**sigurnosnih standarda, uključujući definiciju zajedničkih normi ponašanja, razmjenu informacija, poticanje brže međunarodne suradnje kao odgovor na pitanja mrežne i informacijske sigurnosti, kao i zajednički globalni pristup tim pitanjima. U tu svrhu Agencija bi pružanjem, prema potrebi, potrebnog stručnog znanja i analize relevantnim institucijama, [...] agencijama **i tijelima** Unije trebala podupirati daljnje uključivanje Unije te njezinu suradnju s trećim zemljama i međunarodnim organizacijama.

(38) Agencija bi trebala moći odgovoriti na *ad hoc* zahtjeve za savjete i pomoć država članica i institucija, agencija i tijela EU-a ako su u okviru njezinih ciljeva.

(39) Potrebno je provesti određena načela povezana s upravljanjem Agencijom radi usklađivanja sa zajedničkom izjavom i zajedničkim pristupom koje je u srpnju 2012. dogovorila Međuinstitucionalna radna skupina za decentralizirane agencije EU-a, pri čemu je svrha izjave i pristupa usuglašavanje aktivnosti agencija i poboljšanje njihova djelovanja. Zajednička izjava i zajednički pristup trebali bi se, prema potrebi, odražavati i u programima rada Agencije, evaluacijama Agencije te praksi Agencije u vezi s izvješćivanjem i upravljanjem.

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

(41) U cilju pravilnog i djelotvornog funkcioniranja Agencije Komisija i države članice trebale bi osigurati da osobe koje će imenovati u Upravljački odbor imaju odgovarajuća stručna znanja i iskustvo u područjima njezina djelovanja. Komisija i države članice također bi trebale ograničiti učestalost izmjena njihovih predstavnika u Upravljačkom odboru kako bi se osigurao kontinuitet njihova rada.

(42) Kako bi se osiguralo nesmetano funkcioniranje Agencije, njezin izvršni direktor imenuje se na temelju zasluga i dokazanih administrativnih i rukovoditeljskih sposobnosti, kao i sposobnosti i iskustava relevantnih za kibersigurnost, a svoje dužnosti obavlja potpuno neovisno. Izvršni direktor trebao bi, nakon prethodnog savjetovanja s Komisijom, pripremiti prijedlog programa rada Agencije i poduzeti sve potrebne korake kako bi osigurao njegovo pravilno izvršenje. Izvršni direktor trebao bi izraditi godišnje izvješće **uključujući provedbu godišnjeg programa rada Agencije** koji se dostavljaju Upravljačkom odboru, sastaviti nacrt izvješća o procjenama prihoda i rashoda Agencije te izvršavati 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. Izvršni direktor trebao bi osigurati odabir članova ad hoc radnih skupina u skladu s najvišim standardima struke, uzimajući pritom u obzir ravnotežu među predstavnicima kada je to potrebno s obzirom na predmetna specifična pitanja, između javnih uprava država članica, institucija Unije i privatnog sektora, uključujući industriju, korisnike i akademske stručnjake iz područja mrežne i informacijske sigurnosti.

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

(44) Agencija bi trebala imati Stalnu interesnu skupinu kao savjetodavno tijelo kako bi se osigurao redoviti dijalog s privatnim sektorom, organizacijama potrošača i drugim interesnim skupinama. Stalna interesna skupina, koju na prijedlog izvršnog direktora osniva Upravljački odbor, trebala bi se usredotočiti na pitanja relevantna za dionike te bi trebala Agenciji skrenuti pozornost na njih. Sastav Stalne interesne skupine, s kojom se posebno treba savjetovati u pogledu nacrta programa rada, i njezinim zadaćama trebao bi osigurati dostatnu zastupljenost dionika u radu Agencije.

(45) Agencija bi trebala uspostaviti pravila o sprječavanja sukoba interesa i upravljanju njime. Agencija bi trebala primjenjivati relevantne odredbe Unije o javnom pristupu dokumentima u skladu s Uredbom (EZ) br. 1049/2001 Europskog parlamenta i Vijeća[12]. Agencija bi trebala obrađivati osobne podatke u skladu s Uredbom (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka[13]. Agencija bi se trebala pridržavati odredaba primjenljivih na institucije Unije i nacionalnog zakonodavstva u vezi s postupanjem s osjetljivim dokumentima, posebno s osjetljivim neklasificiranim podacima i klasificiranim podacima EU-a.

---

[12] 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.).

[13] SL L 8, 12.1.2001., str. 1.

(46) Kako bi se zajamčila potpuna autonomija i neovisnost Agencije i kako bi joj se omogućilo obavljanje dodatnih i novih zadaća, uključujući nepredviđene hitne zadaće, Agenciji bi trebalo osigurati dostatni i autonomni proračun s prihodima prvenstveno iz doprinosa Unije i doprinosa trećih zemalja koje sudjeluju u radu Agencije. Veći dio osoblja Agencija trebao bi izravno sudjelovati u operativnoj provedbi mandata Agencije. Državi članici domaćinu ili bilo kojoj drugoj državi članici trebalo bi omogućiti davanje dobrovoljnih doprinosa prihodima Agencije. Na subvencije koje se financiraju iz općeg proračuna Unije trebao bi se i dalje primjenjivati proračunski postupak Unije. Štoviše, Revizorski sud trebao bi provesti reviziju računa Agencije radi osiguranja transparentnosti i odgovornosti.

(47) [...]

(48) Kibersigurnosna certifikacija ima važnu ulogu u jačanju povjerenja u IKT proizvode i usluge i njihovu sigurnost. Jedinstveno digitalno tržište, posebno podatkovno gospodarstvo i internet stvari, mogu se razvijati samo ako postoji opće povjerenje javnosti da se takvim proizvodima i uslugama osigurava određena razina kibersigurnosnog jamstva. Povezani i automatizirani automobili, elektronički medicinski proizvodi, industrijski automatizirani kontrolni sustavi ili pametne mreže samo su primjeri sektora u kojima se certificiranje već u velikoj mjeri primjenjuje ili će se vjerojatno primjenjivati u skoroj budućnosti. Kibersigurnosna certifikacija od ključne je važnosti u sektorima uređenima Direktivom NIS. U Komunikaciji iz 2016.

(49) 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 i usluga 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 postupaka certificiranja na razini EU-a neki su od nedostataka koji utječu na jedinstveno tržište kibersigurnosti. S jedne strane, time je europskim poduzećima otežano tržišno natjecanje na nacionalnoj, europskoj i svjetskoj razini. S druge strane, ograničen je izbor održivih i iskoristivih kibersigurnosnih tehnologija koje su dostupne građanima i poduzećima. Slično tomu, u preispitivanju provedbe Strategije jedinstvenog digitalnog tržišta na sredini provedbenog razdoblja Komisija je istaknula da su potrebni sigurni povezani proizvodi i sustavi i navela je da bi se stvaranjem europskog okvira za sigurnost IKT-a kojim se utvrđuju pravila o organizaciji sigurnosnog certificiranja u području IKT-a moglo očuvati povjerenje u internet i riješiti trenutačni problem fragmentacije kibersigurnosnog tržišta.

(50) Trenutačno se kibersigurnosna certifikacija IKT **postupaka,** proizvoda i usluga provodi samo u ograničenoj mjeri. Ako postoji, ona se većinom provodi na razini države članice ili u okviru programa industrijskih sektora. U tom kontekstu druge države članice u načelu ne priznaju certifikat koji je izdalo jedno nacionalno tijelo za kibersigurnost. Trgovačka društva stoga će možda morati certificirati svoje proizvode i usluge u nekoliko država članica u kojima djeluju, na primjer radi sudjelovanja u nacionalnim postupcima javne nabave. Nadalje, iako se javljaju novi programi, čini se da ne postoji usklađen i holistički pristup pitanjima horizontalne kibersigurnosti, na primjer u području interneta stvari. U postojećim programima postoje znatni nedostaci i razlike u pogledu opsega proizvoda, razine jamstva, materijalnih kriterija i stvarne upotrebe.

(51) U prošlosti je bilo pokušaja postizanja uzajamnog priznavanja certifikata u Europi. 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 sigurnosnog certificiranja, [...] SOG-IS uključuje samo dio država članica Unije. Zbog toga je ograničena djelotvornost sporazuma o uzajamnom priznavanju SOG-IS-a sa stajališta unutarnjeg tržišta.

(52) S obzirom na navedeno nužno je uspostaviti europski okvir za kibersigurnosnu certifikaciju kojim se utvrđuju glavni horizontalni zahtjevi za razvoj budućih europskih programa kibersigurnosne certifikacije koji omogućuju priznavanje i uporabu certifikata i **izjava EU-a o sukladnosti** za IKT proizvode i usluge u svim državama članicama. Europski okvir trebao bi imati dvostruku svrhu: s jedne strane, njime bi se trebalo doprinijeti povećanju povjerenja u IKT proizvode i usluge koji su certificirani u skladu s tim programima. S druge strane, njime bi se trebalo izbjeći umnožavanje proturječnih ili preklapajućih nacionalnih kibersigurnosnih certifikacija i tako smanjiti troškovi poduzećima koja djeluju na jedinstvenom digitalnom tržištu. Ti programi trebali bi biti nediskriminirajući i temeljiti se na međunarodnim i/ili [...] **europskim** normama, osim ako su te norme neučinkovite ili neprimjerene za ispunjavanje zakonitih ciljeva EU-a u tom pogledu.

(53) Komisija bi trebala imati ovlasti donositi europske programe kibersigurnosne certifikacije za određene skupine IKT **postupaka,** proizvoda i usluga. 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 certificiranja kojima upravlja industrija ili privatne organizacije trebali bi biti izvan područja primjene Uredbe. Međutim, tijela koja provode takve programe mogu Komisiji predložiti da razmotri odobravanje tih programa kao europskih programa.

(54) Odredbama ove Uredbe ne bi se trebalo dovoditi u pitanje zakonodavstvo Unije kojim se propisuju posebna pravila o certifikaciji IKT proizvoda i usluga. U Uredbi (EU) 2016/679 (Opća uredba o zaštiti podataka) propisane su odredbe o uspostavi programa certificiranja te pečata i oznaka za zaštitu podataka za potrebe dokazivanja usklađenosti s Uredbom postupaka obrade koje obavljaju voditelji ili izvršitelji obrade. Tim postupcima certificiranja i pečatima i oznakama za zaštitu podataka trebalo bi se osobama čiji se podaci obrađuju omogućiti da brzo ocijene razinu zaštite podataka relevantnih proizvoda i usluga. Ovom Uredbom ne dovodi se u pitanje certificiranje postupaka obrade podataka, uključujući kada su ti postupci ugrađeni u proizvode i usluge, u skladu s Općom uredbom o zaštiti podataka.

(55) Svrha europskih programa kibersigurnosne certifikacije trebala bi biti osiguravanje toga da IKT **postupci,** proizvodi i usluge koji su certificirani u okviru takvog programa zadovoljavaju određene zahtjeve [...] **u** cilju [...] **zaštite** 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, postupaka, usluga i sustava **tijekom njihova životnog ciklusa** u smislu ove Uredbe. U ovoj Uredbi ne mogu se podrobno utvrditi kibersigurnosni zahtjevi povezani sa svim IKT **postupcima,** proizvodima i uslugama. IKT **postupci,** proizvodi i usluge i povezane kibersigurnosne potrebe toliko su različiti da je teško osmisliti opće kibersigurnosne zahtjeve koji se mogu svuda primjenjivati. Stoga je za potrebe certifikacije potrebno prihvatiti širok i općenit pojam kibersigurnosti dopunjen skupom kibersigurnosnih ciljeva koje treba uzeti u obzir pri izradi europskih programa kibersigurnosne certifikacije. Načine postizanja tih ciljeva u određenim IKT **postupcima,** proizvodima i uslugama trebalo bi potom podrobnije opisati na razini pojedinačnog programa certificiranja koji je donijela Komisija, na primjer upućivanjem na norme ili tehničke specifikacije **ako nisu dostupne odgovarajuće norme**.

(55a) Tehničke specifikacije koje treba upotrebljavati u europskom programu kibersigurnosne certifikacije trebalo bi utvrditi uz poštovanje načela iz Priloga II. Uredbi (EU) br. 1025/2012. Međutim, neka odstupanja od tih načela mogla bi se smatrati potrebnima u opravdanim slučajevima upotrebe tih tehničkih specifikacija u europskom programu kibersigurnosne certifikacije koji se odnosi na visoku razinu jamstva. Razlozi za takva odstupanja moraju biti javno dostupni.

(55b) Certificirano ocjenjivanje sukladnosti postupak je kojim se evaluira jesu li ispunjeni određeni zahtjevi koji se odnose na IKT postupak, proizvod ili uslugu. Taj postupak provodi neovisna treća strana koja nije proizvođač proizvoda ili pružatelj usluge. Postupak izdavanja certifikata slijedi nakon postupka uspješne evaluacije IKT postupka, proizvoda ili usluge. Trebalo bi ga smatrati potvrdom da je dotična evaluacija pravilno provedena. Ovisno o razini jamstva, europskim kibersigurnosnim programom trebalo bi navesti je li certifikat izdalo privatno ili javno tijelo. Samim ocjenjivanjem sukladnosti i certifikacijom ne može se jamčiti kibersigurnost certificiranih IKT proizvoda i usluga. Riječ je o postupku i tehničkoj metodologiji kojima se potvrđuje da su IKT proizvodi i usluge testirani i da su u skladu s određenim kibersigurnosnim zahtjevima koji su propisani drugdje, na primjer u tehničkim normama.

(55c) Odabir odgovarajuće razine certifikacije i pripadajućih sigurnosnih zahtjeva, koji vrše korisnici certifikata, trebao bi se temeljiti na analizi rizika u vezi s uporabom IKT postupka, proizvoda ili usluge. Razina jamstva stoga bi trebala biti razmjerna razini rizika povezanog s predviđenom uporabom IKT postupka, proizvoda ili usluge.

(55d) Europskim programom kibersigurnosne certifikacije moglo bi se osigurati da se ocjenjivanje sukladnosti provodi pod isključivom odgovornošću proizvođača ili pružatelja IKT proizvoda i usluga (samoocjenjivanje sukladnosti). U takvim je slučajevima dovoljno da proizvođač ili pružatelj usluga sam provodi sve provjere kako bi osigurao sukladnost IKT postupka, proizvoda ili usluga s programom certifikacije. Tu bi se vrstu ocjenjivanja sukladnosti trebalo smatrati primjerenom s obzirom na IKT proizvode i usluge niske razine složenosti (npr. jednostavan dizajn i mehanizam proizvodnje) koji predstavljaju nizak rizik za javni interes. Osim toga, samo bi IKT proizvodi i usluge koji odgovaraju osnovnoj razini jamstva mogli postati podložni samoocjenjivanju sukladnosti.

(55e) Europskim programom kibersigurnosne certifikacije moglo bi se omogućiti i certifikaciju i samoocjenjivanju sukladnosti IKT proizvoda i usluga. U tom slučaju programom bi trebalo osigurati jasan i razumljiv način s pomoću kojeg bi potrošači ili drugi korisnici razlikovali proizvode i usluge koji se ocjenjuju u okviru odgovornosti proizvođača ili pružatelja te proizvode i usluge koje certificira treća strana.

(55f) Proizvođač ili pružatelj IKT proizvoda i usluga koji provodi samoocjenjivanje sukladnosti trebao bi sastaviti i potpisati izjavu EU-a o sukladnosti kao dio postupka ocjenjivanja sukladnosti. Izjava EU-a o sukladnosti dokument je u kojem se navodi da određeni IKT proizvod ili usluga ispunjava zahtjeve programa. Sastavljanjem i potpisivanjem izjave EU-a o sukladnosti proizvođač ili pružatelj preuzima odgovornost za sukladnost IKT proizvoda ili usluge s pravnim zahtjevima programa. Primjerak izjave EU-a o sukladnosti trebalo bi podnijeti nacionalnom tijelu za kibersigurnosnu certifikaciju i ENISA-i.

(55g) Izjavu EU-a o sukladnosti i tehničku dokumentaciju o svim relevantnim informacijama o sukladnosti IKT proizvoda ili usluga s konkretnim programom proizvođač ili pružatelj IKT proizvoda i usluga trebao bi činiti dostupnom nadležnom nacionalnom tijelu za kibersigurnosnu certifikaciju u razdoblju utvrđenim u tom europskom programu kibersigurnosne certifikacije. Tehničkom dokumentacijom trebali bi se pobliže odrediti primjenjivi zahtjevi i obuhvatiti, u mjeri u kojoj je to bitno za ocjenjivanje, oblikovanje, izrada i funkcioniranje IKT proizvoda ili usluge. Tehničku dokumentaciju trebalo bi sastaviti tako da se omogući ocjena sukladnosti IKT proizvoda ili usluge s relevantnim zahtjevima.

(55h) Države članice i zainteresirane organizacije dionika trebale bi imati pravo predložiti Europskoj skupini za kibersigurnosnu certifikaciju izradu prijedloga programa. Zainteresirane organizacije dionika obuhvaćaju udruge predstavnika industrije ili potrošača, uključujući predstavnike organizacija malih i srednjih poduzeća koje imaju valjani interes za razvoj određenog europskog programa kibersigurnosne certifikacije. Takvi prijedlozi trebali bi se ispitati s obzirom na kriterije koje je razvila Europska skupina za kibersigurnosnu certifikaciju na temelju smjernica koje se zasnivaju na načelima transparentnosti, otvorenosti, nepristranosti, konsenzusa, djelotvornosti, relevantnosti i usklađenosti.

(56) Komisija **i Skupina** trebale bi imati ovlasti zatražiti od ENISA-e da **bez nepotrebnog odlaganja** izradi prijedloge programa za određene IKT **postupke,** proizvode ili usluge. Komisija bi na temelju prijedloga programa 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. Oni bi trebali uključivati, među ostalim, područje primjene i cilj kibersigurnosne certifikacije, uključujući kategorije obuhvaćenih IKT **postupaka,** proizvoda i usluga, detaljnu specifikaciju kibersigurnosnih zahtjeva, na primjer upućivanjem na norme ili tehničke specifikacije, posebne kriterije i metode evaluacije i predviđenu razinu jamstva: osnovnu, znatnu i/ili visoku **i razine evaluacije kada je to primjenjivo**.

(56a) Na jamstvu europskog programa certifikacije zasniva se povjerenje u to da IKT postupak, proizvod ili usluga zadovoljava sigurnosne zahtjeve određenog europskog programa kibersigurnosne certifikacije. Kako bi se osigurala dosljednost okvira koji se odnosi na certificirane IKT postupke, proizvode i usluge, europskim programom kibersigurnosne certifikacije moglo bi se definirati razine sigurnosti za europske kibersigurnosne certifikate i izjave EU-a o sukladnosti izdane u okviru tog programa. Svaki bi se certifikat mogao odnositi na jednu od razina jamstva: osnovnu, znatnu ili visoku, dok bi se izjava EU-a o sukladnosti mogla odnositi samo na osnovnu razinu jamstva. Razine jamstva osiguravaju odgovarajući stupanj napora pri evaluaciji [...] te ih obilježava upućivanje na tehničke specifikacije, norme i s njima povezane procedure, uključujući tehničke kontrole, čija je svrha ublažiti ili spriječiti kibersigurnosne incidente. Svaka razina jamstva trebala bi biti usklađena među različitim sektorima u kojima se primjenjuje certifikacija.

(56b) U okviru europskog programa kibersigurnosne certifikacije može se utvrditi nekoliko razina evaluacije ovisno o strogosti i opsežnosti upotrijebljene metodologije evaluacije, koja bi trebala odgovarati jednoj od razina jamstva i biti povezana s odgovarajućom kombinacijom sastavnica jamstva. Na svim razinama jamstva IKT proizvod ili usluga trebali bi sadržavati niz sigurnih funkcija, kako je definirano programom, koje mogu uključivati: sigurnu zadanu konfiguraciju, potpisanu šifru, sigurno ažuriranje i ublažavanje mogućnosti iskorištavanja te potpunu zaštitu *stack*/*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 (i softver i hardver) pouzdano ugrađeni. Za osnovnu razinu jamstva evaluacija bi se trebala rukovoditi barem sljedećim sastavnicama jamstva: evaluacija bi trebala uključivati barem pregled tehničke dokumentacije IKT proizvoda ili usluge od strane tijela za ocjenjivanje sukladnosti. Ako certifikacija uključuje IKT postupke, i postupak koji se upotrebljava za oblikovanje, razvoj i održavanje IKT proizvoda ili usluge trebao bi biti podložan tehničkom preispitivanju. U slučajevima kada se europskim programom kibersigurnosne certifikacije predviđa samoocjenjivanje sukladnosti, trebalo bi biti dovoljno da proizvođač ili pružatelj usluga provede samoocjenu usklađenosti IKT postupka, proizvoda ili usluga s programom certifikacije. Kad je riječ o znatnoj razini jamstva, evaluacija bi, uz osnovnu razinu jamstva, trebala biti u skladu barem s provjerom sukladnosti sigurnosnih funkcija IKT proizvoda ili usluge s njegovom tehničkom dokumentacijom. Kad je riječ o visokoj razini jamstva, pri evaluaciji bi, uz znatnu razinu jamstva, trebalo provesti barem ispitivanje učinkovitosti kojim se procjenjuje otpornost sigurnosnih funkcija IKT proizvoda ili usluge na one koji provode napredne kibernapade i posjeduju značajne vještine i resurse.

(56c) Pri izradi prijedloga programa ENISA bi se trebala savjetovati sa svim relevantnim dionicima kao što su europske organizacije za normizaciju, relevantna nacionalna tijela, organizacije koje se temelje na sporazumima o uzajamnom priznavanju kao što su sporazumi o uzajamnom priznavanju SOG-IS, MSP-ovima, udrugama potrošača te okolišnim i društvenim dionicima.

(56d) ENISA bi trebala održavati internetske stranice na kojima pruža informacije o europskim programima kibersigurnosne certifikacije i daje im vidljivost, a koje bi, među ostalim, trebale uključivati zahtjeve za izradu prijedloga europskog programa kibersigurnosne certifikacije kao i povratne informacije dobivene u okviru postupka savjetovanja koje ENISA provodi u pripremnoj fazi. Takve internetske stranice također bi trebale pružiti informacije o certifikatima i izjavama EU-a o sukladnosti izdanima na temelju ove Uredbe.

(57) Primjena europske kibersigurnosne certifikacije **i izjave EU-a o sukladnosti** trebala bi biti dobrovoljna, osim ako je u zakonodavstvu Unije ili nacionalnom zakonodavstvu **donesenom u skladu s pravom Unije** predviđeno drugačije. **U nedostatku usklađenog zakonodavstva države članice mogu donijeti nacionalne tehničke propise u skladu s Direktivom (EU) 2015/1535 o obveznom certificiranju u okviru europskog programa kibersigurnosne certifikacije. Države članice mogle bi upotrebljavati i europsku kibersigurnosnu certifikaciju u kontekstu javne nabave i Direktive 2014/214/EU.**[...]

(57a) Kako bi se ostvarili ciljevi ove Uredbe i izbjegla fragmentacija unutarnjeg tržišta, nacionalni programi kibersigurnosne certifikacije ili procedure za IKT proizvode i usluge obuhvaćene europskim programom kibersigurnosne certifikacije trebali bi prestati proizvoditi učinke od datuma koji Komisija odredi provedbenim aktom. Štoviše, države članice ne bi trebale uvoditi nove nacionalne programe kibersigurnosne certifikacije IKT proizvoda i usluga 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.

(58) Nakon donošenja europskog programa kibersigurnosne certifikacije proizvođači IKT proizvoda ili pružatelji IKT usluga moći će podnijeti zahtjev za certifikaciju svojih proizvoda i usluga tijelu za ocjenjivanje sukladnosti po svojem izboru. Tijela za ocjenjivanje sukladnosti trebalo bi akreditirati akreditacijsko tijelo ako ispunjavaju određene zahtjeve propisane ovom Uredbom. Akreditacija bi se trebala izdavati na najviše pet godina i može se obnoviti pod istim uvjetima ako tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve. 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.

(59) [...] Države članice [...] **trebale bi** imenovati jedno **ili više tijela** za kibersigurnosnu certifikaciju [...] za nadzor usklađenosti **s obvezama koje proizlaze iz ove Uredbe. Ako država članica to smatra primjerenim, zadaće se mogu dodijeliti i već postojećim tijelima. Države članice također bi trebale moći odlučivati, na temelju uzajamnog dogovora s drugom državom članicom, o imenovanju jednog ili više nadzornih tijela na državnom području te druge države članice. To bi tijelo posebno trebalo pratiti i izvršavati obveze proizvođača ili pružatelja IKT proizvoda i usluga s poslovnim nastanom na njihovim državnim područjima koje se odnose na izjavu EU-a o sukladnosti, pomagati nacionalnim tijelima za akreditaciju u praćenju i nadzoru aktivnosti tijela za ocjenjivanje sukladnosti tako što će im pružiti stručno znanje i relevantne informacije, ovlastiti tijela za ocjenjivanje sukladnosti za izvršavanje svojih zadaća ako ispunjavaju dodatne zahtjeve iz programa i pratiti relevantne promjene u području kibersigurnosne certifikacije** [...]. Nacionalna tijela za [...] **kibersigurnosnu** certifikaciju trebala bi rješavati pritužbe fizičkih ili pravnih osoba u pogledu certifikata koje su **sama** izdala **ili certifikata koja su izdala tijela za ocjenjivanje sukladnosti koja se odnose na visoku razinu jamstva** [...], u prikladnoj mjeri istražiti predmet pritužbe i u razumnom roku obavijestiti podnositelja pritužbe o napretku i rezultatu istrage. Nadalje, ona bi trebala surađivati s drugim nacionalnim tijelima za [...] **kibersigurnosnu** certifikaciju ili s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj neusklađenosti IKT proizvoda i usluga sa zahtjevima iz ove Uredbe ili s posebnim programima kibersigurnosne certifikacije.

(60) Radi osiguranja dosljedne primjene europskog okvira kibersigurnosne certifikacije trebalo bi osnovati Europsku skupinu za kibersigurnosnu certifikaciju („skupina”) koja se sastoji od **predstavnika** nacionalnih tijela za **kibersigurnosnu** certifikaciju **ili drugih relevantnih nacionalnih tijela**. Glavne bi zadaće skupine trebale biti savjetovanje Komisije i pomoć Komisiji u radu kako bi se osigurala dosljedna provedba i primjena europskog okvira za kibersigurnosnu certifikaciju; pomoć Agenciji i suradnju s njome u izradi prijedloga programa kibersigurnosne certifikacije; preporuka Komisiji da od Agencije zatraži izradu prijedloga europskog programa kibersigurnosne certifikacije; i donošenje mišljenja upućenih **Agenciji o prijedlozima programa** Komisiji o održavanju i preispitivanju postojećih europskih programa kibersigurnosne certifikacije.

(60a) Skupina bi trebala olakšati razmjenu dobre prakse i stručnog znanja između nacionalnih tijela za kibersigurnosnu certifikaciju odgovornih za ovlašćivanje tijela za ocjenjivanje sukladnosti i izdavanje certifikata. Skupina bi trebala podupirati razvoj mehanizma istorazinske ocjene u kontekstu izrade prijedloga programa i njegove provedbe za tijela koja izdaju europske kibersigurnosne certifikate za visoku razinu jamstva. Takvim bi se istorazinskim ocjenama konkretno trebalo ustanoviti imaju li dotična tijela odgovarajuće stručno znanje i obavljaju li svoje zadaće na usklađen način. Rezultati istorazinskih ocjena trebali bi biti javno dostupni. Ta tijela mogu donijeti odgovarajuće mjere za prilagodbu svojih praksi i stručnog znanja.

(61) U cilju podizanja razine osviještenosti i radi lakšeg prihvaćanja budućih programa kibersigurnosti EU-a 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 i usluga.

(61a) Kako bi se dodatno olakšala trgovina i prepoznalo da su lanci opskrbe IKT-a globalni, u skladu s člankom 218. UFEU-a Unija može sklopiti sporazume o uzajamnom priznavanju certifikata izdanih u sklopu programa uspostavljenih u okviru Europskog okvira za kibersigurnosnu certifikaciju. Komisija može, uzimajući u obzir mišljenje ENISA-e i Europske skupine za kibersigurnosnu certifikaciju, preporučiti pokretanje relevantnih pregovora. Svakim programom trebalo bi osigurati posebne uvjete za uzajamno priznavanje s trećim zemljama.

(62) [...]

(63) [...]

(64) Kako bi se osigurali ujednačeni uvjeti za provedbu ove Uredbe, provedbene ovlasti trebalo bi dodijeliti Komisiji u slučajevima predviđenima ovom Uredbom. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011.

(65) Postupak ispitivanja trebao bi se upotrebljavati za donošenje provedbenih akata o europskim programima kibersigurnosne certifikacije za IKT proizvode i usluge; o načinima na koje Agencija provodi [...] **istrage**; te o okolnostima, formatima i postupcima u skladu s kojima nacionalna tijela za [...] **kibersigurnosnu** certifikaciju Komisiji dostavljaju obavijesti o akreditiranim tijelima za ocjenjivanje sukladnosti.

(66) Rad Agencije trebao bi se evaluirati neovisno. Evaluacijom bi trebalo uzeti u obzir ostvaruje li Agencija svoje ciljeve, njezin način rada i relevantnost njezinih zadaća. Evaluacijom bi trebalo procijeniti i učinak, djelotvornost i učinkovitost Europskog okvira za kibersigurnosnu certifikaciju.

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

(68) Budući da države članice ne mogu dostatno ostvariti ciljeve ove Uredbe, nego se oni 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. U skladu s načelom proporcionalnosti, kako je utvrđeno u navedenom članku, ovom Uredbom ne prelaze se okviri onoga što je potrebno za ostvarivanje tog cilja.

DONIJELI SU OVU UREDBU:

GLAVA I.
OPĆE ODREDBE

Članak 1.

Predmet i područje primjene

1. U cilju osiguravanja pravilnog funkcioniranja unutarnjeg tržišta uz istodobno postizanje visoke razine kibersigurnosti, kiberotpornosti i povjerenja u Uniji, ovom Uredbom:

(a) utvrđuju se ciljevi, zadaće i ustrojstveni aspekti ENISA-e, „[...] Agencije **Europske unije za kibersigurnost**”, dalje u tekstu „Agencija”; i

(b) utvrđuje se okvir za uspostavu europskih programa kibersigurnosne certifikacije za potrebe osiguranja prikladne razine kibersigurnosti IKT **postupaka,** proizvoda i usluga u Uniji. Taj okvir primjenjuje se ne dovodeći u pitanje posebne odredbe o dobrovoljnoj ili obveznoj certifikaciji u drugim aktima Unije.

2. **Ovom Uredbom ne dovode se u pitanje nadležnosti država članica u pogledu kibersigurnosti ni, u bilo kojem slučaju, 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” obuhvaća sve aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, njihovih korisnika i osoba na koje utječu;

(2) „mrežni i informacijski sustav” znači sustav u smislu članka 4. točke 1. Direktive (EU) 2016/1148;

(3) „nacionalna strategija za sigurnost mrežnih i informacijskih sustava” znači okvir u smislu članka 4. točke 3. Direktive (EU) 2016/1148;

(4) „operator ključne usluge” znači javni ili privatni subjekt definiran u članku 4. točki 4. Direktive (EU) 2016/1148;

(5) „pružatelj digitalnih usluga” znači svaka pravna osoba koja pruža digitalnu uslugu kako je definirano člankom 4. točkom 6. Direktive (EU) 2016/1148;

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

(7) „rješavanje incidenta” znači svi postupci kako su definirani u članku 4. točki 8. Direktive (EU) 2016/1148;

(8) „kiberprijetnja” znači svaka moguća okolnost ili događaj koji bi mogli **oštetiti, poremetiti ili na drugi način** negativno utjecati na mrežne i informacijske sustave, njihove korisnike i pogođene osobe.

(9) „europski program kibersigurnosne certifikacije” znači sveobuhvatni skup pravila, tehničkih zahtjeva, normi i procedura definiranih na razini Unije koji se primjenjuju na certificiranje **ili ocjenjivanje sukladnosti postupaka,** proizvoda i usluga informacijske i komunikacijske tehnologije (IKT) obuhvaćenih područjem primjene tog konkretnog programa;

(9a) „nacionalni program kibersigurnosne certifikacije” znači sveobuhvatni skup pravila, tehničkih zahtjeva, normi i procedura koja je razvilo i donijelo nacionalno javno tijelo koji se primjenjuju na certifikaciju ili ocjenjivanje sukladnosti IKT postupaka, proizvoda i usluga obuhvaćenih područjem primjene tog konkretnog programa;

(10) „europski kibersigurnosni certifikat” znači dokument [...] kojim se potvrđuje da je IKT **postupak,** proizvod ili usluga [...] **evaluiran u pogledu toga je li skladu sa** specifičnim **sigurnosnim** zahtjevima utvrđenima u europskom programu kibersigurnosne certifikacije;

(11) „IKT proizvod [...]” znači bilo koji element ili skupina elemenata mrežnih i informacijskih sustava;

(11a) „IKT usluga” znači svaka usluga koja se u cijelosti ili uglavnom sastoji od prijenosa, pohranjivanja, preuzimanja ili obrade informacija s pomoću mrežnih i informacijskih sustava;

(11b) „IKT postupak” znači svaki skup aktivnosti koje se provode radi oblikovanja, razvoja, ostvarivanja i održavanja IKT proizvoda ili usluge;

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

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

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

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

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

(16a) „tehnička specifikacija” znači dokument kojim se propisuju tehnički zahtjevi koje IKT postupak, proizvod ili usluga moraju ispunjavati;

(16b) „razina jamstva” znači osnova za povjerenje u to da IKT postupak, proizvod ili usluga zadovoljavaju sigurnosne zahtjeve određenog europskog programa kibersigurnosne certifikacije i navođenje razine na kojoj su evaluirani; razinom sigurnosti ne mjeri se sigurnost samog IKT postupka, proizvoda ili usluge.

GLAVA II.

ENISA – „*[...] Agencija Europske unije za kibersigurnost*”

POGLAVLJE I.

MANDAT I CILJEVI *[...]*

Članak 3.

Mandat

1. Agencija obavlja zadaće koje su joj dodijeljene ovom Uredbom u svrhu doprinosa visokoj razini kibersigurnosti [...] **diljem** Unije, **posebno podupiranjem država članica te institucija, agencija i tijela Unije u poboljšanju kibersigurnosti**. **Agencija djeluje kao referentna točka za pružanje savjeta i stručnog znanja o kibersigurnosti institucijama, agencijama i tijelima Unije.**

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

2.a **U obavljanju svojih zadaća Agencija djeluje neovisno i u najvećoj mogućoj mjeri uzima u obzir stručno znanje relevantnih tijela država članica, izbjegavajući pritom udvostručavanje aktivnosti.**

3. [...]

Članak 4.

Ciljevi

1. Agencija djeluje kao stručni centar za kibersigurnost 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. Agencija pomaže institucijama, agencijama i tijelima Unije te državama članicama u razvoju i provedbi politika **Unije** povezanih s kibersigurnošću**, uključujući sektorske politike o kibersigurnosti**.

3. Agencija podupire jačanje kapaciteta i pripravnosti u cijeloj Uniji na način da **institucijama, agencijama i tijelima** 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. Agencija promiče suradnju i koordinaciju na razini Unije među državama članicama, institucijama, agencijama i tijelima Unije te relevantnim **privatnim i javnim dionicima** [...] u pitanjima povezanima s kibersigurnošću.

5. Agencija **doprinosi povećanju** [...] kibersigurnosne sposobnosti na razini Unije kako bi [...] **pomogla** državama članicama u sprečavanju kiberprijetnji i odgovoru na njih, posebno u slučaju prekograničnih incidenata.

6. Agencija promiče upotrebu certifikacije **kako bi se izbjegla fragmentacija sustavâ certificikacije u EU-u. Agencija osobito doprinosi** [...] uspostavi i održavanju okvira za kibersigurnosnu certifikaciju na razini Unije u skladu s glavom III. ove Uredbe u cilju povećanja transparentnosti kibersigurnosnog jamstva IKT proizvoda i usluga i jačanja povjerenja u jedinstveno digitalno tržište.

7. Agencija promiče visoku razinu osviještenosti građana i poduzeća o pitanjima povezanima s kibersigurnošću.

POGLAVLJE I.A
ZADAĆE

Članak 5.

[...] ***Razvoj i provedba politike i prava Unije***

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

1. pružanjem pomoći i savjeta, osobito svojeg neovisnog mišljenja, i obavljanjem pripremih radnji 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;

2. pružanjem pomoći državama članicama u dosljednoj provedbi politike i prava Unije u području kibersigurnosti, posebno u vezi s Direktivom (EU) 2016/1148, među ostalim i s pomoću mišljenja, smjernica, 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. doprinosom radu Skupine za suradnju u skladu s člankom 11. Direktive (EU) 2016/1148 pružanjem stručnih savjeta i pomoći;

4. podupiranjem:

   (1) razvoja i provedbe politike Unije u području elektroničke identifikacije i usluga povjerenja, posebno pružanjem savjeta i tehničkih smjernica te olakšavanjem razmjene najbolje prakse među nadležnim tijelima;

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

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

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

   (b) obavijesti o povredi sigurnosti i gubitku cjelovitosti u pogledu pružatelja usluga povjerenja koje nadzorna tijela dostavljaju Agenciji u skladu s člankom 19. stavkom 3. Uredbe (EU) 910/2014;

   (c) obavijesti o [...] sigurnosnim **incidentima** koje dostavljaju poduzeća koja pružaju usluge javnih komunikacijskih mreža ili javno dostupne elektroničke komunikacijske usluge, a koje nadležna tijela dostavljaju Agenciji, u skladu s člankom 40. [Direktive o Europskom zakoniku elektroničkih komunikacija].

Članak 6.

[...] ***Izgradnja kapaciteta***

1. Agencija pomaže:

(a) državama članicama u nastojanjima da poboljšaju sprečavanje, otkrivanje i analizu kiber**prijetnji** [...] i kiberincidenata te kapacitet za odgovor na njih osiguravanjem potrebnih znanja i stručnjaka;

(b) institucijama, [...] agencijama **i tijelima** Unije u njihovim nastojanjima da poboljšaju sprečavanje, otkrivanje i analizu kiber**prijetnji** [...] i kiberincidenata [...], **osobito** pružanjem odgovarajuće potpore CERT-u za institucije, agencije i tijela Unije (CERT-EU);

(c) državama članicama, na njihov zahtjev, u razvoju nacionalnih timova za odgovor na računalne sigurnosne incidente (CSIRT-ova) u skladu s člankom 9. stavkom 5. Direktive (EU) 2016/1148;

(d) državama članicama, na njihov zahtjev, u razvoju nacionalnih strategija za sigurnost mrežnih i informacijskih sustava u skladu s člankom 7. stavkom 2. Direktive (EU) 2016/1148; Agencija promiče i širenje tih strategija i [...] **prati** njihovu provedbu diljem Unije u cilju promicanja najbolje prakse;

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

(f) 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;

(g) državama članicama organiziranjem **redovnih** [...] kibersigurnosnih vježbi na razini Unije iz članka 7. stavka 6. i pružanjem preporuka politike na temelju postupka evaluacije vježbi i stečenog iskustva tijekom tih vježbi;

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

(i) Skupini za suradnju razmjenom najbolje prakse među državama članicama, posebno u pogledu identifikacije operatora ključnih usluga, među ostalim u vezi s prekograničnim ovisnostima u pogledu rizika i incidenata, u skladu s člankom 11. stavkom 3. točkom 1. Direktive (EU) 2016/1148.

2. Agencija **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. Agencija podupire operativnu suradnju među **državama članicama, institucijama, agencijama i** [...] tijelima **Unije** te među dionicima.

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

(a) razmjenom znanja i iskustava te najbolje prakse;

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

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

3. Agencija osigurava tajništvo mreže CSIRT-ova u skladu s člankom 12. stavkom 2. Direktive (EU) 2016/1148 i **u tom svojstvu** [...] olakšava razmjenu informacija i suradnju među njezinim članovima.

4. Agencija **podupire** [...] operativnu suradnju unutar mreže CSIRT-ova pružanjem potpore državama članicama **na njihov zahtjev**:

(a) savjetovanjem o tome kako poboljšati sposobnosti za sprječavanje i otkrivanje incidenata te za odgovaranje na njih;

(b) [...] **olakšavanjem** tehničkog **postupanja** u slučaju incidenata sa značajnim ili bitnim učinkom [...], **osobito podupiranjem dobrovoljne razmjene tehničkih rješenja među državama članicama;**

(c) analiziranjem ranjivosti [...] i incidenata**;**

(ca) pružanjem potpore za *ex post* tehničke istrage incidenata sa značajnim ili bitnim učinkom na temelju Direktive (EU) 2016/1148.

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

5. [...]

[...]

6. Agencija organizira **redovne** [...] vježbe u području kibersigurnosti na razini Unije i, na zahtjev, podupire države članice i institucije, agencije i tijela EU-a pri organizaciji takvih vježbi. **Takve vježbe na razini Unije mogu uključivati tehničke, operativne ili strateške elemente** [...]. **Jednom u dvije godine organizira se vježba velikog opsega koja sadrži sve te elemente.** Agencija doprinosi i pomaže u organizaciji, kada je to prikladno, sektorskih kibersigurnosnih vježbi u suradnji s relevantnim [...] **organizacijama koje mogu** sudjelovati i u kibersigurnosnim vježbama na razini Unije.

7. Agencija **u bliskoj suradnji s državama članicama** sastavlja redovito tehničko izvješće o stanju kibersigurnosti u EU-u u pogledu incidenata i prijetnji na temelju informacija iz otvorenih izvora, vlastite analize i izvješća koje dostavljaju, među ostalim: CSIRT-ovi država članica [...] ili jedinstvene kontaktne točke iz Direktive NIS (**u oba slučaja na dobrovoljnoj osnovi** [...]); Europski centar za kiberkriminalitet (EC3) pri Europolu, CERT-EU.

8. Agencija 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 izvješća iz nacionalnih izvora **koja 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 država članica, olakšavanjem** tehničkog postupanja u slučaju incidenta ili krize [...], **osobito** [...] **podupiranjem dobrovoljne** razmjene tehničkih rješenja među državama članicama;

(d) potporom **institucijama, agencijama i tijelima EU-a te, na zahtjev, državama članicama u** javnoj komunikaciji u vezi s incidentom ili krizom;

(e) **potporom državama članicama da na njihov zahtjev** ispitaju [...] planove suradnje za odgovor na takve incidente ili krize.

Članak 8.

*[...] **Tržište, kibersigurnosna certifikacija i normizacija***

Agencija:

(a) podupire i promiče razvoj i provedbu politike Unije o kibersigurnosnoj certifikaciji IKT **postupaka,** proizvoda i usluga, kako je utvrđeno u glavi III. ove Uredbe na sljedeće načine:

(1) izradom prijedloga europskih programa kibersigurnosne certifikacije za IKT **postupke,** proizvode i usluge **u suradnji s industrijom i u** skladu s člankom 44. ove Uredbe;

(2) pomaganjem Komisiji u osiguravanju tajništva Europske skupine za kibersigurnosnu certifikaciju u skladu s člankom 53. ove Uredbe;

(3) sastavljanjem i objavljivanjem smjernica i razvojem dobre prakse u pogledu kibersigurnosnih zahtjeva za IKT proizvode i usluge, u suradnji s nacionalnim tijelima za [...] **kibersigurnosnu** certifikaciju i industrijom;

(3a) preporukom odgovarajućih tehničkih specifikacija za uporabu pri razvoju europskih programa kibersigurnosne certifikacije iz članka 47. stavka 1. točke (b) u slučajevima u kojima norme nisu dostupne;

(3b) doprinosom izgradnji dostatnog kapaciteta u vezi s postupcima evaluacije i certifikacije sastavljanjem i objavljivanjem smjernica te pružanjem potpore državama članicama na njihov zahtjev;

(b) olakšavanjem uspostave i prihvaćanja europskih i međunarodnih normi za upravljanje rizikom i za sigurnost IKT **postupaka,** proizvoda i usluga [...]**;**

(ba) izradom, u suradnji s državama članicama, 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;

(c) provedbom i distribucijom redovitih analiza glavnih trendova na kibersigurnosnom tržištu i na strani ponude i potražnje u cilju poticanja kibersigurnosnog tržišta u Uniji.

Članak 9.

[...] ***Znanje*** **i** [...] ***informiranje*** [...]

Agencija:

(a) provodi analize novih tehnologija i daje tematske procjene očekivanih društvenih, pravnih, gospodarskih i regulatornih učinaka tehnoloških inovacija na kibersigurnost;

(b) provodi dugoročne strateške analize kiberprijetnji i kiberincidenata kako bi utvrdila nove trendove i pomogla spriječiti [...] kibersigurnosne **incidente**;

(c) pruža, u suradnji sa stručnjacima iz tijela država članica, 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) na posebnom portalu objedinjuje, organizira i stavlja na raspolaganje javnosti informacije o kibersigurnosti koje su dostavile institucije, agencije i tijela Unije **te koje su dobrovoljno na raspolaganje stavile države članice i javni i privatni dionici;**

(e) [...]

(f) prikuplja i analizira javno dostupne informacije o značajnim incidentima i sastavlja izvješća u cilju pružanja smjernica poduzećima i građanima u cijeloj Uniji;

(g) [...].

Članak 9.a

Podizanje razine osviještenosti i obrazovanje

Agencija:

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

(b) organizira, u suradnji s državama članicama i institucijama, tijelima i agencijama Unije te industrijom, redovite informativne kampanje u cilju povećanja kibersigurnosti i svoje vidljivosti u Uniji.

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

(d) podupire bližu koordinaciju i razmjenu najboljih praksi među državama članicama u obrazovanju i osviještenosti u području kibersigurnosti olakšavanjem stvaranja i održavanja mreže nacionalnih kontaktnih točaka.

Članak 10.

*[...] **Istraživanja i inovacije***

U pogledu istraživanja i inovacija Agencija obavlja sljedeće zadaće:

(a) savjetuje Uniju i države članice o istraživačkim potrebama i prioritetima u području kibersigurnosti kako bi se omogućili učinkoviti odgovori na postojeće i nove rizike i prijetnje, 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) sudjeluje, ako joj je Komisija delegirala relevantne ovlasti, u fazi provedbe programa za financiranje istraživanja i inovacija ili kao korisnik.

Članak 11.

[...] ***Međunarodna suradnja***

Agencija doprinosi nastojanjima Unije da uspostavi suradnju s trećim zemljama i međunarodnim organizacijama u cilju promicanja međunarodne suradnje u području kibersigurnosti, među ostalim:

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

(b) olakšavanjem, [...] **u relevantnim okvirima međunarodne suradnje**, razmjene najbolje prakse [...];

(c) pružanjem stručnih savjeta Komisiji na njezin zahtjev**;**

(ca) u suradnji s Europskom skupinom za kibersigurnosnu certifikaciju osnovanom na temelju članka 53., pružanjem savjeta i potpore Komisiji o pitanjima koja se odnose na sporazume o uzajamnom priznavanju kibersigurnosnih certifikata s trećim zemljama.

POGLAVLJE II.
ORGANIZACIJA AGENCIJE

Članak 12.

Struktura

Administrativna i upravljačka struktura Agencije sastoji se od sljedećeg:

(a) Upravljačkog odbora koji obavlja funkcije iz članka 14.;

(b) Izvršnog odbora koji obavlja funkcije iz članka 18.;

(c) izvršnog direktora koji obavlja funkcije iz članka 19.;[...]

(d) Stalne interesne skupine koja obavlja funkcije iz članka 20.**;**

(da) Mreže nacionalnih časnika za vezu s funkcijama utvrđenima u članku 20.a.

ODJELJAK 1.
UPRAVLJAČKI ODBOR

Članak 13.

Sastav Upravljačkog odbora

1. Upravljački odbor sastoji se od jednog predstavnika svake države članice i dva predstavnika koje imenuje Komisija. Svi predstavnici imaju pravo glasa.

2. Svaki član Upravljačkog odbora ima zamjenika koji ga predstavlja u slučaju njegove odsutnosti.

3. Članovi Upravljačkog odbora i njihovi zamjenici imenuju se uzimajući u obzir njihovo znanje u području kibersigurnosti i relevantne upravljačke i administrativne vještine i vještine 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 uravnoteženu zastupljenost muškaraca i žena u Upravljačkom odboru.

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

Članak 14.

Funkcije Upravljačkog odbora

1. Upravljački odbor obavlja sljedeće:

(a) definira opći smjer djelovanja Agencije i osigurava da Agencija djeluje u skladu s pravilima i načelima iz ove Uredbe. Osigurava i usklađenost rada Agencije s aktivnostima koje provode države članice i s onima koje se provode na razini Unije;

(b) donosi nacrt jedinstvenog programskog dokumenta Agencije iz članka 21. prije nego što ga podnese Komisiji na mišljenje;

(c) dvotrećinskom većinom glasova svojih članova i u skladu s člankom 17. donosi jedinstveni programski dokument Agencije, uzimajući u obzir mišljenje Komisije;

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

(d) dvotrećinskom većinom glasova svojih članova donosi godišnji proračun Agencije i izvršava ostale funkcije povezane s proračunom Agencije u skladu s poglavljem III.;

(e) ocjenjuje i donosi konsolidirano godišnje izvješće o aktivnostima Agencije i do 1. srpnja sljedeće godine dostavlja izvješće i njegovu ocjenu Europskom parlamentu, Vijeću, Komisiji i Revizorskom sudu. Godišnje izvješće uključuje financijske izvještaje i u njemu se opisuje kako je Agencija ostvarila svoje pokazatelje uspješnosti. Godišnje se izvješće objavljuje;

(f) donosi financijska pravila koja se primjenjuju na Agenciju u skladu s člankom 29.;

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

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

(i) 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;

(j) donosi svoj poslovnik;

(k) u skladu sa stavkom 2., u odnosu na osoblje Agencije izvršava ovlasti koje su Pravilnikom o osoblju za dužnosnike dodijeljene tijelu nadležnom za imenovanja i ovlasti koje su Uvjetima zaposlenja ostalih službenika Unije dodijeljene tijelu ovlaštenom za sklapanje ugovora o radu („ovlasti tijela nadležnog za imenovanja”).

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

(m) imenuje izvršnog direktora i, po potrebi, produžuje njegov mandat ili ga razrješava dužnosti u skladu s člankom 33. ove Uredbe;

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

(o) donosi sve odluke o unutarnjem ustrojstvu Agencije te, prema potrebi, o njegovim izmjenama, uzimajući u obzir potrebe Agencije u pogledu aktivnosti te razumno financijsko upravljanje;

(p) odobrava sklapanje radnih aranžmana u skladu s člancima 7. i 39.

2. Upravljački odbor donosi, u skladu s člankom 110. Pravilnika o osoblju, odluku na temelju članka 2. stavka 1. Pravilnika o osoblju i članka 6. Uvjeta zaposlenja ostalih službenika kojom se ovlasti odgovarajućeg 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.

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

Članak 15.

Predsjednik Upravljačkog odbora

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

Članak 16.

Sastanci Upravljačkog odbora

1. Sastanke Upravljačkog odbora saziva njegov predsjednik.

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

3. Izvršni direktor sudjeluje na sastancima Upravljačkog odbora bez prava glasa.

4. Članovi Stalne interesne skupine mogu na poziv predsjednika sudjelovati na sastancima Upravljačkog odbora, bez prava glasa.

5. Članovima Upravljačkog odbora i njihovim zamjenicima na sastancima mogu, u skladu s njegovim Poslovnikom, pomagati savjetnici ili stručnjaci.

6. Agencija Upravljačkom odboru osigurava tajništvo.

Članak 17.

Pravila o glasovanju Upravljačkog odbora

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

2. Dvotrećinska većina glasova svih članova Upravljačkog odbora potrebna je za jedinstveni programski dokument, godišnji proračun, imenovanje izvršnog direktora te za produljenje njegova mandata ili njegovo razrješenje dužnosti.

3. Svaki član ima jedan glas. U odsutnosti člana ima pravo glasovati njegov zamjenik.

4. Predsjednik 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 ODBOR

Članak 18.

Izvršni odbor

1. Izvršni odbor pomaže Upravljačkom odboru.

2. Izvršni odbor obavlja sljedeće:

   (a) priprema odluke koje donosi Upravljački odbor;

   (b) osigurava, zajedno s Upravljačkim odborom, 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 koje su utvrđene u članku 19., pruža pomoć i savjete izvršnom direktoru u provedbi odluka Upravljačkog odbora o upravnim i proračunskim pitanjima, u skladu s člankom 19.

3. Izvršni odbor sastavljen je od pet članova imenovanih iz redova članova Upravljačkog odbora, uključujući predsjednika Upravljačkog odbora koji može i predsjedati Izvršnim odborom, a jedan od članova predstavnik je Komisije. 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. [...]

ODJELJAK 3.
IZVRŠNI DIREKTOR

Članak 19.

Odgovornosti izvršnog direktora

1. Agencijom 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 Agencijom;

(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 Agencije **uključujući provedbu godišnjeg programa rada** i njegovo dostavljanje Upravljačkom odboru na ocjenjivanje i donošenje;

(f) izradu akcijskog plana na temelju zaključaka naknadnih evaluacija i izvješćivanje Komisije o napretku svake dvije godine;

(g) izradu akcijskog plana na temelju zaključaka iz izvješća o unutarnjoj ili vanjskoj reviziji i istraga Europskog ureda za borbu protiv prijevara (OLAF) i izvješćivanje Komisije o napretku dva puta godišnje te redovito izvješćivanje Upravljačkog odbora;

(h) izradu nacrta financijskih pravila koja se primjenjuju na Agenciju;

(i) izradu nacrta izvješća Agencije o procjeni prihoda i rashoda i izvršenje 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 djelotvornih, razmjernih i odvraćajućih administrativnih i novčanih kazni;

(k) izradu strategije Agencije 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;

(la) redovnu razmjenu informacija s institucijama, agencijama i tijelima Unije u pogledu svojih aktivnosti u području kibersigurnosti kako bi se osigurala usklađenost u razvoju i provedbi politike EU-a;

(m) druge zadaće dodijeljene izvršnom direktoru ovom Uredbom.

4. Prema potrebi i u okviru mandata Agencije te u skladu s ciljevima i zadaćama Agencije, izvršni direktor može osnovati *ad hoc* radne skupine sastavljene od stručnjaka, uključujući stručnjake iz nadležnih tijela država članica. Upravljački odbor mora biti unaprijed obaviješten. 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 Agencije.

5. **Prema potrebi, u svrhu obavljanja zadaća Agencije 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 Agencije te** dobiva prethodnu suglasnost Komisije **i** Upravljačkog odbora[...]. **U slučaju neslaganja tijekom postupka savjetovanja između izvršnog direktora i dotične države članice to se pitanje podnosi Vijeću na raspravu.** U toj se odluci utvrđuje opseg aktivnosti koje treba obavljati taj lokalni ured na način da se izbjegnu nepotrebni troškovi i udvostručavanje administrativnih zadaća Agencije.[...] **Broj osoblja u svim lokalnim uredima svodi se na najmanju moguću mjeru i ne smije prelaziti <u>ukupno</u> 40 % <u>[...]</u> osoblja <u>koje se nalazi u državi članici u kojoj je sjedište Agencije</u>. Broj osoblja u svakom lokalnom uredu ne smije prelaziti 10 % <u>[...]</u>broja <u>[...]</u> osoblja <u>koje se nalazi u državi članici u je nalazi sjedište Agencije</u>.**

ODJELJAK 4.
STALNA INTERESNA SKUPINA

Članak 20.

Stalna interesna skupina

1. Upravljački odbor, djelujući na prijedlog izvršnog direktora, osniva Stalnu interesnu skupinu sastavljenu od priznatih stručnjaka koji zastupaju relevantne interesne skupine, kao što su IKT industrija, pružatelji elektroničkih komunikacijskih mreža ili usluga dostupnih javnosti, **operatori ključnih usluga**, skupine potrošača, akademski stručnjaci za kibersigurnost i predstavnici nadležnih tijela prijavljenih u skladu s [Direktivom o Europskom zakoniku elektroničkih komunikacija] te od tijela za izvršavanje zakonodavstva i tijela za nadzor zaštite podataka.

2. Postupci koji se odnose na Stalnu interesnu skupinu, posebno u pogledu broja, sastava i imenovanja njezinih članova od strane Upravljačkog odbora, prijedlog izvršnog direktora i rad Skupine utvrđuju se u unutarnjem pravilniku o radu Agencije te se objavljuju.

3. Stalnom interesnom skupinom predsjeda izvršni direktor ili bilo koja osoba koju, zasebno za svaki slučaj, imenuje izvršni direktor.

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

5. Stalna interesna skupina savjetuje Agenciju u vezi s obavljanjem njezinih aktivnosti. Ona posebno savjetuje izvršnog direktora u vezi s izradom prijedloga programa rada Agencije i osiguravanjem komunikacije s relevantnim interesnim skupinama o svim pitanjima koja se odnose na program rada.

5.a Stalna interesna skupina redovito obavještava Upravljački odbor o svojim aktivnostima.

ODJELJAK 4.A
MREŽA NACIONALNIH ČASNIKA ZA VEZU

Članak 20.a

Mreža nacionalnih časnika za vezu

1. Upravljački odbor, odlučujući na prijedlog izvršnog direktora, uspostavlja mrežu nacionalnih časnika za vezu sastavljenu od predstavnika država članica.

2. Mreža nacionalnih časnika za vezu sastoji se od predstavnika svih država članica. Svaka država članica imenuje jednog predstavnika; Sastanci mreže mogu se održavati u različitim sastavima stručnjaka.

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

4. Nacionalni časnici za vezu djeluju kao središnje kontaktne točke na nacionalnoj razini kako bi se olakšala suradnja između ENISA-e i nacionalnih stručnjaka u kontekstu provedbe programa rada ENISA-e.

5. Iako bi nacionalni časnici za vezu trebali usko surađivati s predstavnicima svojih zemalja u Upravljačkom odboru, radom same mreže ne udvostručuje se rad Upravljačkog odbora ni drugih foruma EU-a.

6. Funkcije i postupci za mrežu nacionalnih časnika za vezu utvrđuju se u unutarnjem pravilniku o radu Agencije i objavljuju.

ODJELJAK 5.
DJELOVANJE

Članak 21.

Jedinstveni programski dokument

1. Agencija obavlja poslove u skladu s jedinstvenim programskim dokumentom koji sadržava njezine višegodišnje i godišnje programe koji uključuju sve njezine planirane aktivnosti.

2. Izvršni direktor svake godine izrađuje nacrt jedinstvenog programskog dokumenta koji sadržava višegodišnje i godišnje programe s odgovarajućim planovima u pogledu ljudskih i financijskih resursa u skladu s člankom 32. Delegirane uredbe Komisije (EU) br. 1271/2013[14] i uzimajući u obzir smjernice koje je utvrdila Komisija.

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

4. Jedinstveni programski dokument postaje konačan nakon konačnog donošenja općeg proračuna Unije te se, prema potrebi, u skladu s time prilagođava.

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.

[14] 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.).

6. Upravljački odbor mijenja doneseni godišnji program rada ako Agencija dobije novi zadaću. Svaka znatna izmjena godišnjeg programa rada donosi 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 56.

Članak 22.

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 moraju biti 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. Agencija u svojem unutarnjem pravilniku o radu utvrđuje praktična rješenja za pravila o izjavama o interesima iz stavaka 1. i 2.

Članak 23

Transparentnost

1. Agencija obavlja svoje aktivnosti uz visok stupanj transparentnosti i u skladu s člankom 25.

2. Agencija osigurava da javnost i sve zainteresirane strane dobiju odgovarajuće, objektivne, pouzdane i lako dostupne informacije, posebno u pogledu rezultata njezina rada. Agencija objavljuje i izjave o interesima dane u skladu s člankom 22.

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

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

Članak 24.

Povjerljivost

1. Ne dovodeći u pitanje članak 25., Agencija trećim stranama ne otkriva informacije koje obrađuje ili prima, a za koje je podnesen opravdan zahtjev da s njima djelomično ili u cijelosti postupa kao s povjerljivim informacijama.

2. Članovi Upravljačkog odbora, izvršni direktor, članovi Stalne interesne skupine, vanjski stručnjaci koji sudjeluju u radu ad hoc radnih skupina i članovi osoblja Agencije, uključujući službenike koje privremeno upućuju države članice, poštuju zahtjeve u pogledu povjerljivosti iz članka 339. Ugovora o funkcioniranju Europske unije (UFEU) čak i nakon prestanka njihovih dužnosti.

3. Agencija 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 Agencije, Upravljački odbor donosi odluku kojom Agenciji dopušta obradu klasificiranih podataka. U tom slučaju Upravljački odbor, u dogovoru sa službama Komisije, donosi unutarnji pravilnik o radu primjenjujući načela sigurnosti utvrđena odlukama Komisije (EU, Euratom) 2015/443[15] i 2015/444[16]. Ta pravila uključuju odredbe o razmjeni, obradi i pohrani klasificiranih podataka.

---

[15] Odluka Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji (SL L 72, 17.3.2015., str. 41.).

[16] 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.).

Članak 25.

Pristup dokumentima

1. Uredba (EZ) br. 1049/2001 primjenjuje se na dokumente u posjedu Agencije.

2. Upravljački odbor donosi pravila za provedbu Uredbe (EZ) br. 1049/2001 u roku od šest mjeseci od osnivanja Agencije.

3. Odluke koje Agencija 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 III.
DONOŠENJE I STRUKTURA PRORAČUNA

Članak 26.

Donošenje proračuna

1. Izvršni direktor svake godine izrađuje nacrt izvješća o procjenama prihoda i rashoda Agencije 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 prihoda i rashoda iz stavka 1., sastavlja izvješće o procjenama prihoda i rashoda Agencije 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 39. šalje izvješće o procjenama iz stavka 2., 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 unosi u nacrt proračuna Unije, koji podnosi Europskom parlamentu i Vijeću u skladu s člancima 313. i 314. UFEU-a.

5. Europski parlament i Vijeće odobravaju dodjelu sredstava za doprinos Agenciji.

6. Europski parlament i Vijeće donose plan radnih mjesta Agencije.

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

Članak 27.

Struktura proračuna

1. Ne dovodeći u pitanje druge izvore, prihodi Agencije uključuju sljedeće:

   (a) doprinos iz proračuna Unije;

   (b) namjenske prihode za određene stavke rashoda u skladu s financijskim pravilima iz članka 29.;

   (c) financijska sredstva Unije u obliku sporazuma o delegiranju ili ad hoc bespovratnih sredstava u skladu s njezinim financijskim pravilima iz članka 29. i u skladu s odredbama relevantnih instrumenata kojima se podupiru politike Unije;

(d) doprinose trećih zemalja koje sudjeluju u radu Agencije kako je predviđeno u članku 39.;

(e) sve dobrovoljne doprinose država članica u novcu ili naravi; Države članice koje daju dobrovoljne doprinose ne mogu na temelju toga zahtijevati nikakva posebna prava ili usluge.

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

Članak 28.

Izvršenje proračuna

1. Izvršni direktor odgovoran je za izvršenje proračuna Agencije.

2. Unutarnji revizor Komisije ima iste ovlasti u odnosu na Agenciju, kao i u odnosu na službe Komisije.

3. Računovodstveni službenik Agencije dostavlja privremeni financijski izvještaj računovodstvenom službeniku Komisije i Revizorskom sudu do 1. ožujka sljedeće financijske godine (1. ožujka godine N + 1).

4. Računovodstveni službenik Agencije po primitku opažanja Revizorskog suda o privremenom financijskom izvještaju Agencije izrađuje završni izvještaj Agencije pod vlastitom odgovornošću.

5. Izvršni direktor podnosi završni financijski izvještaj Upravljačkom odboru na mišljenje.

6. Izvršni direktor do 31. ožujka godine N + 1 podnosi izvješće o proračunskom i financijskom upravljanju Europskom parlamentu, Vijeću, Komisiji i Revizorskom sudu.

7. Računovodstveni službenik podnosi završni financijski izvještaj, zajedno s mišljenjem Upravljačkog odbora, Europskom parlamentu, Vijeću, računovodstvenom službeniku Komisije i Revizorskom sudu. do 1. srpnja godine N + 1.

8. Na datum podnošenja završnog financijskog izvještaja računovodstveni službenik Revizorskom sudu šalje i izjavu povezanu s tim završnim financijskim izvještajem, a presliku šalje i računovodstvenom službeniku Komisije.

9. Izvršni direktor objavljuje završni financijski izvještaj do 15. studenoga sljedeće godine.

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

11. Izvršni direktor dostavlja Europskom parlamentu, na njegov zahtjev, sve informacije potrebne za nesmetanu provedbu postupka davanja razrješnice za predmetnu financijsku godinu, kako je utvrđeno u članku 165. stavku 3. Financijske uredbe.

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

Članak 29.

Financijska pravila

Financijska pravila koja se primjenjuju na Agenciju donosi Upravljački odbor nakon savjetovanja s Komisijom. Ona ne odstupaju od Uredbe (EU) 1271/2013, osim ako je to odstupanje posebno potrebno za rad Agencije i ako je Komisija prethodno dala suglasnost.

Članak 30.

Borba protiv prijevara

1. Kako bi se olakšalo suzbijanje prijevara, korupcije i drugih nezakonitih aktivnosti u skladu s Uredbom (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća[17], Agencija u roku od šest mjeseci od početka svojeg rada pristupa Međuinstitucionalnom sporazumu od 25. svibnja 1999. u vezi s internim istragama koje provodi Europski ured za borbu protiv prijevara (OLAF) i donosi odgovarajuće odredbe primjenljive na sve zaposlenike Agencije, koristeći se obrascem utvrđenim u prilogu tom Sporazumu.

2. Revizorski sud ovlašten je za provedbu revizije, na temelju dokumenata i na terenu, svih korisnika bespovratnih sredstava, ugovaratelja i podugovaratelja koji su primili sredstva Unije od Agencije.

[17] 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.).

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 Europskog parlamenta i Vijeća i Uredbom Vijeća (Euratom, EZ) br. 2185/96[18] 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 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 Agencija.

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 Agencije 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.

POGLAVLJE IV.
OSOBLJE AGENCIJE

Članak 31.

Opće odredbe

Na osoblje Agencije primjenjuju se Pravilnik o osoblju i Uvjeti zaposlenja ostalih službenika te pravila koja su radi primjene tog Pravilnika o osoblju institucije Unije donijele na temelju zajedničkog dogovora.

[18] 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.).

Članak 32.

Povlastice i imuniteti

Na Agenciju i njezino osoblje primjenjuje se Protokol br. 7 o povlasticama i imunitetima Europske unije koji je priložen Ugovoru o Europskoj uniji i UFEU-u.

Članak 33.

Izvršni direktor

1. Izvršni direktor zapošljava se kao privremeni djelatnik Agencije 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. Agenciju pri sklapanju ugovora s izvršnim direktorom zastupa predsjednik Upravljačkog odbora.

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

5. Mandat izvršnog direktora traje **četiri** [...] godine. Do kraja tog razdoblja Komisija provodi procjenu u kojoj se uzimaju u obzir evaluacija uspješnosti izvršnog direktora te budući izazovi i zadaće Agencije.

6. Upravljački odbor donosi odluku o imenovanju, produljenju mandata ili razrješenju dužnosti izvršnog direktora dvotrećinskom većinom glasova svojih članova s glasačkim pravima.

7. Upravljački odbor na prijedlog Komisije, kojim se uzima u obzir procjena iz stavka 5., može jedanput produljiti mandat izvršnog direktora za razdoblje od najdulje **četiri** [...] godine.

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

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

10. Izvršnog se direktora može razriješiti dužnosti odlukom Upravljačkog odbora[...].

Članak 34.

Upućeni nacionalni stručnjaci i ostalo osoblje

1. Agencija može angažirati upućene nacionalne stručnjake i drugo osoblje koje nije zaposleno u Agenciji. Na to se osoblje ne primjenjuju Pravilnik o osoblju i Uvjeti zaposlenja ostalih službenika.

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

POGLAVLJE V.
OPĆE ODREDBE

Članak 35.

Pravni status Agencije

1. Agencija je tijelo Unije i ima pravnu osobnost.

2. Agencija u svakoj državi članici ima najširu pravnu sposobnost koja se pravnim osobama priznaje nacionalnim zakonodavstvom. Konkretno, može stjecati pokretnine i nekretnine ili njima raspolagati te biti stranka u sudskom postupku[...].

3. Agenciju zastupa njezin izvršni direktor.

Članak 36.

Odgovornost Agencije

1. Ugovorna odgovornost Agencije 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 Agencija.

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

4. Sud Europske unije nadležan je za sve sporove povezane s nadoknadom takve štete.

5. Osobna odgovornost službenika prema Agenciji podliježe odgovarajućim uvjetima koji se primjenjuju na osoblje.

Članak 37.

Pravila o jezicima

1. Na Agenciju[19] se primjenjuje Uredba Vijeća br. 1. Države članice i druga tijela koja su imenovale države članice mogu se obratiti Agenciji i dobiti odgovor na službenom jeziku institucija Unije po svojem izboru.

2. Prevoditeljske usluge potrebne za funkcioniranje Agencije pruža Prevoditeljski centar za tijela Europske unije.

Članak 38.

Zaštita osobnih podataka

1. Obrada osobnih podataka od strane Agencije podliježe Uredbi (EZ) br. 45/2001 Europskog parlamenta i Vijeća[20].

2. Upravljački odbor donosi provedbene mjere iz članka 24. stavka 8. Uredbe (EZ) br. 45/2001. Upravljački odbor može donijeti dodatne mjere koje su potrebne kako bi Agencija primjenjivala Uredbu (EZ) br. 45/2001.

---

[19] Uredba br. 1 o utvrđivanju jezika koji se koriste u Europskoj zajednici za atomsku energiju (SL 17, 6.10.1958., str. 401.).

[20] Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12.1.2001., str. 1.).

Članak 39.

Suradnja s trećim zemljama i međunarodnim organizacijama

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

2. Agencija je otvorena za sudjelovanje trećih zemalja koje su u tu svrhu s Unijom sklopile sporazume. U skladu s relevantnim odredbama tih sporazuma utvrđuju se aranžmani kojima se posebno određuju priroda, opseg i način sudjelovanja tih zemalja u radu Agencije, uključujući odredbe koje se odnose na sudjelovanje u inicijativama koje poduzima Agencija, financijske doprinose i osoblje. Aranžmani koji se odnose na osoblje u svakom slučaju moraju biti u skladu s Pravilnikom o osoblju.

3. Upravljački odbor donosi strategiju za odnose s trećim zemljama ili međunarodnim organizacijama u pogledu pitanja za koja je Agencija nadležna. Komisija osigurava da Agencija djeluje u okviru svojeg mandata i postojećeg institucionalnog okvira sklapanjem odgovarajućeg radnog aranžmana s izvršnim direktorom Agencije.

Članak 40.

Sigurnosna pravila za zaštitu klasificiranih i osjetljivih neklasificiranih podataka

Agencija u dogovoru s Komisijom donosi svoja sigurnosna pravila primjenjujući sigurnosna načela iz sigurnosnih pravila Komisije za zaštitu klasificiranih podataka Europske unije (EUCI) i osjetljivih neklasificiranih podataka, kako je utvrđeno u odlukama Komisije (EU, Euratom) 2015/443 i 2015/444. Navedeno obuhvaća, među ostalim, odredbe o razmjeni, obradi i pohrani takvih podataka.

Članak 41.

Sporazum o sjedištu i uvjeti rada

1. Potrebni dogovori o smještaju Agencije 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 Agencije i članove njihovih obitelji utvrđuju se Sporazumom o sjedištu između Agencije i države članice u kojoj se sjedište nalazi, koji se sklapa nakon dobivanja odobrenja Upravljačkog odbora i najkasnije u roku od [2 godine od stupanja na snagu ove Uredbe].

2. Država članica domaćin Agencije osigurava [...] uvjete za osiguravanje pravilnog funkcioniranja Agencije, uključujući dostupnost lokacije, postojanje odgovarajućih obrazovnih objekata za djecu članova osoblja, odgovarajući pristup tržištu rada, socijalno osiguranje i zdravstvenu zaštitu za djecu i supružnike.

Članak 42

Upravna kontrola

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

GLAVA III.
OKVIR ZA KIBERSIGURNOSNU CERTIFIKACIJU

Članak 14.

Europski* okvir *za kibersigurnosnu certifikaciju[...]

1. **Europski okvir za kibersigurnosnu certifikaciju uspostavlja se u cilju poboljšanja uvjeta za funkcioniranje unutarnjeg tržišta povećanjem razine kibersigurnosti unutar Unije. Okvirom se utvrđuje upravljanje koje omogućuje usklađen pristup na razini EU-a u pogledu europskih programa kibersigurnosne certifikacije s ciljem stvaranja jedinstvenog digitalnog tržišta za IKT postupke, proizvode i usluge.**

2. **Europskim okvirom za kibersigurnosnu certifikaciju utvrđuje se mehanizam za uspostavu** [...] europskih programa kibersigurnosne certifikacije [...] **i** potvrđivanje toga da IKT **postupci**, proizvodi i usluge koji su [...] **evaluirani** u skladu s takvim programom ispunjavaju utvrđene **sigurnosne** zahtjeve [...] **u cilju zaštite** dostupnosti, izvornosti, cjelovitosti i povjerljivosti pohranjenih, poslanih ili obrađenih podataka ili funkcija ili usluga koje se nude s pomoću tih proizvoda, postupaka **i** usluga ili kojima se s pomoću njih može pristupiti [...] **tijekom njihovog cijelog životnog ciklusa**.

Članak 44.

Izrada i donošenje europskog programa kibersigurnosne certifikacije

1. Na temelju zahtjeva Komisije **ili Europske skupine za kibersigurnosnu certifikaciju („Skupina”) uspostavljene člankom 53.** ENISA izrađuje prijedlog europskog programa kibersigurnosne certifikacije koji je u skladu sa zahtjevima iz članaka 45., 46. i 47. ove Uredbe.[...]

1.a Države članice ili zainteresirane organizacije dionika mogu Skupini uputiti zahtjev za izradu prijedloga europskog programa kibersigurnosne certifikacije. Skupina ocjenjuje takav zahtjev prema kriterijima koje je odredila s pomoću smjernica u skladu s člankom 53. stavkom 3. točkom (ca) i može od ENISA-e zatražiti da izradi prijedlog europskog programa kibersigurnosne certifikacije.

2. Pri izradi prijedloga programa iz stavka 1. ovog članka ENISA se savjetuje sa svim relevantnim dionicima **s pomoću transparentnih postupaka savjetovanja** i blisko surađuje sa Skupinom. Skupina ENISA-i pruža pomoć i stručne savjete [...] u vezi s izradom prijedloga programa **i, prije nego što ga podnese Komisiji, donosi mišljenje o prijedlogu programa** [...]**. ENISA osigurava da je prijedlog programa u skladu s primjenjivom usklađenom normom koja se upotrebljava za akreditaciju tijela za ocjenjivanje sukladnosti.**

3. ENISA **u najvećoj mogućoj mjeri uzima u obzir mišljenje Skupine prije nego što Komisiji podnese** [...] prijedlog programa izrađen u skladu sa stavkom 2. ovog članka.

4. Komisija, na temelju prijedloga programa koji je izradila ENISA, može u skladu s člankom 55. stavkom 2. donositi provedbene akte kojima se predviđaju europski programi kibersigurnosne certifikacije za IKT **postupke**, proizvode i usluge koji ispunjavaju zahtjeve iz članaka 45., 46. i 47. ove Uredbe.

5. [...]

Članak 44.a

Održavanje europskog programa kibersigurnosne certifikacije

1. Agencija održava namjenske internetske stranice na kojima pruža informacije o europskim programima kibersigurnosne certifikacije, certifikatima i izjavama EU-a o sukladnosti izdanima u skladu s člankom 47.a i daje im vidljivost.

2. Agencija, u bliskoj suradnji sa Skupinom, najmanje svakih pet godina preispituje donesene programe kibersigurnosne certifikacije uzimajući u obzir povratne informacije primljene od zainteresiranih strana. Prema potrebi, Komisija ili Skupina mogu od Agencije zatražiti da pokrene postupak izrade revidiranog prijedloga programa u skladu s člankom 44. stavcima 2. i 3.

Članak 45.

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 postupka, proizvoda ili usluge**;

(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 postupka, proizvoda ili usluge;**

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

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

(e) [...] moguće je 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;

(f) pravodobno osigurati ponovnu dostupnost podataka i pristup podacima, uslugama i funkcijama u slučaju fizičkog ili tehničkog incidenta;

(g) [...] IKT **postupci**, proizvodi i usluge imaju osiguran ažuriran softver **i hardver** koji [...] ne sadrže **javno** poznate ranjivosti te imaju osigurane mehanizme za sigurno ažuriranje [...];

(ga) IKT postupci, proizvodi i usluge, osmišljavaju se, proizvode i dostavljaju u skladu sa sigurnosnim zahtjevima navedenim u pojedinom programu.

Članak 46.

Razine jamstva europskih programa kibersigurnosne certifikacije

1. Europskim programom kibersigurnosne certifikacije može se za IKT **postupke**, proizvode i usluge[...] utvrditi jedna od sljedećih razina jamstva ili više njih: osnovna, znatna i/ ili visoka. **Razina jamstva razmjerna je stoga razini rizika povezanog s predviđenom uporabom IKT postupka, proizvoda ili usluge.**

2. Osnovna, znatna i visoka razina jamstva odnose se [...]**na certifikat ili izjavu EU-a o sukladnosti izdane u kontekstu europskog programa kibersigurnosne certifikacije kojim se za svaku razinu jamstva predviđaju odgovarajući sigurnosni zahtjevi uključujući sigurnosne funkcionalnosti i odgovarajuću razinu napora za evaluaciju IKT postupka, proizvoda ili usluge**. **Certifikat ili izjava EU-a o sukladnosti sadrži upućivanje na odgovarajuće tehničke specifikacije, norme i procedure, uključujući tehničke kontrole, čija je svrha smanjiti rizik od incidenata u području kibersigurnosti ili ih spriječiti, kako slijedi:**

(a) e**uropskim kibersigurnosnim certifikatom ili izjavom o sukladnosti EU-a koji se odnosi na** razinu jamstva „osnovna” **pruža se jamstvo da IKT postupci, proizvodi i usluge ispunjavaju odgovarajuće sigurnosne zahtjeve uključujući sigurnosne funkcije te je evaluacijom utvrđeno da su na razini na kojoj se nastoje maksimalno smanjiti poznati osnovni rizici za kiberincidente i kibernapade. Aktivnosti evaluacije obuhvaćaju barem preispitivanje tehničke dokumentacije, ili ako to nije primjenjivo, zamjenske aktivnosti istovrsnog učinka[...];**

(b) **Europskim kibersigurnosnim certifikatom s koji se odnosi na** razinu jamstva **„**znatna**”** **pruža se jamstvo da IKT postupci, proizvodi i usluge ispunjavaju odgovarajuće sigurnosne zahtjeve uključujući sigurnosne funkcije te je evaluacijom utvrđeno da su na razini na kojoj se nastoje maksimalno smanjiti poznati kiberrizici, kiberincidenti i kibernapadi koje provode subjekti ograničenih vještina i resursa. Aktivnosti evaluacije obuhvaćaju barem: preispitivanje neprimjenjivosti javno poznatih ranjivosti i testiranje toga primjenjuju li IKT postupci, proizvodi ili usluge potrebnu sigurnosnu funkciju na ispravan način; ili ako to nije primjenjivo, obuhvaćaju zamjenske aktivnosti istovrsnog učinka[...];**

(c) **Europskim kibersigurnosnim certifikatom koji se odnosi na** razinu jamstva **„**visoka**”** **pruža se jamstvo da IKT postupci, proizvodi i usluge ispunjavaju odgovarajuće sigurnosne zahtjeve uključujući sigurnosne funkcije te je evaluacijom utvrđeno da su na razini na kojoj se nastoje maksimalno smanjiti rizik najsuvremenijih kibernapada koje provode subjekti znatnih vještina i resursa. Aktivnosti evaluacije obuhvaćaju najmanje: preispitivanje neprimjenjivosti javno poznatih ranjivosti, testiranje toga primjenjuju li IKT postupci, proizvodi ili usluge potrebnu sigurnosnu funkciju na ispravan način na najsuvremenijoj razini i procjenu njihove otpornosti na napad vještih napadača s pomoću penetracijskog testiranja; ili ako to nije primjenjivo, obuhvaćaju zamjenske aktivnosti istovrsnog učinka [...];**

2.a U okviru europskog programa kibersigurnosne certifikacije može se utvrditi nekoliko razina evaluacije ovisno o strogoći i opsežnosti metodologije evaluacije. Svaka razina evaluacije odgovara jednoj od razina jamstva i definira se odgovarajućom kombinacijom komponenata jamstva.

Članak 47.

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 **postupaka**, proizvoda i usluga, **kao i obrazloženje o načinu na koji program certifikacije odgovara potrebama očekivanih ciljnih skupina**;

(b) [...]upućivanje na [...] međunarodne, **europske ili nacionalne norme u skladu s kojima se provodi evaluacija. Ako norme nisu dostupne, upućuje se na** [...] tehničke specifikacije **koje ispunjavaju zahtjeve iz Priloga II. Uredbi 1025/2012 ili, ako nisu dostupne, tehničke specifikacije ili druge kibersigurnosne zahtjeve utvrđene u programu;**

(c) jednu ili više razina jamstva, ako je primjenjivo;

(ca) ako je primjenjivo, posebne ili dodatne zahtjeve koji se primjenjuju na tijela za ocjenjivanje sukladnosti s ciljem jamčenja njihove tehničke stručnosti za evaluaciju kibersigurnosnih zahtjeva;

(d) posebne kriterije i metode evaluacije, uključujući vrste evaluacije, koji se upotrebljavaju za dokazivanje da su ostvareni posebni ciljevi iz članka 45.;

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

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

(g) [...]pravila za praćenje sukladnosti sa zahtjevima iz certifikata, i**li izjave EU-a o sukladnosti**, uključujući mehanizme za dokazivanje trajne sukladnosti s navedenim kibersigurnosnim zahtjevima;

(h) **ako je primjenjivo**, uvjete za izdavanje **i obnavljanje certifikata**, **kao i za** održavanje, nastavak, produljenje **ili** smanjenje njegova opsega;

(i) pravila u vezi s posljedicama nesukladnosti certificiranih proizvoda **ili samoocijenjenih** IKT proizvoda i usluga [...] sa zahtjevima **programa**;

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

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

(l) utvrđivanje nacionalnih ili **međunarodnih** programa kibersigurnosne certifikacije koji obuhvaćaju iste vrste ili kategorije IKT **postupaka**, proizvoda i usluga, **sigurnosne zahtjeve te kriterije i metode evaluacije;**

(m) sadržaj izdanog certifikata **ili izjave EU-a o sukladnosti;**

(ma) razdoblje u kojem proizvođač ili pružatelj IKT proizvoda i usluga mora čuvati izjavu EU-a o sukladnosti i tehničku dokumentaciju sa svim relevantnim informacijama;

(mb[...]) maksimalno razdoblje valjanosti certifikata;

(mc[...]) politiku objavljivanja u vezi s dodijeljenim, izmijenjenim i povučenim certifikatima;

(md[...]) uvjete za uzajamno priznavanje programa certifikacije s trećim zemljama;

(me[...]) ako je primjenjivo, pravila koja se odnose na mehanizam istorazinske ocjene za tijela koja izdaju europske kibersigurnosne certifikate za visoku razinu jamstva[...] u skladu s člankom 48. stavkom 4.a.

2. Navedeni zahtjevi programa nisu u suprotnosti s primjenjivim pravnim zahtjevima, posebno zahtjevima koji proizlaze iz usklađenog zakonodavstva Unije.

3. Ako je tako predviđeno posebnim aktom Unije, certifikacija **ili izjava EU-a o sukladnosti** u okviru europskog programa kibersigurnosne certifikacije može se upotrijebiti za dokazivanje pretpostavke sukladnosti sa zahtjevima tog akta.

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

Članak 47.a

Samoocjenjivanje sukladnosti

1. Europskim programom kibersigurnosne certifikacije može se omogućiti da se ocjenjivanje sukladnosti provodi pod isključivom odgovornošću proizvođača ili pružatelja IKT proizvoda i usluga. Takvo ocjenjivanje sukladnosti primjenjuje se samo na IKT proizvode i usluge niskog rizika koji odgovaraju osnovnoj razini jamstva.

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

3. Proizvođač ili pružatelj IKT proizvoda i usluga trebao bi čuvati izjavu EU-a o sukladnosti i tehničku dokumentaciju o svim relevantnim informacijama o sukladnosti IKT proizvoda ili usluga s programom i staviti je na raspolaganje nacionalnom tijelu za kibersigurnosnu certifikaciju iz članka 50. stavka 1. u razdoblju utvrđenom u odgovarajućem europskom programu kibersigurnosne certifikacije. Primjerak izjave EU-a o sukladnosti podnosi se nacionalnom tijelu za kibersigurnosnu certifikaciju i ENISA-i.

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

5. Izjava EU-a o sukladnosti izdana u skladu s ovim člankom priznaje se u svim državama članicama.

Članak 48.

Kibersigurnosna certifikacija

1. Smatra se da su IKT **postupci**, proizvodi i usluge koji su certificirani u okviru europskog programa kibersigurnosne certifikacije donesenog u skladu s člankom 44. sukladni sa zahtjevima tog programa.

2. Certificiranje je dobrovoljno, osim ako je drugačije navedeno u pravu Unije **ili u pravu država članica.**

3. Europski certifikat o kibersigurnosti u skladu s ovim člankom, **koji se odnosi na razinu jamstva osnovna ili znatna**, izdaju tijela za ocjenjivanje sukladnosti iz članka 51. na temelju kriterija uključenih u europski program kibersigurnosne certifikacije donesen u skladu s člankom 44.

4. [...] Odstupajući od stavka 3. u opravdanim se slučajevima u pojedinom europskom programu kibersigurnosne **certifikacije** može predvidjeti da europski kibersigurnosni certifikat koji proizlazi iz tog programa može izdati samo javno tijelo. To [...] tijelo može biti:

(a) nacionalno tijelo za [...] **kibersigurnosnu** certifikaciju iz članka 50. stavka 1.;

(b) **javno** tijelo koje je akreditirano kao tijelo za ocjenjivanje sukladnosti u skladu s člankom 51. stavkom 1. [...]

(c) [...].

4.a U slučajevima u kojima [...] europski program kibersigurnosne certifikacije u skladu s člankom 44. zahtijeva visoku razinu jamstva, certifikat može izdati samo nacionalno tijelo za kibersigurnosnu certifikaciju iz članka 50. stavka 1. ili, pod sljedećim uvjetima, tijelo za ocjenjivanje sukladnosti iz članka 51.:

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

(b) na temelju prethodnog općeg delegiranja te zadaće tijelu za ocjenjivanje sukladnosti od strane nacionalnog tijela za kibersigurnosnu certifikaciju.

5. Fizička ili pravna osoba koja podnese svoje IKT **postupke**, proizvode ili usluge programu certificiranja [...] **stavlja na raspolaganje** tijelu za ocjenjivanje sukladnosti iz članka 51. **ili nacionalnom tijelu za kibersigurnosnu certifikaciju iz članka 50**., ako je to nadležno tijelo ono koje izdaje certifikat, [...] sve informacije nužne za vođenje procedure certifikacije.

5.a Nositelj certifikata obavješćuje tijelo koje izdaje certifikat o svim kasnijim otkrivenim ranjivostima ili nepravilnostima koje se odnose na sigurnost certificiranog IKT postupka, proizvoda ili usluge koje mogu imati učinak na zahtjeve u vezi s certifikacijom. Tijelo bez nepotrebne odgode prosljeđuje te informacije nacionalnom tijelu za kibersigurnosnu certifikaciju.

6. Certifikati se izdaju na [...] **razdoblje utvrđeno pojedinim programom certifikacije** te se mogu obnoviti [...] pod uvjetom da su i dalje ispunjeni relevantni zahtjevi.

7. Europski certifikat o kibersigurnosti izdan u skladu s ovim člankom priznaje se u svim državama članicama.

Članak 49.

Nacionalni programi kibersigurnosne certifikacije i certifikati

1. Ne dovodeći u pitanje stavak 3., nacionalni programi kibersigurnosne certifikacije i povezane procedure za IKT **postupke**, proizvode i usluge obuhvaćene europskim programom kibersigurnosne certifikacije prestaju proizvoditi učinke od datuma utvrđenog u provedbenom aktu donesenom u skladu s člankom 44. stavkom 4. **N**acionalni programi kibersigurnosne certifikacije i povezani postupci za IKT **postupke**, proizvode i usluge koji nisu obuhvaćeni europskim programom kibersigurnosne certifikacije i dalje postoje.

2. Države članice ne uvode nove nacionalne programe kibersigurnosne certifikacije IKT **postupaka**, proizvoda i usluga obuhvaćenih europskim programom kibersigurnosne certifikacije koji je na snazi.

3. Postojeći certifikati izdani u okviru nacionalnih programa kibersigurnosne certifikacije **i obuhvaćeni europskim programom kibersigurnosne certifikacije** ostaju na snazi do svojeg datuma isteka.

Članak 50.

Nacionalna tijela za* kibersigurnosnu *[...] certifikaciju

1. Svaka država članica **imenuje [...] jedno ili više** nacionalnih **tijela za** [...] **kibersigurnosnu** certifikaciju **na svom državnom području ili, prema uzajamnom dogovoru s drugom državom članicom, određuje da jedno ili više tijela 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 identitetu **imenovanih tijela [...] i o zadaćama koje su im dodijeljene.**

3. **Ne dovodeći u pitanje članak 48. stavak 4. točku (a) i članak 48. stavak 4.a,** [...] svako nacionalno tijelo za [...] **kibersigurnosnu** certifikaciju neovisno je od subjekata koje nadzire u pogledu svojeg ustrojstva, odluka o financiranju, pravne strukture i odlučivanja.

3.a Države članice osiguravaju da se aktivnostima nacionalnih tijela za kibersigurnosnu certifikaciju u vezi s izdavanjem certifikata u skladu s člankom 48. stavkom 4. točkom (a) i člankom 48. stavkom 4.a poštuje strogo razdvajanje uloga i odgovornosti s nadzornim aktivnostima u ovom članku i da obje aktivnosti funkcioniraju neovisno jedna o drugoj.

4. Države članice osiguravaju da nacionalna tijela za [...] **kibersigurnosnu** certifikaciju imaju odgovarajuće resurse za djelotvorno i učinkovito izvršavanje svojih ovlasti i obavljanje zadaća koje su im dodijeljene.

5. Kako bi se Uredba mogla djelotvorno provoditi, ta tijela trebala bi na aktivan, djelotvoran, učinkovit i siguran način sudjelovati u Europskoj skupini za kibersigurnosnu certifikaciju uspostavljenoj u skladu s člankom 53.

6. Nacionalna tijela za [...] **kibersigurnosnu** certifikaciju:

(a) [...]

(aa) prate i osiguravaju ispunjavanje obveza proizvođača ili pružatelja IKT proizvoda i usluga s poslovnim nastanom na svojim državnim područjima utvrđenim u članku 47.a stavcima 2. i 3. i odgovarajućem europskom programu kibersigurnosne certifikacije;

(b) [...] **ne dovodeći u pitanje članak 51. stavak 1.b, pomažu nacionalnim akreditacijskim tijelima u praćenju i nadzoru** aktivnosti tijela za ocjenjivanje sukladnosti za potrebe ove Uredbe[...];

(ba) prate i nadziru aktivnosti tijela iz članka 48. stavka 4.;

(bb) ovlašćuju tijela za ocjenjivanje sukladnosti iz članka 51. stavka 1.b i ograničavaju, suspendiraju ili povlače postojeće odobrenje u slučajevima neusklađenosti sa zahtjevima ove Uredbe;

(c) obrađuju pritužbe fizičkih ili pravnih osoba u pogledu certifikata koje su izdala [...] **nacionalna tijela za kibersigurnosnu certifikaciju ili, u skladu s člankom 48. stavkom 4.a, tijela za ocjenjivanje sukladnosti**, u prikladnoj mjeri istražuju predmet pritužbe i u razumnom roku obavješćuju podnositelja pritužbe o napretku i rezultatu istrage;

(d) surađuju s drugim nacionalnim tijelima za **kibersigurnosnu** [...] certifikaciju [...] ili s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj neusklađenosti IKT **postupaka**, proizvoda i usluga sa zahtjevima iz ove Uredbe ili s pojedinim europskim programima kibersigurnosne certifikacije;

(e) prate relevantne promjene u području kibersigurnosne certifikacije.

7. Svako nacionalno tijelo za [...] **kibersigurnosnu** certifikaciju ovlašteno je barem za sljedeće:

(a) zatražiti od tijelâ za ocjenjivanje sukladnosti, [...] nositelja europskog certifikata o kibersigurnosti **i izdavateljâ izjave EU-a o sukladnosti** da dostave sve informacije koje su mu potrebne za izvršavanje njegovih zadaća;

(b) provoditi istrage, u obliku revizija, tijelâ za ocjenjivanje sukladnosti**,** [...] nositelja europskog certifikata o kibersigurnosti **i izdavateljâ izjave EU-a o sukladnosti** za potrebe provjere sukladnosti s odredbama iz glave III.;

(c) poduzimati prikladne mjere, u skladu s nacionalnim pravom, kako bi osiguralo sukladnost tijelâ za ocjenjivanje sukladnosti**,** [...] nositelja europskog certifikata o kibersigurnosti **i izdavateljâ izjave EU-a o sukladnosti** s ovom Uredbom ili europskim programom kibersigurnosne certifikacije;

(d) osigurati pristup svim prostorijama tijela za ocjenjivanje sukladnosti i nositelja certifikata o kibersigurnosti za potrebe provedbe istraga u skladu s postupovnim pravom Unije ili države članice;

(e) povući, u skladu s nacionalnim pravom, certifikate koje su **izdala nacionalna tijela za kibersigurnosnu certifikaciju ili, u skladu s člankom 48. stavkom 4.a tijela za ocjenjivanje sukladnosti** koja nisu u skladu s ovom Uredbom ili europskim programom kibersigurnosne certifikacije.

(f) odrediti kazne, kako je predviđeno člankom 54., u skladu s nacionalnim pravom i zatražiti hitan prekid povreda obveza utvrđenih ovom Uredbom.

8. Nacionalna tijela za [...] **kibersigurnosnu** certifikaciju surađuju međusobno i s Komisijom i, posebice, razmjenjuju informacije, iskustva i dobru praksu u području kibersigurnosne certifikacije i tehničkih pitanja povezanih s kibersigurnošću IKT **postupaka**, proizvoda i usluga.

Članak 51

Tijela za ocjenjivanje sukladnosti

1. Tijela za ocjenjivanje sukladnosti akreditiraju nacionalna akreditacijska tijela u skladu s Uredbom (EZ) br. 765/2008 samo ako ispunjavaju zahtjeve utvrđene u Prilogu ovoj Uredbi.

1.a U slučajevima u kojima je europski kibersigurnosni certifikat izdalo nacionalno tijelo za kibersigurnosnu certifikaciju u skladu s člankom 48. stavkom 4. točkom (a) i člankom 48. stavkom 4.a, tijelo za izdavanje certifikata nacionalnog tijela za kibersigurnosnu certifikaciju akreditira se kao tijelo za ocjenjivanje sukladnosti u skladu sa stavkom 1. ovog članka.

1.b Ako je primjenjivo, nacionalno tijelo za kibersigurnosnu certifikaciju ovlašćuje tijela za ocjenjivanje sukladnosti za obavljanje svojih zadaća ako ispune posebne ili dodatne zahtjeve navedene u europskom programu certifikacije u skladu s člankom 47. stavkom 1. točkom (ca).

2. Akreditacija se izdaje na najviše pet godina i može se obnoviti pod istim uvjetima ako tijelo za ocjenjivanje sukladnosti i dalje ispunjava zahtjeve iz ovog članka. Akreditacijska tijela **poduzimaju sve odgovarajuće mjere u razumnom roku kako bi ograničila, suspendirala ili povukla akreditaciju** tijela za ocjenjivanje sukladnosti u skladu sa stavkom 1. ovog članka ako uvjeti za akreditaciju nisu ili više nisu ispunjeni ili ako se mjerama koje je poduzelo tijelo za ocjenjivanje sukladnosti krši ova Uredba.

Članak 52.

Obavješćivanje

1. Za svaki europski program kibersigurnosne certifikacije donesen u skladu s člankom 44. nacionalna tijela za [...] kibersigurnosnu certifikaciju obavješćuju Komisiju o [...] akreditiranim tijelima za ocjenjivanje sukladnosti **i ako je primjenjivo, ovlaštenima u skladu s člankom 51. stavkom 1.b.** za izdavanje certifikata na utvrđenoj razini jamstva iz članka 46. i, bez odgode, svim naknadnim promjenama u vezi s tim tijelima.

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

3. Ako Komisija primi obavijest nakon isteka razdoblja iz stavka **2**.[...], ona u *Službenom listu Europske unije* objavljuje izmjene popisa iz stavka 2., u roku od dva mjeseca od datuma primitka te obavijesti.

4. Nacionalno tijelo za [...] **kibersigurnosnu** certifikaciju može Komisiji podnijeti zahtjev da se tijelo za ocjenjivanje sukladnosti o kojem je država članica poslala obavijest ukloni s popisa iz stavka 2. ovog članka. Komisija objavljuje odgovarajuće izmjene popisa u *Službenom listu Europske unije* u roku od jednog mjeseca od primitka zahtjeva nacionalnog tijela za [...] **kibersigurnosnu** certifikaciju.

5. Komisija može provedbenim aktima definirati okolnosti, formate i postupke prijava iz stavka 1. ovog članka. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 55. stavka 2.

Članak 53.

Europska skupina za kibersigurnosnu certifikaciju

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

2. Skupina se sastoji od **predstavnika** nacionalnih tijela za [...] **kibersigurnosnu** certifikaciju **ili predstavnika drugih relevantnih nacionalnih tijela**. **[...] Svaki član Skupine može predstavljati najviše još jednu državu članicu**.

3. Skupina ima sljedeće zadaće:

(a) savjetovati Komisiju i pomagati joj u radu u cilju osiguravanja usklađene provedbe i primjene ove glave, posebno u pogledu 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 u skladu s člankom 44. ove Uredbe;

(ba) donijeti mišljenje o prijedlogu programa u skladu s člankom 44. ove Uredbe;

(c) [...] **zatražiti** od Agencije da izradi prijedlog europskog programa kibersigurnosne certifikacije u skladu s člankom 44. ove Uredbe;

(ca) osmisliti i donijeti smjernice o kriterijima za ocjenjivanje zahtjeva za izradu prijedloga programa podnesenog [...] Skupini u skladu s člankom 44. stavkom 1.a;

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

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

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

(fa) pružiti potporu provedbi mehanizma istorazinske ocjene u skladu s pravilima utvrđenima u europskom programu kibersigurnosne certifikacije u skladu s člankom 47. stavkom 1. točkom (md) ove Uredbe.

4. Skupinom predsjeda Komisija **u svojstvu moderatora** i osigurava joj tajništvo uz pomoć ENISA-e, kako je predviđeno u članku 8. točki (a).

Članak 53.a

Pravo na podnošenje pritužbe nacionalnom tijelu za [...] kibersigurnosnu certifikaciju

1. Fizička ili pravna osoba ima pravo na podnošenje pritužbe nacionalnom tijelu za [...] kibersigurnosnu certifikaciju u pogledu certifikata koje je izdalo to tijelo ili tijela za ocjenjivanje sukladnosti u skladu s člankom 48. stavkom 4.a.

2. Nacionalno tijelo za kibersigurnosnu certifikaciju kojem je podnesena pritužba obavješćuje podnositelja pritužbe o napretku i ishodu pritužbe, uključujući o mogućnosti pravnog lijeka na temelju članka 53.b.

Članak 53.b

Pravo na učinkovit pravni lijek

1. Fizička ili pravna osoba ima pravo na učinkovit pravni lijek protiv pravno obvezujuće odluke nacionalnog tijela za kibersigurnosnu certifikaciju koja se na nju odnosi.

2. Fizička ili pravna osoba ima pravo na učinkovit pravni lijek ako nacionalno tijelo za kibersigurnosnu certifikaciju ne riješi pritužbu.

3. Postupci protiv nacionalnog tijela za kibersigurnosnu certifikaciju vode se pred sudovima države članice u kojoj tijelo ima poslovni nastan.

Članak 54.

Kazne

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

GLAVA IV.
ZAVRŠNE ODREDBE

Članak 55.

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 56.

Evaluacija i revizija

1. Najkasnije pet godina od datuma iz članka 58. i svakih pet godina nakon toga Komisija ocjenjuje učinak, djelotvornost i učinkovitost Agencije i njezina načina rada kao i moguću potrebu za izmjenom mandata Agencije te financijske posljedice takve izmjene. Evaluacijom iz stavka 1. uzimaju se u obzir sve povratne informacije pružene Agenciji kao odgovor na njezine aktivnosti. Ako Komisija smatra da daljnje postojanje Agencije više nije opravdano s obzirom na ciljeve, mandat i zadaće koji su joj dodijeljeni, ona može predložiti izmjenu odredaba ove Uredbe koje se odnose na Agenciju.

2. Evaluacijom se ocjenjuje i učinak, djelotvornost i učinkovitost odredaba iz glave III. u pogledu ciljeva osiguranja prikladne razine kibersigurnosti IKT proizvoda i usluga u Uniji i poboljšanja funkcioniranja unutarnjeg tržišta.

3. Komisija izvješće o evaluaciji zajedno s njezinim zaključcima prosljeđuje Europskom parlamentu, Vijeću i Upravljačkom odboru. Nalazi te evaluacije objavljuju se.

Članak 57.

Stavljanje izvan snage i nasljeđivanje

1. Uredba (EZ) br. 526/2013 stavlja se izvan snage od [….].

2. Upućivanja na Uredbu (EZ) br. 526/2013 i ENISA-u smatraju se upućivanjima na ovu Uredbu i Agenciju.

3. Agencija nasljeđuje Agenciju osnovanu Uredbom (EZ) br. 526/2013 u pogledu cjelokupnog vlasništva, svih sporazuma, pravnih obveza, ugovora o radu, financijskih obveza i odgovornosti. Sve postojeće odluke Upravljačkog odbora i Izvršnog odbora ostaju na snazi ako nisu u sukobu s odredbama ove Uredbe.

4. Agencija se osniva na neodređeno razdoblje koje započinje od […]

5. Izvršni direktor imenovan u skladu s člankom 24. stavkom 4. Uredbe (EZ) br. 526/2013 izvršni je direktor Agencije do kraja svojeg mandata.

6. Članovi Upravljačkog odbora i njihovi zamjenici imenovani u skladu s člankom 6. Uredbe (EZ) br. 526/2013 nastavljaju biti članovi Upravljačkog odbora Agencije i zamjenici do kraja svojeg mandata.

Članak 58.

Stupanje na snagu

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

1.a Ova se Uredba primjenjuje od [...] osim članaka 50., 51., 52., 53.a, 53.b i 54 koji se primjenjuju [24 mjeseci nakon dana objave u Službenom listu Europske unije].

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

Sastavljeno u Bruxellesu,

Za Europski parlament	*Za Vijeće*
Predsjednik	*Predsjednik*

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 proizvodima odnosno uslugama u području IKT-a 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 ili usluga koje ono ocjenjuje može se smatrati tijelom za ocjenjivanje sukladnosti pod uvjetom da je dokazana njegova neovisnost i nepostojanje bilo kojeg oblika sukoba interesa.

4. Tijelo za ocjenjivanje sukladnosti, njegovo visoko rukovodstvo i osoblje zaduženo za ocjenjivanje sukladnosti ne smije biti projektant, proizvođač, dobavljač, ugraditelj, kupac, vlasnik, korisnik ili održavatelj IKT proizvoda ili usluga koje ocjenjuje, kao ni ovlašteni zastupnik bilo koje od tih strana. To ne isključuje upotrebu ocijenjenih proizvoda koji su potrebni za rad tijela za ocjenjivanje sukladnosti ili upotrebu takvih proizvoda u osobne svrhe.

5. Nadležno tijelo, njegovo visoko rukovodstvo i osoblje zaduženo za provedbu zadaća ocjenjivanja sukladnosti ne smiju izravno sudjelovati u projektiranju, proizvodnji ili izradi, stavljanju na tržište, montaži, uporabi ili održavanju tih IKT proizvoda ili usluga niti zastupati strane uključene u te djelatnosti. Ne smiju sudjelovati ni u kakvoj djelatnosti koja može ugroziti neovisnost njihove prosudbe ili poštenje u odnosu na djelatnosti ocjenjivanja sukladnosti za koje su prijavljeni. Navedeno se posebno odnosi na usluge savjetovanja.

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

7. 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, uključujući one financijske prirode, koji bi mogli utjecati na njihovu prosudbu ili rezultate njihova ocjenjivanja sukladnosti, posebno u vezi s osobama ili skupinama osoba kojima su rezultati tih aktivnosti važni.

8. 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 obavljaju u njegovo ime i pod njegovom odgovornošću.

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

(a) osobljem s tehničkim znanjem te dostatnim i primjerenim iskustvom za obavljanje zadaća ocjenjivanja sukladnosti;

(b) opisima postupaka u skladu s kojima provodi ocjenjivanje sukladnosti, kojima se osigurava transparentnost tih postupaka i mogućnost njihova ponavljanja. Ima i uspostavljenu primjerenu politiku i postupke za razlikovanje između djelatnosti koje provodi kao prijavljeno tijelo i drugih djelatnosti;

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

10. 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.

11. Osoblje zaduženo za aktivnosti ocjenjivanja sukladnosti ima:

(a) dobro tehničko i stručno obrazovanje kojim su obuhvaćene sve aktivnosti ocjenjivanja sukladnosti;

(b) dostatno poznavanje zahtjeva povezanih s ocjenjivanjima koja provodi i odgovarajuće ovlaštenje za provedbu tih ocjenjivanja;

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

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

12. Nepristranost tijela za ocjenjivanje sukladnosti, njihovog visokog rukovodstva i osoblja zaduženog za ocjenjivanje mora biti zajamčena.

13. Naknada za rad visokog rukovodstva i ocjenjivačkog osoblja tijela za ocjenu sukladnosti ne ovisi o broju provedenih ocjenjivanja ni o njihovim rezultatima.

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

15. Osoblje tijela za ocjenjivanje sukladnosti čuva poslovnu tajnu koja se odnosi na sve informacije prikupljene pri obavljanju zadaća u skladu s ovom Uredbom ili na temelju bilo koje odredbe nacionalnoga prava kojom se ona provodi, osim kad ih zahtijeva nadležno tijelo države članice u kojoj se provode njegove aktivnosti.

16. Tijela za ocjenjivanje sukladnosti ispunjavaju zahtjeve **relevantne** norme **usklađene na temelju Uredbe (EZ) br. 765/2008 za akreditaciju tijela za ocjenjivanje sukladnosti koje obavlja certifikaciju postupaka, proizvoda ili usluga [...].**

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