D.E.U. br. 18/002

HRVATSKI SABOR
Odbor za europske poslove

Klasa: 022-03/18-03/31
Urbroj: 6521-31-18-01
Zagreb, 23. ožujka 2018.

ODBOR ZA UNUTARNJU POLITKU I NACIONALNU SIGURNOST
Predsjednik Ranko Ostojić

ODBOR ZA INFORMIRANJE, INFORMATIZACIJU I MEDIJE
Predsjednik dr. sc. Andrija Mikulić

Poštovani predsjednici odbora,

Odbor za europske poslove na temelju članka 154. stavka 1. Poslovnika Hrvatskoga sabora prosljeđuje Odboru za unutarnju politiku i nacionalnu sigurnost te Odboru za informiranje, informatizaciju i medije stajalište o dokumentu Europske unije iz Radnog programa za razmatranje stajališta Republike Hrvatske za 2018. godinu:

Stajalište Republike Hrvatske o Prijedlogu 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") COM (2017) 477

koje je Koordinacija za vanjsku i europsku politiku i ljudska prava Vlade Republike Hrvatske usvojila Zaključkom: Klasa: 022-03/17-07/474, Urbroj: 50301-23/22-17-1 na sjednici održanoj 14. studenoga 2017. godine.

Predmetni Prijedlog uredbe Komisija je dostavila Hrvatskom saboru 12. listopada 2017. te je u tijeku njegovo donošenje u Europskom parlamentu i Vijeću Europske unije.

U skladu s člankom 154. stavkom 2. Poslovnika Hrvatskoga sabora, molim vas da Odboru za europske poslove dostavite mišljenje o Stajalištu Republike Hrvatske najkasnije do 4. svibnja 2018. godine.

S poštovanjem,

PREDSJEDNIK ODBORA
Domagoj Milošević

U prilogu:
- Stajalište Republike Hrvatske o COM (2017) 477
- COM (2017) 477

Na znanje:
- INFODOK služba

PRIJEDLOG OKVIRNOG STAJALIŠTA HR

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")

Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

Brojčana oznaka dokumenta: 12183/17, međuinstitucijski predmet: 2017/0225 (COD)

Koordinativno državno tijelo za izradu prijedloga stajališta (nositelj izrade stajališta), ustrojstvena jedinica i službenik/ica:

Nadležno državno tijelo:
Ured Vijeća za nacionalnu sigurnost (UVNS)

Ustrojstvena jedinica:
Odjel za planiranje i nadzor informacijske sigurnosti (UVNS)

Nadležni službenik/ica:
Aleksandar Klaić, pomoćnik predstojnika za informacijsku sigurnost
aleksandar.klaic@uvns.hr

Zamjena:
Vinko Kuculo, viši stručni savjetnik
vinko.kuculo@uvns.hr

Druga tijela državne uprave, agencije i javne ustanove uključena u izradu Prijedloga stajališta:
Zavod za sigurnost informacijskih sustava (ZSIS)

Nadležni službenik/ica u MVEP (Sektor za COREPER I):
Ana Đukić (ana.dukic@mvep.hr) 01/4569-816

Nadležna radna skupina Vijeća EU i nadležni službenik/ica u SP RH pri EU:
Horizontalna radna skupina za kibernetička pitanja; Tamara Tafra (Tamara.Tafra@mvep.hr)

Osnovne sadržajne odredbe prijedloga EU:

Ključne odredbe i izmjene sadržane u novom Prijedlogu su sljedeće:
- ENISA-i će se odobriti stalni mandat i osigurati stabilna osnova za budućnost. Mandat, ciljevi i zadaće trebali bi se i dalje redovito preispitivati.

- Predloženim mandatom dodatno se pojašnjava uloga ENISA-e kao agencije EU-a za kibersigurnost i kao referentne točke u kiberekosustavu EU-a, koja djeluje u bliskoj suradnji sa svim drugim relevantnim tijelima takvog ekosustava.
- Preispitivanje ustrojstva ENISA-e i upravljanja njome, koji su tijekom ocjenjivanja pozitivno ocijenjeni, provelo bi se u umjerenom opsegu, konkretno kako bi se osiguralo da su radom ENISA-e bolje obuhvaćene potrebe šire zajednice dionika.
- Podrobno je opisan predloženi opseg mandata s većim naglaskom na područjima u kojima je ENISA pokazala jasnu dodanu vrijednost te dodavanjem novih područja u kojima je potrebna potpora zbog novih prioriteta politike i instrumenata, posebno Direktive (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, revizije Strategije EU-a za kibersigurnost, novog Plana EU-a u području kibersigurnosti za suradnju u kiberkrizama i sigurnosno certificiranje u području IKT-a.

Razlozi za donošenje i pozadina dokumenta:

Europska unija (u daljnjem tekstu: EU) poduzela je niz mjera kako bi povećala otpornost i pojačala svoju kibersigurnosnu pripravnost. U prvoj strategiji EU-a za kibersigurnost, koja je donesena 2013., utvrđeni su strateški ciljevi i konkretne mjere za postizanje otpornosti, smanjenje kiberkriminaliteta, razvoj politike kiberobrane i sposobnosti za kiberobranu, razvoj industrijskih i tehnoloških resursa i uspostavu usklađene međunarodne politike kiberprostora za EU. U tom su se kontekstu u međuvremenu dogodile važne promjene, uključujući posebno drugi mandat Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA) i donošenje Direktive (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (tzv. NIS Direktiva).

Nadalje, Europska komisija donijela je 2016. Komunikaciju o jačanju europskog sustava kibernetičke sigurnosti i poticanju konkurentne i inovativne industrije kibernetičke sigurnosti, u kojoj su najavljene daljnje mjere za jačanje suradnje, razmjene informacija i znanja i povećanje otpornosti i pripravnosti EU-a, uzimajući u obzir i vjerojatnost incidenata velikih razmjera i moguću paneuropsku kiberkrizu. U tom kontekstu, Europska komisija je najavila da će predložiti ocjenjivanje i reviziju Uredbe (EU) br. 526/2013 Europskog parlamenta i Vijeća o Agenciji Europske unije za mrežnu i informacijsku sigurnost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004 („Uredba o ENISA-i"). Postupak ocjenjivanja mogao bi dovesti do moguće reforme ENISA-e i jačanja njezinih sposobnosti i kapaciteta za podupiranje država članica na održiv način. Ona bi time dobila aktivniju i važniju ulogu u postizanju kiberotpornosti te bi se u okviru njezina novog mandata priznale nove odgovornosti ENISA-e u skladu s Direktivom NIS.

Status dokumenta:

Zakonodavni prijedlog objavljen je 14. rujna 2017. godine. Europska komisija je prijedlog i prateću procjenu učinka predstavila na Horizontalnoj radnoj skupini za kibernetička pitanja 20. listopada, a početak rasprave na razini Radne skupine očekuje se u prvoj polovici studenog 2017.

Stajalište HR:

HR podupire Prijedlog uredbe. HR smatra kako pomoć ENISA-e državama članicama u vidu ex post tehničke istrage incidenata ne bi trebalo ograničiti samo na situacije kada su pogođene barem dvije države članice (članak 7. stavak 5. Uredbe o ENISA-i). U članku 44. Prijedloga uredbe utvrđuje se izrada i donošenje europskog programa kibersigurnosne certifikacije, no nije definiran rok u kojem, nakon zahtjeva Europske komisije, ENISA treba izraditi i dostaviti prijedlog tog programa, slijedom čega se predlaže dopuniti navedeni članak utvrđivanjem tog roka (primjerice 12, 18 ili 24 mjeseca). Smatramo da je potrebno pojašnjenje u kontekstu certificiranja kada se radi o proizvodima namijenjenim zaštiti klasificiranih podataka te se u tom smislu predlaže raspraviti o potrebi dodavanje recitala (54a) kojim bi se jasnije opisao odnos odredaba Uredbe i postojećih pravila o certifikaciji IKT proizvoda i usluga namijenjenih zaštiti klasificiranih podataka.

Nadalje, HR smatra da je potrebno pojašnjenje u kontekstu certificiranja kada se radi o proizvodima namijenjenim zaštiti klasificiranih podataka te se u tom smislu predlaže raspraviti o potrebi dodavanja recitala (54a) kojim bi se jasnije opisao odnos odredaba Uredbe i postojećih pravila o certifikaciji IKT proizvoda i usluga namijenjenih zaštiti klasificiranih podataka.

HR u ovom trenutku nije sklona poduprijeti stvaranje ograničenja za razvoj i korištenje nacionalnih normi u ovom području.

Sporna/otvorena pitanja za HR:
Opisano u dijelu „Stajalište HR".

Stajališta DČ, Vijeća EU i Predsjedništva EU:

UK pozdravlja prijedlog, ali ističe rizik od nove operacionalne uloge ENISA-e koja bi mogla dovesti do toga da države članice neće investirati dovoljno u vlastite nacionalne resurse. **FR** smatra kako ENISA treba biti središte za razmjenu ekspertize između država članica, drže da ENISA-u treba jačati, umjesto da postane agencija fokusirana na certificiranje. Naglašena je i važnost uvažavanja potreba industrije, kao i primjena „bottom-up" pristupa, što su podržale DE i FI. **DE** ističe kako se radi o ambicioznim prijedlozima o kojima je potrebna detaljna rasprava. Podržavaju jačanje ENISA-e kroz stalni mandat, ali ne podržavaju njene operativne ovlasti. Postojeće mehanizme koji su se pokazali uspješnim treba proširiti, a ne stvarati nove. Jačanje kibernetičke sigurnosti na EU razini moguće je samo jačanjem kibernetičke sigurnosti u državama članicama i međusobnom suradnjom. **FI** podržava stalni mandat za ENISA-u, ali izražava određene sumnje oko predloženog okvira za certificiranje te ističe kako on ne smije uzrokovati dodatne administrativne prepreke za kompanije. **HU** naglašava kako treba izbjeći preklapanja. Implementacija NIS direktive je ključna. Još razmatra treba li ENISA imati stalni mandat ili ne (isto i AT). **LV** je izrazila zabrinutost oko nacionalnih agencija te skepsu kako je ENISA sposobna provesti stratešku komunikaciju u slučaju kibernetičkih incidenata velikih

razmjera. **AT** nije zadovoljna što je certificiranje povezano s obnovom mandata ENISA-e. Ističe nužnost kompatibilnosti s nacionalnim kapacitetima te pozdravlja „security by design" pristup. **SE** smatra da Europska komisija nije dobro izračunala troškove. Također ne bi htjela vidjeti globalnu fragmentaciju zbog europskog okvira za certificiranje. **PL** ima pozitivan stav oko šireg mandata za ENISA-u. **SK** naglašava kako je potrebno uspostaviti poveznicu između CSIRT-a i („Computer Security Incident Response Teams" - timovi za odgovor na računalne sigurnosne incidente) ENISA-e. **BG** pozdravlja prijedlog, smatra da otvara mnoge mogućnosti i prilike za razvoj tržišta.

Sporna/otvorena pitanja za DČ, EK i Predsjedništvo EU:

Uz određena otvorena pitanja navedena u prethodnom odjeljku, detalji će biti poznati uslijed početka rasprava na Radnoj skupini.

Stav HR o spornim/otvorenim pitanjima DČ, EK i Predsjedništva EU:

Nema otvorenih pitanja.

Postojeće zakonodavstvo HR i potreba njegove izmjene slijedom usvajanja dokumenta:

U skladu s konačnim tekstom Uredbe bit će potrebno uskladiti i propisati odgovarajuće nadležnosti tijela u HR za poslove nadzora provedbe certifikacije, koji obuhvaćaju širok opseg poslova certifikacije IT proizvoda i usluga.

Utjecaj provedbe dokumenta na proračun HR:

Točne proračunske zahtjeve u ovom trenutku nije moguće procijeniti. Oni će se prije svega bazirati na dodatnom proračunu ENISA-e i s tim povezanih izdvajanja za funkcioniranje tijela EU-a, te na troškovima funkcioniranja tijela za nadzor certifikaciji.

EUROPSKA
KOMISIJA

Bruxelles, 22.2.2018.
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

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”)

(Tekst značajan za EGP)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

• Razlozi i ciljevi prijedloga

Europska unija poduzela je niz mjera kako bi povećala otpornost i pojačala svoju kibersigurnosnu pripravnost. U prvoj strategiji EU-a za kibersigurnost[1], koja je donesena 2013., utvrđeni su strateški ciljevi i konkretne mjere za postizanje otpornosti, smanjenje kiberkriminaliteta, razvoj politike kiberobrane i sposobnosti za kiberobranu, razvoj industrijskih i tehnoloških resursa i uspostavu usklađene međunarodne politike kiberprostora za EU. U tom su se kontekstu u međuvremenu dogodile važne promjene, uključujući posebno drugi mandat Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA)[2] i donošenje **Direktive o sigurnosti mrežnih i informacijskih sustava**[3] („Direktiva NIS"), na kojima se temelji ovaj prijedlog.

Nadalje, **Europska komisija donijela je 2016. Komunikaciju o jačanju europskog sustava kibernetičke sigurnosti i poticanju konkurentne i inovativne industrije kibernetičke sigurnosti**[4] u kojoj su najavljene daljnje mjere za jačanje suradnje, razmjene informacija i znanja i povećanje otpornosti i pripravnosti EU-a, uzimajući u obzir i vjerojatnost incidenata velikih razmjera i moguću paneuropsku kiberkrizu. U tom kontekstu Komisija je najavila da će predložiti **ocjenjivanje** i **reviziju** Uredbe (EU) br. 526/2013 Europskog parlamenta i Vijeća o Agenciji Europske unije za mrežnu i informacijsku sigurnost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004 („Uredba o ENISA-i"). Postupak ocjenjivanja mogao bi dovesti do moguće reforme Agencije i jačanja njezinih sposobnosti i kapaciteta za podupiranje država članica na održiv način. Ona bi time dobila aktivniju i važniju ulogu u postizanju kiberotpornosti te bi se u okviru njezina novog mandata priznale nove odgovornosti Agencije u skladu s Direktivom NIS.

Direktiva NIS prvi je bitni korak u cilju promicanja kulture upravljanja rizikom uvođenjem sigurnosnih zahtjeva kao pravne obveze za glavne gospodarske aktere, posebno operatore koji pružaju ključne usluge (operatori ključnih usluga – OES) i pružatelje nekih ključnih digitalnih usluga (pružatelji digitalnih usluga – DPS). Budući da se smatra da su sigurnosni zahtjevi od ključne važnosti za zaštitu koristi digitalizacije društva koja se stalno razvija te s obzirom na brzo širenje povezanih uređaja (internet stvari), u Komunikaciji iz 2016. iznesena je ideja uspostave okvira za sigurnosno certificiranje IKT proizvoda i usluga u cilju povećanja povjerenja i sigurnosti na jedinstvenom digitalnom tržištu. Kibersigurnosno certificiranje u području IKT-a postaje posebno važno s obzirom na sve veću uporabu tehnologija koje zahtijevaju visok stupanj kibersigurnosti, kao što su povezani i automatizirani automobili, e-zdravstvo ili kontrolni sustavi za industrijsku automatizaciju (IACS).

Te mjere politike i najave dodatno su pojačane **Zaključcima Vijeća** iz 2016. u kojima se potvrđuje da se „kiberprijetnje i kiberslabosti nastavljaju razvijati i jačati što će zahtijevati

---

1 Zajednička komunikacija Europske komisije i Europske službe za vanjsko djelovanje: Strategija Europske unije za kibernetičku sigurnost: otvoren, siguran i zaštićen kibernetički prostor", JOIN(2013) final

2 Uredba (EU) br. 526/2013 o Agenciji Europske unije za mrežnu i informacijsku sigurnost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004.

3 Direktiva (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.

4 Komunikacija Komisije o jačanju europskog sustava kibernetičke sigurnosti i poticanju konkurentne i inovativne industrije kibernetičke sigurnosti, COM/2016/0410 final.

trajnu i bližu suradnju, posebice u pogledu suočavanja s prekograničnim kiberincidentima velikih razmjera". U Zaključcima je potvrđeno da je „Uredba o ENISA-i jedan od temeljnih elemenata okvira kiberotpornosti EU-a"[5] i traži se od Komisije da poduzme daljnje korake za rješavanje pitanja certifikacije na europskoj razini.

Za uspostavu programa certificiranja trebalo bi uspostaviti primjereni sustav upravljanja na razini EU-a, među ostalim s pomoću stručnih savjeta neovisne agencije EU-a. U tom je pogledu prirodan odabir ENISA-e u ovom prijedlogu kao tijela na razini EU-a nadležnog za pitanja kibersigurnosti koje bi moglo preuzeti ulogu okupljanja nacionalnih nadležnih tijela u području certificiranja i koordinacije njihova rada.

U svojoj **Komunikaciji o preispitivanju provedbe Strategije jedinstvenog digitalnog tržišta na sredini provedbenog razdoblja iz svibnja 2017.** Komisija je dalje navela da će do rujna 2017. preispitati mandat ENISA-e. Cilj je tog preispitivanja definirati njezinu ulogu u promijenjenom kiberekosustavu i razviti mjere povezane s normama u području kibersigurnosti, certificiranjem i označavanjem kako bi se povećala kibersigurnost sustava utemeljenih na IKT-u, uključujući povezane objekte[6]. U **zaključcima Europskog vijeća** iz lipnja 2017.[7] pozdravljena je namjera Komisije da u rujnu preispita strategiju za kibersigurnost i da do kraja 2017. predloži dodatne ciljane mjere.

Predloženom Uredbom osigurava se sveobuhvatni skup mjera koje se temelje na prethodnim djelovanjima te se potiču posebni ciljevi koji se uzajamno podupiru:

- jačanje **sposobnosti i pripravnosti** država članica i poduzeća,
- poboljšanje **suradnje i koordinacije** među državama članicama i institucijama, agencijama i tijelima EU-a,
- jačanje **sposobnosti na razini EU-a za dopunu djelovanja država članica**, posebno u slučaju prekograničnih kiberkriza,
- jačanje **osviještenosti** građana i poduzeća o pitanjima kibersigurnosti,
- povećanje opće **transparentnosti kibersigurnosnog jamstva**[8] za IKT proizvode i usluge u cilju jačanja povjerenja u jedinstveno digitalno tržište i u digitalne inovacije i
- izbjegavanje **fragmentiranja programa certificiranja** u EU-u i povezanih sigurnosnih zahtjeva i kriterija za ocjenjivanje po državama članicama i sektorima.

U sljedećem dijelu Obrazloženja podrobnije se objašnjavaju temeljni razlozi za inicijativu u odnosu na predložene aktivnosti ENISA-a i kibersigurnosnu certifikaciju.

---

5 Zaključci Vijeća o jačanju europskog sustava kiberotpornosti i poticanju konkurentne i inovativne industrije kibersigurnosti – 15. studenoga 2016.

6 Komunikacija Komisije o preispitivanju provedbe Strategije jedinstvenog digitalnog tržišta na sredini provedbenog razdoblja – COM(2017) 228.

7 Sastanak Europskog vijeća (22. i 23. lipnja 2017.) – Zaključci EUCO 8/17.

8 Transparentnost kibersigurnosnog jamstva znači pružanje korisnicima dovoljno informacija o kibersigurnosnim značajkama s pomoću kojih mogu objektivno utvrditi razinu sigurnosti određenog IKT proizvoda, usluge ili postupka.

ENISA

ENISA djeluje kao stručni centar za jačanje mrežne i informacijske sigurnosti u Uniji i potporu jačanju kapaciteta u državama članicama.

ENISA je osnovana 2004.[9] kako bi se pridonijelo općem cilju osiguranja visoke razine mrežne i informacijske sigurnosti u EU-u. Godine 2013. Uredbom (EU) br. 526/2013 utvrđen je novi mandat Agencije na razdoblje od sedam godina, do 2020. Uredi Agencije nalaze se u Grčkoj, odnosno njezino administrativno središte je u Heraklionu (Kreta), a operativno središte u Ateni.

ENISA je mala agencija s malim proračunom i malim brojem osoblja u usporedbi s drugim agencijama EU-a. Njezin je mandat ograničen.

ENISA pruža potporu europskim institucijama, državama članicama i poslovnoj zajednici u **rješavanju problema povezanih s mrežnom i informacijskom sigurnošću, u odgovaranju na te probleme i posebno u njihovom sprječavanju.** Ona to čini nizom aktivnosti u pet područja utvrđenih u strategiji[10]:

- stručno znanje: pružanje informacija i stručnog znanja o ključnim pitanjima mrežne i informacijske sigurnosti,
- politika: potpora donošenju i provedbi politike u Uniji,
- kapacitet: potpora jačanju kapaciteta u Uniji (npr. s pomoću osposobljavanja, preporuka i aktivnosti osvješćivanja).
- zajednica: jačanje zajednice mrežne i informacijske sigurnosti (npr. potpora timovima za hitne računalne intervencije (CERT-ovima), koordinacija paneuropskih vježbi u području kibersigurnosti),
- omogućavanje (npr. suradnja s dionicima i međunarodni odnosi).

Tijekom pregovora o Direktivi NIS suzakonodavci EU-a odlučili su ENISA-i dodijeliti važne uloge u njezinoj provedbi. Konkretno, Agencija mreži CSIRT-ova osigurava tajništvo (uspostavljeno u cilju promicanja brze i učinkovite operativne suradnje među državama članicama u slučaju određenih kiberincidenata i razmjene informacija o rizicima) i od nje se traži da pomaže Skupini za suradnju pri izvršavanju njezinih zadaća. Nadalje, Direktivom se zahtijeva od ENISA-e da pomaže državama članicama i Komisiji pružanjem stručnog znanja i savjetovanjem te olakšavanjem razmjene najbolje prakse.

U skladu s Uredbom o ENISA-i Komisija je izvršila ocjenjivanje Agencije koja uključuje neovisnu studiju i javno savjetovanje. Tijekom ocjenjivanja procijenjeni su relevantnost, učinak, djelotvornost, učinkovitost, usklađenost Agencije te njezina dodana vrijednost za EU s obzirom na njezinu uspješnost, upravljanje, unutarnje ustrojstvo i radnu praksu u razdoblju od 2013. do 2016.

[9] 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.

[10] https://www.enisa.europa.eu/publications/corporate/enisa-strategy

Većina ispitanika u javnom savjetovanju pozitivno je ocijenila uspješnost rada ENISA-e[11] (74 %). Nadalje, većina ispitanika smatrala je da ENISA ostvaruje svoje različite ciljeve (barem 63 % za svaki cilj). Približno pola ispitanika (46 %) redovito (mjesečno ili češće) koristi se uslugama i proizvodima ENISA-e i te su usluge i proizvodi cijenjeni jer ih pruža tijelo na razini EU-a (83 %) i zbog njihove kvalitete (62 %).

Međutim, velika većina (88 %) ispitanika smatrala je da trenutačni instrumenti i mehanizmi koji su dostupni na razini EU-a nisu dostatni ili su samo djelomično prikladni za rješavanje trenutačnih izazova u području kibersigurnosti. Velika većina ispitanika (98 %) navela je da bi se zadovoljavanjem tih potrebe trebalo baviti tijelo EU-a, a 99 % ispitanika smatralo je da je ENISA prava organizacija za to. Nadalje, 67,5 % ispitanika izjavilo je da bi ENISA mogla imati ulogu u uspostavi usklađenog okvira za sigurnosno certificiranje IKT proizvoda i usluga.

Tijekom općeg ocjenjivanja (koje se ne temelji samo na javnom savjetovanju već i na nizu pojedinačnih razgovora, dodatnih ciljanih anketa i radionica) doneseni su sljedeći zaključci:

- Ciljevi ENISA-e još uvijek su relevantni. U kontekstu brzog tehnološkog razvoja i rastućih prijetnji te s obzirom na sve veće globalne rizike u području kibersigurnosti jasno je da EU mora poticati i dalje jačati tehničku stručnost za pitanja kibersigurnosti na visokoj razini. U državama članicama treba jačati kapacitete za razumijevanje prijetnji i za odgovor na prijetnje i dionici moraju surađivati u svim tematskim područjima i sa svim institucijama.
- Unatoč malom proračunu Agencija je učinkovito iskorištavala svoje resurse i izvršavala svoje zadaće. Međutim, zbog dvije lokacije u Ateni i Heraklionu nastali su dodatni administrativni troškovi.
- Kada je riječ o djelotvornosti, ENISA je djelomično ostvarila svoje ciljeve. Agencija je uspješno pridonijela poboljšanju mrežne i informacijske sigurnosti u Europi ponudom jačanja kapaciteta u 28 država članica[12], jačanjem suradnje među državama članicama i dionicima u području mrežne i informacijske sigurnosti te pružanjem stručnih savjeta, jačanja zajedništva i potpore razvoju politika. ENISA se vrijedno usmjerila na provedbu svojeg programa rada i bila je pouzdani partner svojim dionicima u području čija je velika prekogranična važnost priznata tek nedavno.
- ENISA je uspjela ostvariti učinak, barem u određenoj mjeri, u širokom području mrežne i informacijske sigurnosti, ali nije u potpunosti uspjela razviti prepoznatljivost i dostatnu vidljivost da bi bila priznata kao „glavni" stručni centar u Europi. To se može objasniti širokim mandatom ENISA-e za koji joj nisu osigurana razmjerna i dostatna sredstva. Nadalje, ENISA je jedina agencija EU-a s ograničenim

[11] U savjetovanju je sudjelovalo ukupno 90 dionika iz 19 država članica (88 odgovora i 2 stajališta), uključujući nacionalna tijela iz 15 država članica i 8 krovnih organizacija koje predstavljaju znatan broj europskih poduzeća.

[12] Od sudionika u javnom savjetovanju tražilo se da navedu što smatraju glavnim postignućima ENISA-e u razdoblju od 2013. do 2016. Ispitanici iz svih skupina (ukupno 55, uključujući 13 iz nacionalnih nadležnih tijela, 20 iz privatnog sektora i 22 iz „ostalih") smatrali su da su glavna postignuća ENISA-e sljedeća: 1) koordinacija vježbi Cyber Europe; 2) pružanje potpore CERT-ovima/CSIRT-ovima organiziranjem osposobljavanja i radionica za poticanje koordinacije i razmjene; 3) publikacije ENISA-e (smjernice i preporuke, izvješća o prijetnjama, strategije za izvješćivanje o incidentima i upravljanje krizom itd.) koje su se smatrale korisnima za izradu i ažuriranje nacionalnih sigurnosnih okvira te kao referenca za kreatore politike i kiberstručnjake; 4) potpora promicanju Direktive NIS; 5) napori usmjereni na podizanje razine osviještenosti o kibersigurnosti u okviru mjeseca kibersigurnosti.

mandatom, zbog čega je ograničena njezina mogućnost razvoja dugoročne vizije i održive potpore dionicima. To je i u suprotnosti s odredbama Direktive NIS kojom se ENISA-i povjeravaju zadaće koje nisu ograničenog trajanja. Naposljetku, ocjenjivanjem je utvrđeno da se njezina ograničena djelotvornost dijelom može objasniti znatnim oslanjanjem na vanjske stručnjake umjesto na vlastite stručnjake te teškoćama sa zapošljavanjem i zadržavanjem stručnog osoblja.

- Naposljetku, ali ne najmanje važno, zaključak je ocjenjivanja da dodana vrijednost ENISA-e poglavito proizlazi iz sposobnosti Agencije da pojača suradnju poglavito među državama članicama, a posebno s povezanim zajednicama mrežne i informacijske sigurnosti (posebno između CSIRT-ova). Na razini EU-a ne postoji nijedan drugi akter koji podupire tako široki raspon dionika u području mrežne i informacijske sigurnosti. Međutim, budući da ENISA mora strogo odrediti prioritete među svojim aktivnostima, njezin program rada većinom se temelji na potrebama država članica. Ona zbog toga ne rješava u dovoljnoj mjeri potrebe drugih dionika, posebno industrije. Osim toga, Agencija poglavito zadovoljava potrebe svojih ključnih dionika, a zbog toga ne može ostvariti veći učinak. Stoga se dodana vrijednost Agencije razlikovala ovisno o različitim potrebama njezinih dionika i mjeri do koje ih je mogla zadovoljiti (npr. velike države članice u odnosu na male države članice; države članice u odnosu na industriju).

Ukratko, na temelju rezultata savjetovanja s dionicima i ocjenjivanja moglo se zaključiti da treba prilagoditi resurse i mandat ENISA-e kako bi ona mogla imati odgovarajuću ulogu u odgovoru na sadašnje i buduće izazove.

Uzimajući u obzir te nalaze u ovom prijedlogu preispituje se trenutačni mandat ENISA-e i utvrđuje obnovljeni skup zadaća i funkcija u cilju djelotvorne i učinkovite potpore nastojanju država članica, institucija EU-a i ostalih dionika da u Europskoj uniji osiguraju siguran kiberprostor. Novim predloženim mandatom nastoji se Agenciji dati snažnija i važnija uloga koja će posebno uključivati podupiranje država članica u provedbi Direktive NIS te osigurati da aktivnije suzbija određene prijetnje (operativni kapacitet) i da postane stručni centar za pomoć državama članicama i Komisiji u postupku kibersigurnosne certifikacije. Ovim prijedlogom:

- ENISA-i će se odobriti stalni mandat i osigurati stabilna osnova za budućnost. Mandat, ciljevi i zadaće trebali bi se i dalje redovito preispitivati.
- Predloženim mandatom dodatno se pojašnjava uloga ENISA-e kao agencije EU-a za kibersigurnost i kao referentne točke u kiberekosustavu EU-a koja djeluje u bliskoj suradnji sa svim drugim relevantnim tijelima takvog ekosustava.
- Preispitivanje ustrojstva Agencije i upravljanja njome, koji su tijekom ocjenjivanja pozitivno ocijenjeni, provelo bi se u umjerenom opsegu, konkretno kako bi se osiguralo da su radom Agencije bolje obuhvaćene potrebe šire zajednice dionika.
- Podrobno je opisan predloženi opseg mandata s većim naglaskom na područjima u kojima je agencija pokazala jasnu dodanu vrijednost te dodavanjem novih područja u kojima je potrebna potpora zbog novih prioriteta politike i instrumenata, posebno Direktive NIS, revizije Strategije EU-a za kibersigurnost, novog Plana EU-a u području kibersigurnosti za suradnju u kiberkrizama i sigurnosno certificiranje u području IKT-a:
    - **Razvoj i provedba politike EU-a:** ENISA bi dobila zadaću da proaktivno pridonosi razvoju politike u području mrežne i informacijske sigurnosti te drugim inicijativama politike koja obuhvaća elemente kibersigurnosti u

različitim sektorima (npr. energija, promet, financije). Ona bi u tu svrhu imala snažnu savjetodavnu ulogu koju bi mogla ispuniti pružanjem neovisnih mišljenja i pripremnih aktivnosti za razvoj i ažuriranje politike i zakona. ENISA bi također podupirala politiku i zakonodavstvo EU-a u području elektroničkih komunikacija, elektroničkog identiteta i usluga povjerenja u cilju promicanja veće razine kibersigurnosti. U fazi provedbe, a posebno u kontekstu skupine za suradnju NIS, ENISA bi pomagala državama članicama da ostvare usklađeni pristup provedbi Direktive NIS-u preko granica i u svim sektorima te u drugim relevantnim politikama i zakonima. ENISA bi pridonosila redovitom preispitivanju politika i zakona u području kibersigurnosti i redovitim izvješćivanjem o stanju provedbe pravnog okvira EU-a.

- **Jačanje kapaciteta:** ESISA bi pridonosila jačanju sposobnosti i stručnosti tijela EU-a i nacionalnih javnih tijela, uključujući u području odgovora na incidente i nadzora regulatornih mjera povezanih s kibersigurnošću. Agencija bi imala obvezu pridonijeti i uspostavi centara za razmjenu i analizu informacija (ISAC-ovi) u različitim sektorima pružanjem najbolje prakse i savjeta o dostupnim alatima i postupcima te prikladnim rješavanjem regulatornih pitanja povezanih s razmjenom informacija.

- **Znanje i informacije, podizanje razine osviještenosti:** ENISA bi postala informativni centar EU-a. To bi značilo promicanje i razmjenu najbolje prakse i inicijativa u cijelom EU-u prikupljanjem informacija o kibersigurnosti od institucija, agencija i tijela EU-a i nacionalnih institucija, agencija i tijela. Agencija bi pružala i savjete, smjernice i najbolju praksu u pogledu sigurnosti ključne infrastrukture. Nakon znatnih prekograničnih kiberincidenata ENISA bi sastavljala izvješća u cilju pružanja savjeta poduzećima i građanima u cijelom EU-u. Takva organizacija posla uključivala bi i redovitu organizaciju aktivnosti osvješćivanja u koordinaciji s nadležnim tijelima država članica.

- **Zadaće povezane s tržištem (normizacija, kibersigurnosna certifikacija):** ENISA bi obavljala niz funkcija kojima se posebno podupire unutarnje tržište i koje obuhvaćaju „opservatorij tržišta" kibersigurnosti, a uključuju analizu relevantnih trendova na kibersigurnosnom tržištu radi boljeg usklađivanja ponude i potražnje i podupiranje razvoja politike EU-a u području normizacije IKT-a i kibersigurnosne certifikacije u području IKT-a. Kada je konkretno riječ o normizaciji, njome bi se olakšala uspostava i prihvaćanje normi u području kibersigurnosti. ENISA bi obavljala i zadaće koje su predviđene u kontekstu budućeg okvira za certifikaciju (vidi odjeljak u nastavku).

- **Istraživanje i inovacije:** ENISA bi pružala stručne savjete tijelima EU-a i nacionalnim tijelima o utvrđivanju prioriteta u području istraživanja i razvoja, među ostalim u kontekstu ugovornog javno-privatnog partnerstva u području kibersigurnosti (cPPP). Savjeti ENISA-e o istraživanju uzeli bi se u obzir u novom Europskom centru za istraživanje i kompetencije u području kibersigurnosti u okviru sljedećeg višegodišnjeg financijskog okvira. ENISA bi, na zahtjev Komisije, sudjelovala i u provedbi programa EU-a za financiranje istraživanja i inovacija.

- **Operativna suradnja i upravljanje krizom:** te aktivnosti temeljile bi se na jačanju postojećih operativnih sposobnosti za prevenciju, što bi konkretno uključivalo unaprjeđenje paneuropskih vježbi u području kibersigurnosti (Cyber Europe) njihovim održavanjem svake godine te pomoćnu ulogu u

operativnoj suradnji koju bi ona imala kao tajništvo mreže CSIRT-ova (u skladu s odredbama Direktive NIS) koja uključuje osiguranje, među ostalim, dobrog funkcioniranja IT infrastrukture i komunikacijskih kanala mreže CSIRT-ova. U tom bi kontekstu bila potrebna strukturirana suradnja s CERT-EU-om, Europskim centrom za kiberkriminal (EC3) i drugim nadležnim tijelima EU-a. Nadalje, strukturirana suradnja s CERT-EU-om, u velikoj fizičkoj blizini, trebala bi dovesti do funkcije pružanja tehničke pomoći u slučaju znatnih incidenata i podupiranja analize incidenata. Države članice koje to zatraže dobile bi pomoć za rješavanje incidenata i potporu za analizu ranjivosti, tragova i incidenata u cilju jačanja njihovih preventivnih i reaktivnih sposobnosti.

- ENISA bi imala važnu ulogu i u **EU-ovu planu za kibersigurnost** koji se predstavlja u okviru ovog paketa i u kojem je navedena preporuka Komisije državama članicama o koordiniranom odgovoru na velike prekogranične incidente u području kibersigurnosti i krize na razini EU-a[13]. ENISA bi olakšala suradnju među pojedinim državama članicama u okviru hitnih odgovora analizom i objedinjavanjem nacionalnih izvješća o stanju na temelju informacija koje joj dobrovoljno dostavljaju države članice i ostali subjekti.

- **Kibersigurnosna certifikacija IKT proizvoda i usluga**

U cilju uspostave i očuvanja povjerenja i sigurnosti IKT proizvodi i usluge moraju izravno uključivati sigurnosne značajke u ranim fazama svojeg tehničkog dizajna i razvoja (integrirana sigurnost). Nadalje, potrošači i korisnici moraju moći provjeriti razinu sigurnosnog jamstva proizvoda i usluga koje nabavljaju ili kupuju.

Certifikacija, koja obuhvaća formalno ocjenjivanje proizvoda, usluga i postupaka koje obavlja neovisno i akreditirano tijelo u skladu s utvrđenim skupom kriterija i izdavanje certifikata o sukladnosti, ima važnu ulogu za povećanje povjerenja i sigurnosti proizvoda i usluga. Iako je ocjenjivanje sigurnosti u dobroj mjeri tehničko područje, svrha je certificiranja informirati kupce i korisnike o sigurnosnim obilježjima IKT proizvoda i usluga koje kupuju i kojima se koriste i uvjeriti ih u njihovu sigurnost. Kako je prethodno navedeno, to se posebno odnosi na nove sustave u kojima se u velikoj mjeri upotrebljavaju digitalne tehnologije i koji zahtijevaju visoku razinu sigurnosti, primjerice povezani i automatizirani automobili, e-zdravlje, kontrolni sustavi za industrijsku automatizaciju[14] ili pametne mreže.

Trenutačno je kibersigurnosna certifikacija IKT proizvoda i usluga u EU-u u znatnoj mjeri fragmentirana. Postoji niz međunarodnih inicijativa, na primjer Zajednički kriteriji (CC) za sigurnosno ocjenjivanje informacijske tehnologije (ISO 15408), što je međunarodna norma za ocjenjivanje računalne sigurnosti. Temelji se na evaluaciji treće strane i predviđa sedam razina Procjene razine osiguranja (EAL). Zajednički kriteriji i prateća Zajednička metodologija za ocjenjivanje sigurnosti informacijske tehnologije (CEM) tehnička su osnova za međunarodni sporazum, Sporazum o zajedničkim kriterijima za priznavanje (CCRA) kojim

[13] „Plan" će se primjenjivati na kiberincidente koji uzrokuju poremećaje koje države članice ne mogu same riješiti ili koje utječu na više država članica i imaju toliko opsežan i znatan utjecaj ili političku važnost da zahtijevaju pravodobnu koordinaciju politike i odgovor na političkoj razini Unije.

[14] GU JRC objavio je izvješće u kojem se predlaže početni skup zajedničkih europskih zahtjeva i općih smjernica povezanih s kibersigurnosnom certifikacijom komponenata IACS-a Dostupno na: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

se osigurava da certifikate o ispunjavanju zajedničkih kriterija priznaju svi njegovi potpisnici. Međutim, u okviru trenutačne verzije CCRA-a uzajamno se priznaju samo ocjene do razine EAL 2. Nadalje, sporazum je potpisalo samo 13 država članica.

Tijela za certificiranje 12 država članica sklopila su sporazum o uzajamnom priznavanju koji se odnosi na certifikate izdane u skladu sa sporazumom na temelju Zajedničkih kriterija[15]. Nadalje, u državama članicama trenutačno postoji određeni broj inicijativa za certifikaciju IKT-a ili je njihova uspostava u tijeku. Bez obzira na njihovu važnost, prisutan je rizik od rascjepkanosti tržišta i pojave problema povezanih s interoperabilnošću. Zbog toga će trgovačko društvo možda morati prolaziti nekoliko postupaka certificiranja u različitim državama članicama da bi svoj proizvod moglo ponuditi na više tržišta. Na primjer, proizvođač brojila koji želi prodavati svoje proizvode u tri države članice, na primjer u Njemačkoj, Francuskoj i UK-u trenutačno se mora uskladiti s tri različita programa certificiranja. To su Jamstvo za komercijalne proizvode (CPA) u UK-u, Certification de Sécurité de Premier Niveau u Francuskoj (CSPN) i profil za posebnu zaštitu na temelju Zajedničkih kriterija u Njemačkoj.

To stanje dovodi do većih troškova i trgovačkim društvima koja djeluju u nekoliko država članica stvara znatno administrativno opterećenje. Iako se trošak certificiranja može znatno razlikovati ovisno o predmetnom proizvodu/usluzi, traženoj razini osiguranja u okviru ocjenjivanja i/ili ostalim komponentama, u načelu je riječ o velikim troškovima za poduzeća. BSI-jev certifikat „Smart Meter Gateway”, na primjer, košta više od milijun EUR (najviša razina ispitivanja i jamstva, ne odnosi se samo na jedan proizvod već i na cijelu infrastrukturu oko proizvoda). Certifikacija pametnih brojila u UK-u košta približno 150 000 EUR. Trošak u Francuskoj sličan je trošku u UK-u, približno 150 000 EUR ili više.

Ključni javni i privatni dionici potvrdili su da trgovačka društva, zbog nepostojanja programa kibersigurnosne certifikacije za cijeli EU, moraju u mnogim okolnostima biti zasebno certificirana u svakoj državi članici, što dovodi do rascjepkanosti tržišta. Još je važnije napomenuti da bi, u nedostatku zakonodavstva EU-a o usklađivanju u području IKT proizvoda i usluga, zbog razlika u normama i praksi kibersigurnosne certifikacije u državama članicama u EU-u moglo nastati 28 odvojenih sigurnosnih tržišta s vlastitim tehničkim zahtjevima, metodologijama ispitivanja i postupcima za kibersigurnosna certifikacija. Ako se ne poduzmu prikladne mjere na razini EU-a, ti različiti pristupi na nacionalnoj razini mogli bi uzrokovati znatne probleme u uspostavi jedinstvenog digitalnog tržišta jer bi se usporili ili spriječili povezani pozitivni učinci u pogledu rasta i zapošljavanja.

Na temelju prethodno navedenih kretanja predloženom Uredbom uspostavlja se okvir za kibersigurnosnu certifikaciju („**Okvir**”) IKT proizvoda i usluga i opisuju osnovne funkcije i zadaće ENISA-e u području kibersigurnosne certifikacije. Ovim prijedlogom uspostavlja se opći okvir pravila kojima se uređuju europski programi kibersigurnosne certifikacije. Prijedlogom se ne uvode izravno operativni programi certificiranja već se stvara sustav (okvir) za uspostavu posebnih programa certificiranja za određene IKT proizvode/usluge („Europski programi kibersigurnosne certifikacije”). Stvaranjem europskih programa kibersigurnosne certifikacije u skladu s Okvirom omogućit će se da certifikati izdani na temelju tih programa budu važeći i priznati u svim državama članicama te će se riješiti postojeći problem rascjepkanosti tržišta.

[15] Skupina viših dužnosnika o sigurnosti informacijskih sustava (SOG-IS) uključuje 12 država članica i Norvešku i razvila je nekoliko profila za zaštitu na ograničenom broju proizvoda kao što su digitalni potpis, digitalni tahograf i pametne kartice. Sudionici zajedno rade na koordinaciji normizacije profila zaštite CC i koordiniraju razvoj profila zaštite. Države članice često traže certificiranje SOG-IS za nacionalne postupke javne nabave.

Opća je svrha europskog programa kibersigurnosne certifikacije potvrditi da su IKT proizvodi i usluge koji su certificirani u skladu s takvim programom u skladu s navedenim kibersigurnosnim zahtjevima. To bi, primjerice, uključivalo njihovu sposobnost da zaštite podatke (pohranjene, poslane ili obrađene na neki drugi način) od slučajnog ili neovlaštenog pohranjivanja, obrade, pristupa, otkrivanja, uništavanja, slučajnog gubitka ili izmjene. Programima kibersigurnosne certifikacije EU-a iskoristile bi se postojeće norme u pogledu tehničkih zahtjeva i postupaka evaluacije s kojima se proizvodi moraju uskladiti, a ne bi se razvijale posebne tehničke norme[16]. Na primjer, certificiranje proizvoda poput pametnih kartica, koji se trenutačno ispituju na temelju međunarodnih normi CC-a u skladu s multilateralnim programom SOG-IS (kako je prethodno opisano) u cijelom EU-u značilo bi da se taj program primjenjuje u cijelom EU-u.

U prijedlogu se ne ističe samo poseban skup sigurnosnih ciljeva koje treba uzeti u obzir pri oblikovanju posebnog europskog programa kibersigurnosne certifikacije već se propisuje i minimalni sadržaj takvih programa Takvim programima morat će se odrediti, među ostalim, broj posebnih elemenata kojima se utvrđuju područje primjene i cilj kibersigurnosne certifikacije. To uključuje utvrđivanje obuhvaćenih kategorija proizvoda i usluga, detaljnu specifikaciju kibersigurnosnih zahtjeva (na primjer upućivanjem na primjenjive norme ili tehničke specifikacije), posebne kriterije i metode za ocjenjivanje i razinu jamstva koja se njima planira osigurati (npr. osnovna, znatna ili visoka).

Europske programe kibersigurnosne certifikacije izradit će ENISA uz pomoć i stručne savjete Europske skupine za kibersigurnosnu certifikaciju (vidjeti u nastavku) i u suradnji s njome, a donijet će ih Komisija provedbenim aktima. Kada se utvrdi da je potreban program kibersigurnosne certifikacije, Komisija će zatražiti od ENISA-e da izradi program za određene IKT proizvode i usluge. ENISA će raditi na programu u bliskoj suradnji s nacionalnim tijelima za nadzor certifikacije koja su zastupljena u Skupini. Države članice i skupina mogu Komisiji predložiti da od ENISA-e zatraži izradu određenog programa.

Certificiranje može biti vrlo skup postupak koji bi mogao dovesti do viših cijena za kupce i potrošače. Potreba za certificiranjem može se znatno razlikovati i zbog posebnog konteksta uporabe proizvoda i usluga i brzine tehnoloških promjena. Uporaba europske kibersigurnosne certifikacije stoga bi i dalje trebala biti dobrovoljna, osim ako je drugačije predviđeno u zakonodavstvu Unije kojim su propisani sigurnosni zahtjevi za IKT proizvode i usluge.

Kako bi se osigurala usklađenost i izbjegla rascjepkanost, nacionalni programi ili postupci kibersigurnosne certifikacije za IKT proizvode i usluge obuhvaćene europskim programom kibersigurnosne certifikacije prestat će se primjenjivati od datuma utvrđenog u provedbenom aktu o donošenju programa. Države članice ne bi trebale uvoditi nove nacionalne programe kibersigurnosne certifikacije IKT proizvoda i usluga koji su već obuhvaćeni postojećim europskim programom kibersigurnosne certifikacije.

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. Ako tijela za ocjenjivanje sukladnosti ispunjavaju određene propisane zahtjeve, trebalo bi ih akreditirati akreditacijsko tijelo. Akreditacija se izdaje na najviše pet godina i može se obnoviti pod istim uvjetima ako tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve. Akreditacijska tijela ukidaju akreditaciju tijela za ocjenjivanje sukladnosti ako ono ne ispunjava, ili je prestalo ispunjavati, uvjete za

[16] U slučaju europskih normi postupak se provodi preko europskih organizacija za normizaciju i potvrđuje ga Europska komisija objavom u Službenom listu (vidjeti Uredbu 1025/2012).

akreditaciju ili ako se mjerama koje je poduzelo tijelo za ocjenjivanje sukladnosti krši ova Uredba.

U skladu s ovim prijedlogom države članice odgovorne su za zadaće praćenja, nadzora i izvršenja. Države članice morat će osigurati jedno tijelo za nadzor certifikacije. To će tijelo nadzirati usklađenost tijela za ocjenjivanje sukladnosti i certifikate koje izdaju tijela za ocjenjivanje sukladnosti osnovana na njihovu državnom području sa zahtjevima iz ove Uredbe i relevantnim europskim programima za kibersigurnosnu certifikaciju. Nacionalna tijela za nadzor certifikacije bit će nadležna za rješavanje pritužbi fizičkih ili pravnih osoba u vezi s certifikatima koje su izdala tijela za ocjenjivanje sukladnosti na njihovu državnom području. Ona će u određenoj mjeri provoditi istragu predmeta pritužbe i u razumnom roku obavijestiti podnositelja pritužbe o napretku i ishodu istrage. Nadalje, ona će surađivati s drugim tijelima za nadzor certifikacije ili s drugim javnim tijelima, na primjer razmjenom informacija o mogućoj neusklađenosti IKT proizvoda i usluga sa zahtjevima iz ove Uredbe ili s posebnim europskim programima kibersigurnosne certifikacije.

Naposljetku, prijedlogom se uspostavlja Europska skupina za kibersigurnosnu certifikaciju („Skupina”) sastavljena od nacionalnih tijela za nadzor certifikacije iz svih država članica. Glavna je zadaća te Skupine savjetovati Komisiju o pitanjima povezanima s politikom kibersigurnosne certifikacije i surađivati s ENISA-om na razvoju nacrta europskih programa kibersigurnosne certifikacije. ENISA će pomagati Komisiji osiguravanjem tajništva Skupine i vođenjem ažurnog javnog popisa programa koji su odobreni unutar europskog okvira za kibersigurnosnu certifikaciju. ENISA bi se povezala i s normizacijskim tijelima kako bi osigurala primjenu odgovarajućih normi u odobrenim programima i utvrdila područja u kojima su kibersigurnosne norme potrebne.

Europskim okvirom za kibersigurnosnu certifikaciju („Okvir”) osigurat će se koristi za građane i poduzeća, primjerice:

- uspostavom programa za kibersigurnosnu certifikaciju u cijelom EU-u za određene proizvode ili usluge trgovačkim društvima osigurat će se „jedinstvena točka” za kibersigurnosnu certifikaciju u EU-u. Ta trgovačka društva moći će svoj proizvod certificirati samo jednom i dobiti certifikat koji je valjan u svim državama članicama. Ona svoje proizvode neće morati ponovno certificirati kod različitih nacionalnih tijela za certifikaciju. Time će se znatno smanjiti troškovi za trgovačka društva, olakšati prekogranično poslovanje i u konačnici smanjiti i izbjeći rascjepkanost unutarnjeg tržišta predmetnih proizvoda.
- Okvirom se utvrđuje prednost europskih programa kibersigurnosne certifikacije u odnosu na nacionalne programe. U skladu s tim pravilom, donošenjem europskog programa kibersigurnosne certifikacije zamijenit će se svi postojeći usporedni nacionalni sustavi za iste IKT proizvode i usluge na određenoj razini jamstva. Time će se povećati jasnoća i smanjiti trenutačni porast broja nacionalnih programa za kibersigurnosnu certifikaciju koji se preklapaju ili su međusobno proturječni.
- Prijedlogom se podupire i dopunjuje provedba Direktive NIS na način da se poduzećima na koja se primjenjuje Direktiva osigurava vrlo koristan alat za dokazivanje sukladnosti sa zahtjevima mrežne i informacijske sigurnosti u cijeloj Uniji. Pri razvoju novih programa kibersigurnosne certifikacije Komisija i ENISA posebnu će pozornost posvetiti potrebi da osiguraju uključenost zahtjeva mrežne i informacijske sigurnosti u programe kibersigurnosne certifikacije.
- Prijedlogom će se poduprijeti i olakšati razvoj europske politike kibersigurnosti usklađivanjem uvjeta i materijalnih zahtjeva za kibersigurnosnu certifikaciju IKT

proizvoda i usluga u EU-u. U europskim programima kibersigurnosne certifikacije upućivat će se na zajedničke norme ili kriterije za ocjenjivanje i metodologije ispitivanja. Time će se znatno, ali neizravno, pridonijeti prihvaćaju zajedničkih sigurnosnih rješenja u EU-u i istodobno će se ukloniti prepreke na unutarnjem tržištu.

- Okvir je izrađen tako da se njime osigurava nužna fleksibilnost programa kibersigurnosne certifikacije. Ovisno o posebnim kibersigurnosnim potrebama, proizvod ili usluga mogu se certificirati prema višoj ili nižoj razini sigurnosti. Europski programi kibersigurnosne certifikacije bit će osmišljeni uzimajući u obzir tu fleksibilnost, čime će se omogućiti različite razine jamstva (tj. osnovna, znatna ili visoka) i njihova upotreba u različite svrhe ili u različitim kontekstima.
- Svim prethodno navedenim elementima povećat će se privlačnost kibersigurnosne certifikacije za poduzeća kao učinkovitog sredstva za obavješćivanje o razini kibersigurnosnog jamstva za IKT proizvode i usluge. U mjeri u kojoj kibersigurnosna certifikacija postane jeftinija, učinkovitija i komercijalno privlačnija, poduzeća će imati više poticaja za certifikaciju svojih proizvoda od kibersigurnosnih rizika i time će pridonijeti širenju bolje kibersigurnosne prakse u oblikovanju IKT proizvoda i usluga (kibersigurnost u dizajnu).

- **Usklađenost s postojećim odredbama politike u tom području politike**

U skladu s Direktivom NIS, operatori u sektorima koji su ključni za naše gospodarstvo i društvo, primjerice energetika, promet, vodoopskrba, bankarstvo, infrastrukture financijskog tržišta, zdravstvena skrb i digitalna infrastruktura, i pružatelji digitalnih usluga (npr. tražilice, usluge računalstva u oblaku i trgovačka mjesta na internetu) dužni su poduzeti mjere za prikladno upravljanje sigurnosnim rizicima. Novim pravilima u ovom prijedlogu dopunjuju se odredbe Direktive NIS i osigurava se usklađenost s tim odredbama u cilju daljnjeg razvoja kiberotpornosti EU-a jačanjem sposobnosti, suradnje, upravljanja rizikom i kiberosviještenosti.

Nadalje, pravilima o kibersigurnosnoj certifikaciji osigurava se bitan alat za trgovačka društva na koja se primjenjuje Direktiva NIS jer će ona moći certificirati svoje IKT proizvode i usluge u odnosu na kibersigurnosne rizike na temelju programâ kibersigurnosnog certificiranja koji su valjani i priznaju se u cijelom EU-u. Njima će se dopuniti i sigurnosni zahtjevi iz Uredbe o eIDAS-u[17] i Direktive o radijskoj opremi[18].

- **Usklađenost s drugim politikama Unije**

U Uredbi (EU) 2016/679 (Opća uredba o zaštiti podataka, „GDPR”)[19] predviđena je uspostava programa certificiranja te pečata i oznaka za zaštitu podataka za potrebe dokazivanja da su postupci obrade koje obavljaju voditelji ili izvršitelji obrade u skladu s tom

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

[18] Direktiva 2014/53/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ.

[19] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) SL L 119, 4.5.2016., str. 1. – 88.

Uredbom. 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.

Predloženom Uredbom osigurat će se usklađenost s Uredbom 765/2008 o zahtjevima za akreditaciju i nadzor tržišta[20] upućivanjem na pravila iz tog okvira o nacionalnim akreditacijskim tijelima i tijelima za ocjenjivanje sukladnosti. Kada je riječ o nadzornim tijelima, predloženom Uredbom tražit će se od država članica da imenuju nacionalna tijela za nadzor certifikacije koja će biti odgovorna za nadzor, praćenje i izvršavanje pravila. Ta će tijela biti odvojena od tijela za ocjenjivanje sukladnosti kako je propisano Uredbom 765/2008.

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

- **Pravna osnova**

Pravna osnova za djelovanje EU-a je članak 114. Ugovora o funkcioniranju Europske unije (UFEU) koji se odnosi na usklađivanje zakona država članica u cilju ostvarivanja ciljeva članka 26. UFEU-a, odnosno pravilnog funkcioniranja unutarnjeg tržišta.

Pravnu osnovu na unutarnjem tržištu za uspostavu ENISA-e potvrdio je Sud EU-a (u predmetu C-217/04 *Ujedinjena Kraljevina protiv Europskog parlamenta i Vijeća*) i ona je dodatno potvrđena uredbom iz 2013. kojom je utvrđen trenutačni mandat Agencije. Nadalje, aktivnosti usmjerene na jačanje suradnje i koordinacije među državama članicama te aktivnosti kojima se dodaju sposobnosti na razini EU-a za dopunu djelovanja država članica mogu se svrstati u kategoriju „operativne suradnje”. To je posebno utvrđeno Direktivom NIS (za koju je pravna osnova članak 114. UFEU-a) kao cilj koji treba ostvariti u kontekstu mreže CSIRT-ova u kojoj „ENISA osigurava tajništvo i aktivno podržava suradnju” (članak 12. stavak 2.). Konkretno, člankom 12. stavkom 3. točkom (f) dodatno se opisuju različiti oblici operativne suradnje u okviru zadaća mreže CSIRT-ova, među ostalim u odnosu na: i. kategorije rizika i incidenata; ii. rana upozorenja; iii. uzajamnu pomoć i iv. načela i načine koordinacije, kada države članice odgovaraju na prekogranične rizike i incidente.

- Trenutačna rascjepkanost programa certificiranja IKT proizvoda i usluga rezultat je i nepostojanja zajedničkog pravno obvezujućeg i učinkovitog okvirnog postupka koji se primjenjuje na države članice. Time se sprječava stvaranje unutarnjeg tržišta za IKT proizvode i usluge i ugrožava konkurentnost europske industrije u tom sektoru. Ovim prijedlogom nastoji se riješiti postojeća rascjepkanost i s tim povezane prepreke za unutarnje tržište osiguravanjem zajedničkog okvira za uspostavu programa kibersigurnosne certifikacije koji je valjan u cijelom EU-u.

Supsidijarnost (za neisključivu nadležnost)

Načelo supsidijarnosti zahtijeva procjenu nužnosti i dodane vrijednosti djelovanja EU-a. Poštovanje supsidijarnosti u ovom području već je priznato pri donošenju postojeće Uredbe o ENISA-i[21].

---

[20] Uredba (EZ) br. 765/2008 o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93.

[21] 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.

Kibersigurnost je pitanje od zajedničkog interesa za Uniju. Mreže i informacijski sustavi toliko su međusobno ovisni da se pojedinačni akteri (javni i privatni, uključujući građane) često ne mogu sami suočiti s prijetnjama i upravljati rizicima i mogućim učincima kiberincidenata. S druge strane, zbog međuovisnosti država članica, među ostalim u pogledu funkcioniranja ključnih infrastruktura (energetika, promet, vodoopskrba), javna intervencija na europskoj razini nije samo korisna, već i nužna. S druge strane, intervencijom EU-a mogu se ostvariti pozitivni učinci „prelijevanja" zbog razmjene dobre prakse među državama članicama, čime se može povećati kibersigurnost u Uniji.

Ukratko, u sadašnjem kontekstu i ako se razmotre budući scenariji čini se da **odvojena djelovanja država članica EU-a i rascjepkani pristup kibersigurnosti** neće biti dostatni za **povećanje kolektivne kiberotpornosti** Unije.

Smatra se da je djelovanje EU-a nužno i radi smanjenja rascjepkanosti trenutačnih programa kibersigurnosne certifikacije. Time bi se proizvođačima omogućilo da potpuno ostvaruju koristi unutarnjeg tržišta uz znatne uštede u pogledu troškova ispitivanja i redizajniranja. Iako su primjerice trenutačnim sporazumom o uzajamnom priznavanju (MRA) Skupine viših dužnosnika za sigurnost informacijskih sustava (SOG-IS) ostvareni važni rezultati u tom pogledu, sporazum je pokazao i da postoje važna ograničenja zbog kojih nije prikladan da se njime osiguraju dugoročna održiva rješenja za ostvarivanje potpunog potencijala unutarnjeg tržišta.

Dodana vrijednost djelovanja na razini EU-a, posebno za jačanje suradnje među državama članicama, ali i među zajednicama za mrežnu i informacijsku sigurnost, priznata je u Zaključcima Vijeća iz 2016. [22], a razvidna je i iz ocjene ENISA-e.

- **Proporcionalnost**

Predviđenom mjerom ne prelazi se ono što je nužno za ostvarivanje njezinih ciljeva politike. Nadalje, područjem primjene intervencije EU-a ne sprječavaju se daljnje nacionalne mjere povezane s pitanjima nacionalne sigurnosti. Djelovanje EU-a stoga je opravdano na temelju supsidijarnosti i proporcionalnosti.

- **Odabir instrumenta**

Ovim prijedlogom preispituje se Uredba (EU) br. 526/2013 kojom se utvrđuju trenutačni mandat i zadaće ENISA-e. Nadalje, s obzirom na važnu ulogu ENISA-e u uspostavi okvira za kibersigurnosnu certifikaciju EU-a, njezin novi mandat i navedeni okvir najbolje je uspostaviti jednim pravnim instrumentom. Taj će instrument biti uredba.

3. REZULTATI EX - POST EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENE UČINAKA

***Ex post* evaluacije / provjere primjerenosti postojećeg zakonodavstva**

Komisija je, u skladu s planom evaluacije[23], ocijenila **relevantnost, učinak, djelotvornost, učinkovitost, usklađenost i dodanu vrijednost** Agencije s obzirom na njezinu uspješnost, upravljanje, unutarnje ustrojstvo i način rada u razdoblju od 2013. do 2016. Glavni zaključci

[22] Zaključci Vijeća o jačanju europskog sustava kiberotpornosti i poticanju konkurentne i inovativne industrije kibersigurnosti – 15. studenoga 2016.

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

mogu se sažeti kako slijedi (više informacija navedeno je u radnom dokumentu službi Komisije na tu temu koji je priložen procjeni učinka).

- **Relevantnost:** u kontekstu tehnološkog razvoja i rastućih prijetnji te uzimajući u obzir znatnu potrebu za pojačanom kibersigurnošću u EU-u, pokazalo se da su ciljevi ENISA-e relevantni. Države članice i tijela EU-a oslanjaju se na njezinu stručnost u području kibersigurnosti. Nadalje, u državama članicama potrebno je jačati kapacitete za bolje razumijevanje prijetnji i za odgovor na prijetnje, a dionici moraju surađivati u svim tematskim područjima i sa svim institucijama. Kibersigurnost je i dalje ključan politički prioritet EU-a i očekuje se da će ENISA na njega odgovoriti. Međutim, budući da je ENISA agencija EU-a ograničenog mandata: i. nije moguće dugoročno planiranje i održiva potpora državama članicama i institucijama EU-a; ii. to može dovesti do pravnog vakuuma jer su odredbe Direktive NIS kojom se ENISA-i povjeravaju njezine zadaće trajne prirode[24]; iii. nije usklađena s vizijom kojom se ENISA povezuje se pojačanim kibersigurnosnim ekosustavom EU-a.
- **Djelotvornost**: ENISA je u načelu ispunila svoje ciljeve i izvršila svoje zadaće. Pridonijela je većoj mrežnoj i informacijskoj sigurnosti u Europi s pomoću svojih glavnih aktivnosti (jačanje kapaciteta, pružanje stručnosti, izgradnja zajedništva i potpora politici). Međutim, potencijal za unaprjeđenje postoji u svim područjima. Zaključak je evaluacije da je ENISA doista stvorila snažne i pouzdane odnose s nekima od svojih dionika, posebno s državama članicama i zajednicom CSIRT-ova. Intervencije u području jačanja kapaciteta pokazale su se djelotvornima, posebno za države članice s manje resursa. Jedno od istaknutih područja bilo je poticanje široke suradnje i svi su se dionici složili da tu ENISA ima pozitivnu ulogu. Međutim, ENISA se suočila s teškoćama u pokušaju da postigne veliki učinak u golemom području mrežne i informacijske sigurnosti. Jedan je od razloga i to što je za izvršavanje vrlo širokog mandata raspolagala prilično ograničenim ljudskim i financijskim resursima. Zaključak je evaluacije i da je ENISA djelomično ispunila cilj pružanja stručnog znanja povezanog s problemima zapošljavanja stručnjaka (vidjeti u nastavku u odjeljku o učinkovitosti).
- **Učinkovitost**: unatoč malom proračunu, koji je među najnižima u usporedbi s drugim agencijama EU-a, Agencija je uspjela pridonijeti ciljevima te je učinkovito upotrebljavala resurse. Zaključak je evaluacije da su postupci općenito bili učinkoviti te da je jasnom podjelom odgovornosti u organizaciji omogućeno uspješno obavljanje poslova. Jedan od glavnih izazova učinkovitosti Agencije povezan je s problemima s kojima se ENISA suočava pri zapošljavanju i zadržavanju visokokvalificiranih stručnjaka. Nalazi pokazuju da se to može objasniti kombinacijom čimbenika, među ostalim općenitim teškoćama javnog sektora kada se natječe s privatnim sektorom u zapošljavanju visokokvalificiranih stručnjaka, vrstom ugovora (na određeno vrijeme) koje je Agencija mogla ponuditi i niskom razinom privlačnosti lokacije ENISA-e, što je primjerice povezano s teškoćama s kojima se suočavaju bračni partneri pri pronalaženju posla. Zbog dvije lokacije u Ateni i Heraklionu bili su potrebni dodatni koordinacijski napori i nastajali su dodatni troškovi, ali preseljenjem glavnog operativnog odjela Agencije u Atenu 2013. povećala se operativna učinkovitost Agencije.

[24] Upućivanje na članke 7., 9., 11., 12. 19. Direktive o sigurnosti mrežnih i informacijskih sustava (Direktiva NIS).

- **Usklađenost**: Aktivnosti ENISA-e bile su u načelu u skladu s politikama i aktivnostima njezinih dionika, na nacionalnoj razini i razini EU-a, ali potreban je koordiniraniji pristup kibersigurnosti na razini EU-a. Nije potpuno iskorištena mogućnost suradnje između ENISA-e i ostalih tijela EU-a. Zbog razvoja pravnog i političkog okruženja u EU-u trenutačni mandat danas je manje usklađen.
- **Dodana vrijednost EU-a**: Dodana vrijednost ENISA-e poglavito proizlazi iz sposobnosti Agencije da pojača suradnju, uglavnom među državama članicama, ali i s povezanim zajednicama mrežne i informacijske sigurnosti. Na razini EU-a ne postoji nijedan drugi akter koji podupire suradnju toliko velikog broja dionika u području mrežne i informacijske sigurnosti. Dodana vrijednost Agencije razlikovala se prema različitim potrebama i resursima njezinih dionika (npr. velike u odnosu na male države članice; države članice u odnosu na industriju) i potrebi Agencije da daje prednost svojim aktivnostima u skladu s programom rada. Zaključak je evaluacije da bi moguće ukidanje ENISA-e značilo izgubljene prilike za sve države članice. Neće se moći osigurati jednaki stupanj jačanja zajedništva i suradnje među državama članicama u području kibersigurnosti. Bez centralizirane agencije EU-a povećala bi se rascjepkanost, a praznina koja bi ostala nakon ENISA-e morala bi se popuniti bilateralnom ili regionalnom suradnjom.

Uzimajući u obzir prethodne rezultate ENISA-e i budućnost, glavni trendovi koji proizlaze iz savjetovanja iz 2017. jesu sljedeći[25]:

- Većina ispitanika (74 %) pozitivno je ocijenila rad ENISA-e u razdoblju od 2013. do 2016. Nadalje, većina ispitanika smatrala je da ENISA ostvaruje svoje različite ciljeve (barem 63 % za svaki cilj). Približno pola ispitanika (46 %) redovito (mjesečno ili češće) koristi se uslugama i proizvodima ENISA-e i te su usluge i proizvodi cijenjeni jer ih pruža tijelo na razini EU-a (83 %) i zbog njihove kvalitete (62 %).
- Ispitanici su utvrdili niz nedostataka i izazova za budućnost kibersigurnosti u EU-u, a glavnih pet (na popisu od 16) bili su posebno sljedeći: suradnja među državama članicama; kapacitet za sprječavanje, otkrivanje i rješavanje kibernapada velikih razmjera; suradnja među državama članicama u područjima povezanima s kibersigurnošću; suradnja i razmjena informacija među različitim dionicima, uključujući javno-privatnu suradnju; zaštita ključne infrastrukture od kibernapada.
- Velika većina (88 %) ispitanika smatrala je da trenutačni instrumenti i mehanizmi koji su dostupni na razini EU-a nisu dostatni ili su samo djelomično prikladni za njihovo rješavanje. Velika većina ispitanika (98 %) navela je da bi na te potrebe trebalo odgovoriti tijelo EU-a, a 99 % ispitanika smatralo je da to tijelo treba biti ENISA.

[25] Na savjetovanje je odgovorilo 90 dionika iz 19 država članica (88 odgovora i 2 stajališta), uključujući nacionalna tijela iz 15 država članica uključujući Francusku, Italiju, Irsku i Grčku i 9 krovnih organizacija koje predstavljaju znatan broj europskih organizacija, na primjer Europsko udruženje banaka, Digitalna Europa (koja predstavlja digitalnu industriju u Europi), Udruženje europskih operatora telekomunikacijskih mreža (ETNO). Javno savjetovanje o ENISA-i dopunjeno je iz nekoliko drugih izvora, uključujući sljedećim: i. detaljnim razgovorima s približno 50 ključnih dionika u zajednici kibersigurnosti; ii. anketom u mreži CSIRT-ova; iii. anketom provedenom u upravnom i izvršnom odboru ENISA-e i u Stalnoj interesnoj skupini.

Savjetovanja s dionicima

- Komisija je organizirala javno savjetovanje za preispitivanje rada ENISA-e od 12. travnja do 5. srpnja 2016. i zaprimila je 421 odgovor[26]. Rezultati pokazuju da je 67,5 % ispitanika izrazilo stajalište da bi ENISA mogla imati ulogu u uspostavi usklađenog okvira za sigurnosno certificiranje IKT proizvoda i usluga.

Rezultati savjetovanja o kibersigurnosti cPPP-a[27] u odjeljku o certificiranju pokazuju sljedeće:

- 50,4 % (tj. 121 od 240) ispitanika ne zna priznaju li se nacionalni programi certificiranja uzajamno među državama članicama EU-a. 25,8 % (62 od 240) odgovorilo je „ne”, a 23,8 % (57 od 240) odgovorilo je „da”,
- 37,9 % ispitanika (91 od 240) smatra da postojeći programi certificiranja ne zadovoljavaju potrebe europske industrije. S druge strane, 17,5 % (42 od 240), većinom globalna trgovačka društava koja posluju na europskom tržištu, izrazilo je suprotno stajalište,
- 49,6 % (119 od 240) ispitanika kaže da nije lako dokazati jednakovrijednost normi, programa certificiranja i oznaka. 37,9 % (91 od 240) odgovorilo je „ne znam”, a 12,5 % (30 od 240) odgovorilo je „da”.

Prikupljanje i primjena stručnog znanja

Komisija se oslanjala na sljedeće vanjske stručne savjete:

- Studija o ocjenjivanju ENISA-e (Ramboll/Carsa 2017., SMART br. 2016/0077),
- Studija o sigurnosnom certificiranju i označavanju u području IKT-a – prikupljanje dokaza i procjena učinka (PriceWaterhouseCoopers 2017., SMART br. 2016/0029).

Procjena učinka

- U izvješću o procjeni učinka ove inicijative utvrđeni su sljedeći glavni problemi koje treba riješiti:
- rascjepkanost politika i pristupa kibersigurnosti u državama članicama,
- raspršeni resursi i rascjepkanost pristupâ kibersigurnosti u institucijama, agencijama i tijelima EU-a i
- nedostatna osviještenost i informiranost građana i poduzeća u kombinaciji sa sve većim brojem višestrukih nacionalnih i sektorskih programa certificiranja.

U izvješću su ocijenjene sljedeće mogućnosti u pogledu mandata ENISA-e:

- očuvanje *statusa quo*, koja uključuje prošireni mandat koji je i dalje ograničenog trajanja (osnovna mogućnost),
- istek trenutačnog mandata ENISA-e bez obnove i ukidanje ENISA-e (bez intervencije politike),

[26] 162 doprinosa građana, 33 doprinosa civilnog društva i organizacija potrošača; 186 doprinosa industrije i 40 doprinosa javnih tijela, uključujući nadležna tijela koja provode Direktivu o e-privatnosti.

[27] Na odjeljak o certificiranju odgovorilo je 240 dionika iz nacionalnih javnih uprava, velikih poduzeća, MSP-ova, mikropoduzeća i istraživačkih tijela.

- „reformirana ENISA” i
- agencija EU-a za kibersigurnost s potpunim operativnim sposobnostima.

U izvješću su ocijenjene sljedeće mogućnosti u pogledu kibersigurnosne certifikacije:

- nepoduzimanje intervencije u području politike (osnovna mogućnost),
- nezakonodavne („pravno neobvezujuće”) mjere,
- zakonodavni akt EU-a kojim će se stvoriti obvezni sustav za sve države članice na temelju sustava SOG-IS-a i
- i opći okvir EU-a za kibersigurnosnu certifikaciju u području IKT-a.

Na temelju analize donesen je zaključak da je „reformirana ENISA” u kombinaciji s općim okvirom EU-a za kibersigurnosnu certifikaciju u području IKT-a najprihvatljivija opcija.

Ocijenjeno je da je ta opcija najučinkovitije rješenje s pomoću kojeg EU može ostvariti sljedeće utvrđene ciljeve: jačanje kibersigurnosnih sposobnosti, pripravnosti, suradnje, osviještenosti, transparentnosti i izbjegavanje rascjepkanosti tržišta. Ocijenjeno je da je ta opcija ujedno i najusklađenija s prioritetima politike iz strategije EU-a za kibersigurnost i povezanih politika (npr. Direktive NIS) i strategijom jedinstvenog digitalnog tržišta. Osim toga, tijekom savjetodavnog postupka pokazalo se da ta opcija uživa potporu većine dionika. Nadalje, analiza provedena u okviru procjene učinka pokazala je da ta opcija omogućuje ostvarivanje ciljeva iskorištavanjem razumne količine resursa.

Komisijin Odbor za regulatorni nadzor prvo je 24. srpnja dao negativno mišljenje, a 25. kolovoza 2017. nakon ponovnog podnošenja pozitivno mišljenje. Izmijenjeno izvješće o procjeni učinka sadržavalo je dodatne dokaze, konačne zaključke evaluacije ENISA-e i dodatna pojašnjenja opcija politike i njihovih učinaka. U prilogu 1. završnom izvješću o procjeni učinka sažeto se opisuje kako su napomene Odbora iz drugog mišljenja uzete u obzir. Konkretno, izvješće je ažurirano kako bi se iscrpnije opisao kibersigurnosni kontekst EU-a, uključujući mjere iz zajedničke komunikacije „Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a” (JOIN(2017) 450) koje su posebno relevantne za ENISA-u: EU-ov plan za kibersigurnost i Europski centar za istraživanje i stručnost u području kibersigurnosti, s kojima bi Agencija povezivala svoje preporuke u pogledu istraživačkih potreba EU-a.

U izvješću se objašnjava kako bi se reformom Agencije, uključujući nove zadaće, bolje uvjete zaposlenja i strukturnu suradnju s tijelima EU-a u tom području, poboljšala njezina privlačnost kao poslodavca i pridonijelo rješavanju problema povezanih sa zapošljavanjem stručnjaka. Prilog 6. izvješću sadržava i revidiranu procjenu troškova povezanih s opcijama politike za ENISA-u. Kada je riječ o certifikaciji, izvješće je revidirano kako bi se najprihvatljivija opcija iscrpnije pojasnila, među ostalim i grafičkim prikazom, te kako bi se uključile procjene troškova koje bi države članice i Komisija snosili u vezi s tim novim okvirom certifikacije. Razlozi odabira ENISA-e kao ključnog aktera u tom okviru dodatno su poduprti njezinom stručnošću u tom području i činjenicom da je ENISA jedina agencija na razini EU-a koja se bavi kibersigurnošću. Konačno, revidirani su odjeljci koji se odnose na certifikaciju kako bi se razjasnile razlike između postojećeg sustava SOG-IS i prednosti različitih opcija politike te objasnilo da će vrsta IKT proizvoda i usluge obuhvaćena europskim programom certifikacije biti definirana u okviru samog odobrenog programa.

Primjerenost propisa i pojednostavnjivanje

Nije primjenjivo

Utjecaj na temeljna prava

Kibersigurnost ima bitnu ulogu u zaštiti privatnosti i osobnih podataka građana u skladu s člancima 7. i 8. Povelje Europske unije o temeljnim pravima. U slučaju kiberincidenata jasno je da su izloženi privatnost i zaštita naših osobnih podataka. Kibersigurnost je stoga nužan preduvjet za poštovanje privatnosti i povjerljivosti naših osobnih podataka. U tom kontekstu, prijedlogom, čiji je cilj pojačati kibersigurnost u Europi, osigurava se važna dopuna postojećem zakonodavstvu u zaštiti temeljnih prava na privatnost i osobne podatke. Kibersigurnost je od ključne važnosti i za zaštitu povjerljivosti naše elektroničke komunikacije i za ostvarivanje slobode izražavanja i informiranja i ostalih povezanih prava, poput slobode mišljenja, savjesti i vjeroispovijedi.

4. UTJECAJ NA PRORAČUN

Vidi financijski plan

5. OSTALI ELEMENTI

- **Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja**

Komisija će pratiti primjenu Uredbe i svakih pet godina podnosit će izvješće o njezinoj evaluaciji Europskom parlamentu i Vijeću te Europskom gospodarskom i socijalnom odboru. Ta će izvješća biti javna i sadržavat će detaljni opis primjene i izvršenja ove Uredbe.

- **Detaljno obrazloženje pojedinih odredbi prijedloga**

Glava I. Uredbe sadržava opće odredbe: predmet (članak 1.), definicije (članak 2.), uključujući upućivanja na relevantne definicije iz drugih instrumenata EU-a, na primjer iz Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (Direktiva NIS), Uredbe (EZ) br. 765/2008 Europskog parlamenta i Vijeća o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 i Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća o europskoj normizaciji.

Glava II. Uredbe sadržava ključne odredbe o ENISA-i, agenciji EU-a za kibersigurnost.

U poglavlju I. te glave opisan je mandat (članak 3.), ciljevi (članak 4.) i zadaće Agencije (članci od 5. do 11.)

U poglavlju II. opisano je ustrojstvo ENISA-e i navode se ključne odredbe o njezinoj strukturi (članak 12.). Njime su obuhvaćeni sastav, pravila glasovanja i funkcije Upravljačkog odbora (odjeljak 1., članci od 13. do 17.), Izvršnog odbora (odjeljak 2. članak 18.) i izvršnog direktora (odjeljak 3. članak 19.). Ono uključuje i odredbe o sastavu i ulozi Stalne interesne skupine (odjeljak 4. članak 20.). I naposljetku, u odjeljku 5. tog poglavlja navedena su operativna pravila Agencije, među ostalim u pogledu programiranja njezinih operacija, sukoba interesa, transparentnosti, povjerljivosti i pristupa dokumentima (članci od 21. do 25.).

Poglavlje III. odnosi se na uspostavu i strukturu proračuna Agencije (članci 26. i 27). te na pravila o njegovoj provedbi (članci 28. i 29.). Uključuje i odredbe kojima se olakšava borba protiv prijevara, korupcije i ostalih nezakonitih aktivnosti (članak 30.).

Poglavlje IV. odnosi se na zaposlenike Agencije. Ono uključuje odredbe o Pravilniku o osoblju i uvjetima zaposlenja te pravila o povlasticama i imunitetima (članci 31. i 32.). U

njemu su također detaljno opisana pravila mandata i imenovanja izvršnog direktora Agencije (članak 33.). I na kraju, ali ne najmanje važno, ono uključuje odredbe o angažmanu upućenih nacionalnih stručnjaka ili drugih zaposlenika koji nisu zaposleni u Agenciji (članak 34.).

Naposljetku, poglavlje V. sadržava opće odredbe o Agenciji. U njemu je opisan pravni položaj (članak 35.) i uključuje odredbe kojima se uređuju pitanja odgovornosti, jezika, zaštite osobnih podataka (članci od 36. do 38.) te sigurnosna pravila o zaštiti klasificiranih i osjetljivih neklasificiranih podataka (članak 40.). U njemu su opisana pravila kojima se uređuje suradnja Agencije s trećim zemljama i međunarodnim organizacijama (članak 39.). I konačno, ali ne najmanje važno, ono sadržava odredbe o sjedištu Agencije i uvjetima rada te o administrativnom nadzoru koji provodi Europski ombudsman (članci 41. i 42.).

Glavom III. Uredbe uspostavlja se europski okvir za kibersigurnosnu certifikaciju („**Okvir**”) za IKT proizvode i usluge kao *lex generalis* (članak 1.). Definira se opća svrha europskih programa kibersigurnosne certifikacije, tj. osiguranje usklađenosti IKT proizvoda i usluga s određenim kibersigurnosnim zahtjevima u pogledu njihove sposobnosti, na određenoj razini jamstva, da se odupru djelovanju kojim se ugrožava dostupnost, izvornost, cjelovitost ili povjerljivost pohranjenih, poslanih ili obrađenih podataka ili povezanih funkcija ili usluga (članak 43.). Nadalje, navode se sigurnosni ciljevi koji se nastoje ostvariti europskim programima kibersigurnosne certifikacije (članak 45.), na primjer sposobnost zaštite podataka od slučajnog ili neovlaštenog pristupa ili otkrivanja, uništavanja ili mijenjanja i sadržaj (tj. elementi) europskih programa kibersigurnosne certifikacije, na primjer detaljni opis njihova područja primjene, sigurnosnih ciljeva, kriterija za ocjenjivanje itd. (članak 47.).

Glavom III. utvrđuju se i glavni pravni učinci europskih programa kibersigurnosne certifikacije, odnosno i. obveza provođenja programa na nacionalnoj razini i dobrovoljna priroda certificiranja; ii. učinak poništavanja koji europski programi kibersigurnosne certifikacije imaju u odnosu na nacionalne programe koji se odnose na isti proizvod ili usluge (članci 48. i 49.).

Tom glavom dodatno se propisuje postupak za donošenje europskih programa kibersigurnosne certifikacije i uloge Komisije, ENISA-e i Europske skupine za kibersigurnosnu certifikaciju – „Skupina” – (članak 44.). Naposljetku, u toj glavi utvrđuju se odredbe o tijelima za ocjenjivanje sukladnosti, među ostalim o njihovim zahtjevima, ovlastima i zadaćama, nacionalnim tijelima za nadzor certifikacije i o kaznama.

U toj glavi „Skupina” se uspostavlja i kao osnovno tijelo koje se sastoji od predstavnika nacionalnih tijela za nadzor certifikacije čija je glavna funkcija surađivati s ENISA-om na izradi europskih programa kibersigurnosne certifikacije i savjetovati Komisiju o općim i posebnim pitanjima povezanima s politikom kibersigurnosne certifikacije.

Glava IV. Uredbe uključuje završne odredbe u kojima se opisuje delegiranje, zahtjevi za ocjenjivanje, stavljanje izvan snage i nasljeđivanje te stupanje na snagu.

2017/0225 (COD)

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”)

(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[28],

uzimajući u obzir mišljenje Odbora regija[29],

u skladu s redovnim zakonodavnim postupkom,

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 donose 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,

[28] SL C , , str...
[29] SL C , , str...

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 kiberprijetnji 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 ocjenjivanje na svim nacionalnim tržištima i u svim sektorima.

(6) Europski parlament i Vijeće donijeli su 2004. Uredbu (EZ) br. 460/2004[30] o osnivanju Europske agencije za mrežnu i informacijsku sigurnost kako bi pridonijeli ciljevima osiguravanja visoke razine mrežne i informacijske sigurnosti u Uniji i 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[31] o produljenju mandata Agencije do ožujka 2012. Uredbom (EZ) br. 580/2011[32] produljen je mandat Agencije do 13. rujna 2013. Europski parlament i Vijeće donijeli su 2013. Uredbu (EU) br. 526/2013[33] o ENISA-i i stavljanju izvan snage Uredbe (EZ) br. 460/2004, kojom je mandat Agencije proširen do lipnja 2020.

---

30 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.).

31 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 njenog trajanja (SL L 293, 31.10.2008., str. 1.).

32 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 njenog trajanja (SL L 165, 24.6.2011., str. 3.).

33 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 pri obavljanju svojih zadaća trebala proaktivno pridonositi nacionalnim naporima i naporima Unije u potpunoj suradnji s institucijama, tijelima, uredima i agencijama Unije i 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 reviziju politike i zakonodavstva u području kibersigurnosti, uključujući zaštitu kritične informacijske infrastrukture i kiberotpornost. 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, tijelima, uredima i agencijama Unije u njihovim naporima usmjerenima na izgradnju i jačanje sposobnosti i pripravnosti u cilju sprječavanja i otkrivanja problema i incidenata u području kibersigurnosti i odgovaranja 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. Agencija bi trebala pomagati i u razvoju i ažuriranju strategija Unije i država članica o sigurnosti mrežnih i informacijskih sustava, posebno o kibersigurnosti, promicati njihovo širenje i pratiti napredak u njihovoj provedbi. 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, posebno radi potpore zaštiti ključnih infrastruktura, Agencija bi trebala olakšati uspostavu sektorskih centara za razmjenu informacija i analizu (ISAC-ovi) pružanjem najbolje prakse i smjernica o dostupnim alatima i postupcima te davanjem smjernica o rješavanju regulatornih pitanja povezanih s razmjenom informacija.

(18) Agencija bi trebala objedinjavati i analizirati nacionalna izvješća CSIRT-ova i CERT-EU-a utvrđivanjem zajedničkih pravila, 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 stvaranjem mreže CSIRT-ova.

(19) Agencija bi trebala pridonijeti odgovoru na razini EU-a u slučaju prekograničnih kiberincidenata i kiberkriza velikih razmjera. Ta funkcija trebala 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 postupak ispitivanjem načina takve suradnje s pomoću godišnjih vježbi u području kibersigurnosti.

(20) Agencija bi pri izvršavanju svojih operativnih zadaća trebala iskoristiti dostupnu stručnost CERT-EU-a u okviru strukturirane suradnje, u velikoj fizičkoj blizini. Strukturiranom suradnjom olakšat će se nužne sinergije i prikupljanje stručnog znanja ENISA-e. Prema potrebi trebalo bi definirati odgovarajuće posebne mehanizme između dvije organizacije kojima će se utvrditi praktična provedba takve suradnje.

(21) U skladu sa svojim operativnim zadaćama Agencija bi trebala moći pružiti potporu državama članicama, na primjer pružanjem savjeta ili tehničke pomoći, ili osiguravanjem analiza prijetnji i incidenata. 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 promptno razmjenjuju informacije o velikim incidentima i krizama u području kibersigurnosti. Takvim informacijama trebalo bi se dodatno pomoći ENISA-i pri izvršavanju operativnih zadaća.

(22) U okviru redovne suradnje na tehničkoj razini u cilju podupiranja informiranosti o stanju u Uniji, Agencija bi trebala redovito 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 (dobrovoljno) ili jedinstvene kontaktne točke iz Direktive NIS, Europski centar za kiberkriminal (EC3) pri Europolu, CERT-EU i, prema potrebi, Centar EU-a za analizu obavještajnih podataka (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) *Ex-post* tehničke istrage incidenata sa značajnim učinkom u više država članica koje Agencija podupire ili provodi na zahtjev, ili uz suglasnost, pogođenih država članica trebale bi biti usmjerene na sprječavanje budućih incidenata i provoditi se ne dovodeći u pitanje sudske ili upravne postupke za utvrđivanje krivnje ili odgovornosti.

(24) Pogođene države članice trebale bi Agenciji pružiti nužne informacije i pomoć za potrebe istrage ne dovodeći u pitanje članak 346. Ugovora o funkcioniranju Europske unije ili druge razloge javne politike.

(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 ona bi trebala, u suradnji s državama članicama i, prema potrebi, s tijelima za statistiku i drugim tijelima, prikupljati relevantne informacije i provoditi analize novih tehnologija te davati posebne 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 pomoći državama članicama i institucijama, agencijama i tijelima Unije da prepoznaju nove prijetnje i spriječe probleme povezane s kibersigurnošću.

(27) U cilju povećanja otpornosti Unije Agencija bi trebala razvijati izvrsnost u području sigurnosti internetske infrastrukture i ključnih infrastruktura pružanjem savjeta, smjernica i najbolje prakse. 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 pridonijeti 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 pridonositi i promicanju najbolje prakse i rješenja na razini građana 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. Agencija bi, nadalje, u suradnji s državama članicama i institucijama, tijelima, uredima i agencijama Unije trebala organizirati redovite kampanje informiranja i obrazovanja krajnjih korisnika s ciljem poticanja sigurnijeg ponašanja pojedinaca na internetu, podizanja razine osviještenosti o potencijalnim opasnostima u kiberprostoru, uključujući kiberkriminalitet 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 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 se osiguralo da Agencija potpuno ostvari svoje ciljeve, ona bi se trebala povezati s relevantnim institucijama, agencijama i tijelima, među ostalim s CERT-EU-om, Europskim centrom za kiberkriminal (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) 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, kao članica koja osigurava i tajništvo mreže CSIRT-ova, trebala bi podupirati CSIRT-ove u državama članicama i CERT-EU u operativnoj suradnji u skladu sa 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 godišnje vježbe u području kibersigurnosti na razini Unije i 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 tekuće aktivnosti istraživanja, razvoja i tehnološkog ocjenjivanja, posebno one aktivnosti koje provode različite istraživačke inicijative Unije kako bi institucije tijela, urede i agencije Unije i, prema potrebi, države članice, na njihov zahtjev savjetovala o potrebama za istraživanjem u području mrežne i informacijske sigurnosti, posebno kibersigurnosti.

(37) Problemi kibersigurnosti globalni su problemi. Potrebna je i bliža međunarodna suradnja radi unaprjeđenja sigurnosnih standarda, uključujući definiciju zajedničkih normi ponašanja i kodeksa 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 trebala, pružanjem, prema potrebi, potrebnog stručnog znanja i analize relevantnim institucijama, tijelima, uredima i agencijama Unije, podupirati daljnje uključivanje Unije i 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, ocjenama 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 koje se dostavlja 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[34]. 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[35]. 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.

(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) Ocjenjivanje sukladnosti postupak je kojim se dokazuje da su ispunjeni određeni zahtjevi koji se odnose na proizvod, postupak, uslugu, sustav, osobu ili tijelo. Za potrebe ove Uredbe certifikacija bi se trebala smatrati vrstom ocjenjivanja sukladnosti u pogledu kibersigurnosnih značajki proizvoda, postupka, usluge, sustava ili njihove kombinacije („IKT proizvodi i usluge”) koju obavlja neovisna treća strana koja nije proizvođač proizvoda ili pružatelj usluge. Samom 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.

(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.

(49) U Komunikaciji iz 2016. „Jačanje europskog sustava kibernetičke sigurnosti i poticanje konkurentne i inovativne industrije kibernetičke sigurnosti” Komisija je istaknula potrebu za visokokvalitetnim, povoljnim i interoperabilnim proizvodima i

---

34 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.).

35 SL L 8, 12.1.2001., str. 1.

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 rascjepkanosti kibersigurnosnog tržišta.

(50) Trenutačno se kibersigurnosna certifikacija IKT 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 je sporazum o uzajamnom priznavanju SOG-IS-a najvažniji model suradnje i uzajamnog priznavanja u području sigurnosnog certificiranja, s njim su povezani znatni nedostaci koji se odnose na visoke troškove i ograničeno područje primjene. Dosad je razvijeno samo nekoliko profila zaštite digitalnih proizvoda, na primjer digitalni potpis, digitalni tahograf i pametne kartice. Najvažnije je napomenuti da 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 buduće europske programe kibersigurnosne certifikacije koji omogućuju priznavanje i uporabu certifikata IKT proizvoda i usluga u svim državama članicama. Europski okvir trebao bi imati dvostruku svrhu: s jedne strane njime bi se trebalo pridonijeti 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. Programi certificiranja trebali bi biti nediskriminirajući i temeljiti se na međunarodnim normama ili normama Unije, 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 proizvoda i usluga. Programe bi trebala

provoditi i nadzirati nacionalna tijela za nadzor certifikacije, a certifikati izdani na temelju 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) Europskim programima kibersigurnosne certifikacije trebalo bi se osigurati da proizvodi i usluge koji su certificirani u skladu s takvim programom zadovoljavaju određene zahtjeve. Ti zahtjevi odnose se na mogućnost odupiranja, na određenoj razini jamstva, djelovanjima kojima bi se mogla ugroziti dostupnost, izvornost, cjelovitost ili povjerljivost pohranjenih, poslanih ili obrađenih podataka ili povezanih funkcija ili usluge koje se nude s pomoću tih proizvoda, postupaka, usluga i sustava ili kojima se s pomoću njih može pristupiti u smislu ove Uredbe. U ovoj Uredbi ne mogu se podrobno utvrditi kibersigurnosni zahtjevi povezani sa svim IKT proizvodima i uslugama. IKT 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. Načina postizanja tih ciljeva u određenim IKT proizvodima i uslugama trebalo bi potom podrobnije opisati na razini pojedinačnog programa certificiranja kojeg je donijela Komisija, na primjer upućivanjem na norme ili tehničke specifikacije.

(56) Komisija bi trebala imati ovlasti zatražiti od ENISA-e da izradi prijedloge programa za određene IKT 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 proizvoda i usluga, detaljnu specifikaciju kibersigurnosnih zahtjeva, na primjer upućivanjem na norme ili tehničke specifikacije, posebne kriterije i metode ocjenjivanja i predviđenu razinu jamstva: osnovna, znatna i/ili visoka.

(57) Primjena europske kibersigurnosne certifikacije trebala bi biti dobrovoljna, osim ako je u zakonodavstvu Unije ili nacionalnom zakonodavstvu predviđeno drugačije. Međutim, kako bi se ostvarili ciljevi ove Uredbe i izbjegla rascjepkanost unutarnjeg tržišta, nacionalni programi kibersigurnosne certifikacije ili postupci 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.

(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 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) Od svih država članica treba tražiti da imenuju jedno tijelo za nadzor kibersigurnosne certifikacije koje će nadzirati usklađenost tijela za ocjenjivanje sukladnosti i certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovom državnom području sa zahtjevima iz ove Uredbe i s relevantnim programima kibersigurnosne certifikacije. Nacionalna tijela za nadzor certifikacije trebala bi rješavati pritužbe fizičkih ili pravnih osoba u pogledu certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovu državnom području, 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 nadzor certifikacije 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 nacionalnih tijela za nadzor certifikacije. 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 Komisiji o održavanju i preispitivanju postojećih europskih programa kibersigurnosne certifikacije.

(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.

(62) Potpora Agencije kibersigurnosnoj certifikaciji trebala bi uključivati i povezivanje s Odborom Vijeća za sigurnost i odgovarajućim nacionalnim tijelom u pogledu kriptografskog odobravanja proizvoda koji će se upotrebljavati u zaštićenim mrežama.

(63) Kako bi se dodatno utvrdili kriteriji za akreditaciju tijela za ocjenjivanje sukladnosti, ovlast donošenja akata u skladu s člankom 290. Ugovora o funkcioniranju Europske unije treba prenijeti na Komisiju. Komisija bi tijekom svojeg pripremnog rada trebala provoditi odgovarajuća savjetovanja, uključujući i savjetovanje sa stručnjacima. Savjetovanja bi trebalo provoditi u skladu s načelima propisanima u

Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016. Kako bi se osiguralo ravnopravno sudjelovanje u izradi delegiranih akata, Europski parlament i Komisija trebali bi sve dokumente zaprimiti istodobno kada i stručnjaci država članica, a njihovi stručnjaci trebali bi sustavno imati pristup sastancima skupina stručnjaka Komisije koje se bave izradom delegiranih akata.

(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 koristiti za donošenje provedbenih akata o europskim programima kibersigurnosne certifikacije za IKT proizvode i usluge; o načinima provođenja istraga Agencije te o okolnostima, formatima i postupcima u skladu s kojima nacionalna tijela za nadzor certifikacije Komisiji dostavljaju obavijesti o akreditiranim tijelima za ocjenjivanje sukladnosti.

(66) Rad Agencije trebao bi se ocjenjivati neovisno. Ocjenjivanjem bi trebalo uzeti u obzir ostvaruje li Agencija svoje ciljeve, njezin način rada i relevantnost njezinih zadaća. Ocjenjivanjem bi trebalo procijeniti i učinak, djelotvornost i učinkovitost europskog okvira za kibersigurnosno certificiranje.

(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:

NASLOV I.
OPĆE ODREDBE

Članak 1.
Predmet i područje primjene

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 EU-a za kibersigurnost), dalje u tekstu „Agencija”; i

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

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 negativno utjecati na mrežne i informacijske sustave, njihove korisnike i uključene osobe.

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

(10) „europski kibersigurnosni certifikat” znači dokument koji izdaje tijelo za ocjenjivanje sukladnosti kojim se potvrđuje da IKT proizvod ili usluga ispunjavaju određene zahtjeve utvrđene u europskom programu kibersigurnosne certifikacije;

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

(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.

GLAVA II.
ENISA – „Agencija EU-a za kibersigurnost”

POGLAVLJE I.
MANDAT, CILJEVI I ZADAĆE

Članak 3.
Mandat

1. Agencija obavlja zadaće koje su joj dodijeljene ovom Uredbom kako bi pridonijela ostvarivanju visoke razine kibersigurnosti u Uniji.

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.

3. Ciljevima i zadaćama Agencije ne dovode se u pitanje nadležnosti država članica u pogledu kibersigurnosti ni aktivnosti koje se odnose na javnu sigurnost, obranu, nacionalnu sigurnost i aktivnosti države u područjima kaznenog prava.

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 povezanih s kibersigurnošću.

3. Agencija podupire jačanje kapaciteta i pripravnosti u cijeloj Uniji na način da Uniji, državama članicama i javnim i privatnim dionicima pomaže da povećaju zaštitu svojih mrežnih i informacijskih sustava, razviju vještine i sposobnosti u području kibersigurnosti i postanu kiberotporne.

4. Agencija promiče suradnju i koordinaciju na razini Unije među državama članicama, institucijama, agencijama i tijelima Unije i relevantnim dionicima, uključujući privatni sektor, u pitanjima povezanima s kibersigurnošću.

5. Agencija povećava kibersigurnosne sposobnosti na razini Unije kako bi dopunila djelovanja država članica usmjerena na sprječavanje kiberprijetnji i odgovaranje na kiberprijetnje, posebno u slučaju prekograničnih incidenata.

6. Agencija promiče uporabu certifikacije, među ostalim i pridonošenjem 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.

Članak 5.

Zadaće koje se odnose na razvoj i provedbu politika i prava Unije

Agencija pridonosi 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. pridonošenjem 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 povredama sigurnosti 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.

Zadaće povezane s jačanjem kapaciteta

1. Agencija pomaže:

(a) državama članicama u nastojanjima da poboljšaju sprječavanje, otkrivanje i analizu kibersigurnosnih problema i kiberincidenata te kapacitet za odgovor na njih osiguravanjem potrebnih znanja i stručnjaka;

(b) institucijama, tijelima, uredima i agencijama Unije u njihovim nastojanjima da poboljšaju sprječavanje, otkrivanje i analizu kibersigurnosnih problema i kiberincidenata te kapacitet za odgovor na njih 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 u cijeloj Uniji 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 svoje 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 godišnjih opsežnih kibersigurnosnih vježbi velikih razmjera na razini Unije iz članka 7. stavka 6. i pružanjem preporuka politike na temelju postupka ocjenjivanja vježbi i stečenog iskustva tijekom tih vježbi;

(h) relevantnim javnim tijelima pružanjem mogućnosti 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 olakšava uspostavu centara za razmjenu i analizu informacija (ISAC) i stalno ih podupire, posebno u sektorima navedenima u Prilogu II. Direktivi (EU) 2016/1148 pružanjem najbolje prakse i smjernica o dostupnim alatima, postupku i o tome kako riješiti regulatorne probleme povezane s razmjenom informacija.

Članak 7.

Zadaće povezane s operativnom suradnjom na razini Unije

1. Agencija podupire operativnu suradnju nadležnih javnih tijela i dionika.

2. Agencija surađuje na operativnoj razini i uspostavlja sinergije s institucijama, tijelima, uredima i agencijama 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 i 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 aktivno olakšava razmjenu informacija i suradnju među njezinim članovima.

4. Agencija pridonosi operativnoj suradnji u okviru mreže CSIRT-ova pružanjem potpore državama članicama na sljedeći način:

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

(b) pružanjem, na njihov zahtjev, tehničke pomoći u slučaju incidenata sa značajnim ili znatnim učinkom;

(c) analiziranjem ranjivosti, tragova i incidenata.

Pri obavljaju tih zadaća Agencija i CERT-EU uspostavljaju strukturiranu suradnju kako bi ostvarili koristi od sinergija, posebno u pogledu operativnih aspekata.

5. Na zahtjev najmanje dviju pogođenih država članica i u isključivu svrhu pružanja savjeta za sprječavanje budućih incidenata, Agencija pruža potporu ili provodi *ex-post* tehničku istragu nakon obavijesti pogođenih poduzeća o incidentima koji imaju znatan učinak u skladu s Direktivom (EU) 2016/1148. Agencija provodi takvu istragu i na temelju obrazloženog zahtjeva Komisije u dogovoru s pogođenim državama članicama u slučaju incidenata koji utječu na najmanje dvije države članice.

Opseg istrage i postupak koji treba slijediti pri provedbi takve istrage dogovaraju pogođene države članice i Agencija, čime se ne dovode u pitanje tekuće kaznene istrage istog incidenta. Istraga se zaključuje završnim tehničkim izvješćem koje sastavlja Agencija prije svega na temelju informacija i primjedbi koje su dostavile pogođene države članice i poduzeća i koje se dogovara s pogođenim državama članicama. Sažetak izvješća u kojem se naglasak stavlja preporuke za sprječavanje budućih incidenata dostavlja se mreži CSIRT-ova.

6. Agencija organizira godišnje vježbe u području kibersigurnosti na razini Unije i, na zahtjev, podupire države članice i institucije, agencije i tijela EU-a pri organizaciji takvih vježbi. Godišnje vježbe na razini Unije uključuju tehničke, operativne i strateške elemente i pomoć u pripremi usklađenog odgovora na razini Unije na prekogranične kiberincidente velikih razmjera. Agencija pridonosi i sektorskim vježbama u području kibersigurnosti i, prema potrebi, u suradnji s relevantnim ISAC-ovima pomaže u njihovoj organizaciji te dopušta ISAC-ovima da sudjeluju i u kibersigurnosnim vježbama na razini Unije.

7. Agencija 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 (dobrovoljno) ili jedinstvene kontaktne točke iz Direktive NIS (u skladu s člankom 14. stavkom 5. Direktive NIS); Europski centar za kiberkriminal (EC3) pri Europolu, CERT-EU.

8. Agencija pridonosi 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 kako bi se pridonijelo zajedničkoj informiranosti o stanju;

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

(c) podupiranjem tehničkog rješavanja incidenta ili krize, među ostalim olakšavanjem razmjene tehničkih rješenja među državama članicama;

(d) podupiranjem izvješćivanja javnosti o incidentu ili krizi;

(e) ispitivanjem planova za suradnje pri odgovorima na takve incidente ili krize.

Članak 8.

Zadaće povezane s tržištem, kibersigurnosnom certifikacijom i normizacijom

Agencija:

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

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

(2) pomaganjem Komisiji u osiguravanju tajništva Europske skupine za kibersigurnosno certificiranje 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 nadzor certifikacije i industrijom;

(b) olakšavanjem uspostave i prihvaćanja europskih i međunarodnih normi za upravljanje rizikom i za sigurnost IKT proizvoda i usluga te 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.

Zadaće povezane sa znanjem, informiranjem i podizanjem razine osviještenosti

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 probleme povezane s kibersigurnošću;

(c) pruža, u suradnji sa stručnjacima iz tijela država članica, savjete, smjernice i najbolju praksu za sigurnost mrežnih i informacijskih sustava, posebno za sigurnost internetske infrastrukture i infrastruktura kojima se podupiru sektori navedeni u Prilogu II. Direktivi (EU) 2016/1148;

(d) na posebnom portalu objedinjuje, organizira i stavlja na raspolaganje javnosti informacije o kibersigurnosti koje su dostavile institucije, agencije i tijela Unije;

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

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

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

Članak 10.
Zadaće povezane s istraživanjem i inovacijama

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.
Zadaće povezane s međunarodnom suradnjom

Agencija pridonosi 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, na zahtjev Komisije, razmjene najbolje prakse među relevantnim međunarodnim organizacijama;

(c) pružanjem stručnih savjeta Komisiji na njezin zahtjev.

POGLAVLJE II.
USTROJSTVO 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.; i

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

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;

(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 praćenje nalaza i preporuka proizišlih iz istraga Europskog ureda za borbu protiv prijevara (OLAF) i različitih unutarnjih ili vanjskih izvješća o reviziji i ocjenjivanja;

(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 relevantne ovlasti tijela nadležnog za imenovanja delegiraju izvršnom direktoru i utvrđuju uvjeti pod kojima se to delegiranje ovlasti može obustaviti. 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 Upravljačkog odbora o glasovanju

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 praćenje nalaza i preporuka proizišlih iz istraga OLAF-a i različitih unutarnjih ili vanjskih izvješća o reviziji i ocjenjivanja;

   (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. Prema potrebi, Izvršni odbor može u slučaju hitnosti donijeti određene privremene odluke u ime Upravljačkog odbora, osobito o pitanjima povezanima s administrativnim upravljanjem, uključujući obustavu delegiranja ovlasti tijela nadležnog za imenovanja, i o proračunskim pitanjima.

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 i njegovo dostavljanje Upravljačkom odboru na ocjenu i donošenje;

(f) izradu akcijskog plana na temelju zaključaka naknadnog ocjenjivanja 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;

(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. Izvršni direktor odlučuje o tome je li, radi učinkovitog i djelotvornog obavljanja zadaća Agencije, potrebno postaviti osoblje u jednu državu članicu ili više njih. Prije nego što donese odluku o osnivanju lokalnog ureda izvršni direktor mora dobiti prethodnu suglasnost Komisije, Upravljačkog odbora i dotične države članice odnosno dotičnih država članica. U toj se odluci utvrđuje opseg aktivnosti koje će obavljati taj lokalni ured na način da se izbjegnu nepotrebni troškovi i udvostručavanje administrativnih zadaća Agencije. Kada je to prikladno ili potrebno, postiže se dogovor s dotičnim državama članicama.

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, skupine potrošača, akademski stručnjaci za kibersigurnost i predstavnici nadležnih tijela prijavljenih u skladu s [Direktivom o Europskom zakoniku elektroničkih komunikacija] te od tijela za izvršenje 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.

ODJELJAK 5.
RAD

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[36] 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.

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 ocjenjivanja iz članka 56.

Članak 22.
Izjava o interesima

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.

---

[36] 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.).

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[37] i 2015/444[38]. Ta pravila uključuju odredbe o razmjeni, obradi i pohrani klasificiranih podataka.

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.

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

[38] 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.).

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 PRORAČUNA I NJEGOVA STRUKTURA

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[39], 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.

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[40] 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.

---

39 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.).

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

POGLAVLJE 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.

Članak 32.
Povlastice i imunitet

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 izvršnoga direktora traje pet godina. Do kraja tog razdoblja Komisija provodi procjenu u kojoj se uzimaju u obzir ocjena 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 pet godina.
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. Izvršni direktor može biti razriješen dužnosti samo na temelju odluke Upravljačkog odbora, koji djeluje na prijedlog Komisije.

Članak 34.
Upućeni nacionalni stručnjaci i drugo 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. Agencija osobito može stjecati ili otuđivati pokretnu i nepokretnu imovinu te biti stranka u sudskom postupku ili i jedno i drugo.
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.
Jezični režim

1. Na Agenciju se primjenjuje Uredba Vijeća br. 1[41]. 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.

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

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

Članak 38.

Zaštita osobnih podataka

1. Agencija obrađuje osobne podatke u skladu s Uredbom (EZ) br. 45/2001 Europskog parlamenta i Vijeća[42].

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.

Članak 39.

Međunarodna 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.

[42] 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 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 najbolje moguće 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.

Administrativni nadzor

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

NASLOV III.
OKVIR ZA KIBERSIGURNOSNU CERTIFIKACIJU

Članak 43.

Europski programi kibersigurnosne certifikacije

Europskim programom kibersigurnosne certifikacije potvrđuje se da su IKT proizvodi i usluge koji su certificirani u skladu s tim programom usklađeni s utvrđenim zahtjevima u pogledu njihove sposobnosti da se odupru, na određenoj razini jamstva, djelovanjima kojima se nastoji ugroziti dostupnost, izvornost, cjelovitost ili povjerljivost pohranjenih ili poslanih ili obrađenih podataka ili funkcija ili usluga koje se nude tim proizvodima, postupcima, uslugama ili sustavima ili koje su preko njih dostupne.

Članak 44.

Izrada i donošenje europskog programa kibersigurnosne certifikacije

1. Na temelju zahtjeva Komisije ENISA izrađuje prijedlog europskog programa kibersigurnosne certifikacije koji je u skladu sa zahtjevima iz članaka 45., 46. i 47. ove Uredbe. Države članice ili Europska skupina za kibersigurnosnu certifikaciju („Skupina”) uspostavljena u skladu s člankom 53. mogu Komisiji predložiti izradu prijedloga europskog programa kibersigurnosne certifikacije.
2. Pri izradi prijedloga programa iz stavka 1. ovog članka ENISA se savjetuje sa svim relevantnim dionicima i blisko surađuje sa Skupinom. Skupina pruža ENISA-i pomoć i stručne savjete koji su joj potrebni u vezi s izradom prijedloga programa, među ostalim davanjem mišljenja kada je potrebno.
3. ENISA dostavlja Komisiji prijedlog europskog programa kibersigurnosne certifikacije izrađenog u skladu sa stavkom 2. ovog članka.
4. Komisija, na temelju prijedloga programa koji je izradila ENISA, može donositi provedbene akte, u skladu s člankom 55. stavkom 2., kojima su predviđeni europski programi kibersigurnosne certifikacije za IKT proizvode i usluge koji ispunjavaju zahtjeve iz članaka 45., 46. i 47. ove Uredbe.
5. ENISA održava posebno *web*-mjesto na kojem pruža informacije i promovira europske programe kibersigurnosne certifikacije.

Članak 45.

Sigurnosni ciljevi europskih programa kibersigurnosne certifikacije

Europski program kibersigurnosne certifikacije izrađuje se tako da se njime uzimaju u obzir, prema potrebi, sljedeći sigurnosni ciljevi:

(a) zaštititi pohranjene, poslane ili na drugačiji način obrađene podatke od slučajnog ili neovlaštenog pohranjivanja, obrade, pristupa ili objave;

(b) zaštititi pohranjene, poslane ili na drugačiji način obrađene podatke od slučajnog ili neovlaštenog uništavanja, slučajnog gubitka ili izmjene;

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

(d) evidentirati koji su podaci, funkcije ili usluge priopćeni, kada i tko ih je priopćio;

(e) osigurati da je moguće provjeriti kojim se podacima, uslugama ili funkcijama pristupilo odnosno koji su podaci, usluge ili funkcije upotrijebljeni, kada i tko im je pristupio ili ih upotrijebio;

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

(g) osigurati da je softver za IKT proizvode i usluge ažuriran i da ne sadržava poznate ranjivosti i da ti IKT proizvodi u usluge raspolažu mehanizmima za sigurno ažuriranje softvera.

Članak 46.

Razine jamstva europskih programa kibersigurnosne certifikacije

1. Europskim programom kibersigurnosne certifikacije može se utvrditi jedna od sljedećih razina jamstva ili više njih: osnovna, znatna i/ ili visoka za IKT proizvode i usluge certificirane u skladu s tim programom.

2. Osnovna, znatna i visoka razina jamstva ispunjavaju sljedeće kriterije:

(a) osnovna razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava ograničeni stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT proizvoda ili usluge i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha smanjiti rizik od kiberincidenata;

(b) znatna razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava znatan stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT proizvoda ili usluge i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha znatno smanjiti rizik od kiberincidenata;

(c) visoka razina jamstva odnosi se na certifikat izdan u kontekstu europskog programa kibersigurnosne certifikacije kojim se osigurava viši stupanj povjerenja u navedena ili zajamčena kibersigurnosna obilježja IKT proizvoda ili usluge nego certifikatima o znatnoj razini jamstva i opisuje se upućivanjem na odgovarajuće tehničke specifikacije, norme i postupke, uključujući tehničke kontrole, čija je svrha spriječiti kiberincidente.

Članak 47.

Elementi europskih programa kibersigurnosne certifikacije

1. Europski program kibersigurnosne certifikacije uključuje sljedeće elemente:

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

(b) iscrpnu specifikaciju kibersigurnosnih zahtjeva u odnosu na koje se određeni IKT proizvodi i uslugeo cjenjuju, na primjer upućivanjem na norme Unije ili međunarodne norme ili tehničke specifikacije;

(c) jednu ili više razina jamstva, ovisno o slučaju;

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

(e) informacije koje podnositelj zahtjeva mora dostaviti tijelima za ocjenjivanje sukladnosti, a koje su nužne za certificiranje;

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

(g) ako je nadzor dio programa, pravila za praćenje sukladnosti sa zahtjevima iz certifikata, uključujući mehanizme za dokazivanje trajne sukladnosti s navedenim kibersigurnosnim zahtjevima;

(h) uvjete za izdavanje, održavanje i produljenje certifikata te za proširenje ili smanjenje njegova opsega;

(i) pravila u vezi s posljedicama nesukladnosti certificiranih proizvoda i usluga IKT-a sa zahtjevima za certifikaciju;

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

(k) pravila o čuvanju evidencije tijela za ocjenjivanje sukladnosti;

(l) utvrđivanje nacionalnih programa kibersigurnosne certifikacije kojima je obuhvaćena ista vrsta ili iste kategorije IKT proizvoda i usluga;

(m) sadržaj izdanog certifikata.

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, certificiranje 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 48.

Kibersigurnosna certifikacija

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

2. Certifikacija je dobrovoljna, osim ako je pravom Unije predviđeno drukčije.

3. Europski certifikat o kibersigurnosti u skladu s ovim člankom 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 europskom kibersigurnosnom programu može predvidjeti da europski certifikat o kibersigurnosti u okviru tog programa može izdati samo javno tijelo. To javno tijelo može biti:

(a) nacionalno tijelo za nadzor certifikacije iz članka 50. stavka 1.;

(b) tijelo koje je akreditirano kao tijelo za ocjenjivanje sukladnosti u skladu s člankom 51. stavkom 1. ili

(c) tijelo osnovano u skladu sa zakonima, pravnim instrumentima ili drugim službenim upravnim postupcima dotične države članice koje ispunjava zahtjeve za tijela koja certificiraju proizvode, postupke i usluge u skladu s normom ISO/IEC 17065:2012.

5. Pravna ili fizička osoba koja prijavi svoje IKT proizvode ili usluge za postupak certifikacije dostavlja tijelu za ocjenjivanje sukladnosti iz članka 51. sve informacije potrebne za provedbu postupka certifikacije.

6. Certifikati se izdaju na najviše tri godine i mogu se obnoviti pod istim uvjetima ako 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 povezani postupci za IKT 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. Postojeći nacionalni programi kibersigurnosne certifikacije i povezani postupci za IKT proizvode i usluge koji nisu obuhvaćeni europskim programom kibersigurnosne certifikacije i dalje postoje.

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

3. Postojeći certifikati izdani u okviru nacionalnih programa kibersigurnosne certifikacije ostaju na snazi do svojeg datuma isteka.

Članak 50.

Nacionalna tijela za nadzor certifikacije

1. Svaka država članica imenuje nacionalno tijelo za nadzor certifikacije.

2. Svaka država članica obavješćuje Komisiju o identitetu imenovanog tijela.

3. Svako nacionalno tijelo za nadzor certifikacije neovisno je od subjekata koje nadzire u pogledu svojeg ustrojstva, odluka o financiranju, pravne strukture i odlučivanja.

4. Države članice osiguravaju da nacionalna tijela za nadzor certifikacije 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 uspostavljenu u skladu s člankom 53.

6. Nacionalna tijela za nadzor certifikacije obavljaju sljedeće:

(a) prate i izvršavaju primjenu odredaba iz ove glave na nacionalnoj razini i nadziru sukladnost certifikata koje su izdala tijela za ocjenjivanje sukladnosti osnovana na njihovu državnom području sa zahtjevima iz ove glave i odgovarajućeg europskog programa kibersigurnosne certifikacije;

(b) prate i nadziru aktivnosti tijela za ocjenjivanje sukladnosti za potrebe ove Uredbe, među ostalim i u pogledu obavijesti tijela za ocjenjivanje sukladnosti i povezanih zadaća iz članka 52. ove Uredbe;

(c) obrađuju pritužbe fizičkih ili pravnih osoba u pogledu certifikata koje su izdala tijela za ocjenjivanje sukladnosti s poslovnim nastanom na njihovu državnom području, 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 nadzor certifikacije ili s drugim javnim tijelima, među ostalim razmjenom informacija o mogućoj nesukladnosti IKT proizvoda i usluga sa zahtjevima iz ove Uredbe ili s posebnim europskim programima kibersigurnosne certifikacije;

(e) prate relevantne promjene u području kibersigurnosne certifikacije.

7. Svako nacionalno tijelo za nadzor certifikacije ovlašteno je barem za sljedeće:

(a) zatražiti od tijela za ocjenjivanje sukladnosti i nositelja europskog certifikata o kibersigurnosti da dostave sve informacije koje su mu potrebne za izvršavanje njegovih zadaća;

(b) provoditi istrage, u obliku revizija, tijela za ocjenjivanje sukladnosti i nositelja europskog certifikata o kibersigurnosti za potrebe provjere sukladnosti s odredbama iz glave III.;

(c) poduzimati prikladne mjere, u skladu s nacionalnim pravom, kako bi osiguralo sukladnost tijela za ocjenjivanje sukladnosti ili nositelja certifikata 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 koji 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 nadzor certifikacije surađuju međusobno i s Komisijom i, posebno, razmjenjuju informacije, iskustva i dobru praksu u području kibersigurnosne certifikacije i tehničkih pitanja povezanih s kibersigurnošću IKT 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.

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 povlače akreditaciju tijela za ocjenjivanje sukladnosti u skladu sa stavkom 1. ovog članka ako uvjeti za akreditaciju nisu i ili više nisu ispunjeni ili ako se mjerama koje je poduzelo tijelo za ocjenjivanje sukladnosti krši ova Uredba.

Članak 52.
Obavijest

1. Za svaki europski program kibersigurnosne certifikacije donesen u skladu s člankom 44. nacionalna tijela za nadzor certifikacije prijavljuju Komisiji akreditirana tijela za ocjenjivanje sukladnosti akreditirana za izdavanje certifikata na utvrđenoj razini jamstva iz članka 46. i, bez odgode, sve naknade promjene 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 zaprimi prijavu nakon isteka razdoblja iz stavka 2., ona objavljuje izmjene popisa iz stavka 2. u *Službenom listu Europske unije* u roku od dva mjeseca od datuma primitka te prijave.
4. Nacionalno tijelo za nadzor certifikacije može Komisiji podnijeti zahtjev da se tijelo za ocjenjivanje sukladnosti koje je to nacionalno tijelo za nadzor certifikacije prijavilo 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 nadzor certifikacije.
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 je sastavljena od nacionalnih tijela za nadzor certifikacije. Ta tijela predstavljaju njihovi čelnici ili drugi predstavnici nacionalnih tijela za nadzor certifikacije na visokoj razini.
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;
   (c) predložiti Komisiji da od Agencije zatraži da izradi prijedlog europskog programa kibersigurnosne certifikacije u skladu s člankom 44. ove Uredbe;

(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 nacionalnih tijela za nadzor certifikacije iz ove glave razmjenom informacija, posebno uspostavom metoda za učinkovitu razmjenu informacija povezanih sa svim pitanjima koja se odnose na kibersigurnosnu certifikaciju.

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

*Članak 54.**Sankcije***

Države članice utvrđuju pravila o sankcijama 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.
Odborski postupak

1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.
2. U slučaju upućivanja na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

Članak 56.
Ocjenjivanje i preispitivanje

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. Ocjenom 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. Ocjenjivanjem 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 ocjenjivanju zajedno s njegovim zaključcima prosljeđuje Europskom parlamentu, Vijeću i Upravljačkom odboru. Nalazi tog ocjenjivanja objavljuju se.

Članak 57.
Stavljanje izvan snage i sljedništvo

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*.

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*

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

Prijedlog Uredbe Europskog parlamenta i Vijeća o ENISA-i (agenciji EU-a za kibersigurnost) i stavljanju izvan snage Uredbe (EU) 526/2013 te o sigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt/Uredba o kibersigurnosti”)

1.2. Odgovarajuća područja politike

Područje politike: 09 – Komunikacijske mreže, sadržaj i tehnologija

Aktivnost: 09.02 jedinstveno digitalno tržište

1.3. Vrsta prijedloga/inicijative

☒Prijedlog/inicijativa odnosi se na **novo djelovanje (Glava III. – Certifikacija)**

☐ Prijedlog/inicijativa odnosi se na **novo djelovanje nakon pilot-projekta/pripremnog djelovanja**[43]

☒Prijedlog/inicijativa odnosi se na **produženje postojećeg djelovanja (Glava II. – mandat ENISA-e)**

☐ Prijedlog/inicijativa odnosi se na **djelovanje koje je preusmjereno na novo djelovanje**

1.4. Cilj/ciljevi

1.4.1. Višegodišnji strateški ciljevi Komisije na koje se odnosi prijedlog/inicijativa

1. Povećati otpornost država članica, poduzeća i EU-a u cjelini

2. Osigurati pravilno funkcioniranje unutarnjeg tržišta EU-a za IKT proizvode i usluge

3. Povećati globalnu konkurentnost poduzeća EU-a koja djeluju području IKT-a

4. Približiti zakone i ostale propise država članica za koje je potrebna kibersigurnost

1.4.2. Posebni cilj/ciljevi

Imajući na umu opće ciljeve, u širem kontekstu revidirane strategije za kibersigurnost, instrumentom se, određivanjem djelokruga i mandata ENISA-e i uspostavom europskog okvira za certifikaciju IKT proizvoda i usluga, nastoje ostvariti sljedeći posebni ciljevi:

1. jačanje **sposobnosti i pripravnosti** država članica i poduzeća;
2. poboljšanje **suradnje i koordinacije** među državama članicama i institucijama, agencijama i tijelima EU-a;
3. jačanje **sposobnosti na razini EU-a za dopunu djelovanja država članica**, posebno u slučaju prekograničnih kiberkriza;
4. povećanje **osviještenosti** građana i poduzeća o pitanjima kibersigurnosti;
5. jačanje povjerenja u jedinstveno digitalno tržište i u digitalne inovacije povećanjem opće **transparentnosti kibersigurnosnog jamstva**[44] IKT proizvoda i usluga.

[43] Kako je navedeno u članku 54. stavku 2. točkama (a) ili (b) Financijske uredbe.

ENISA će pridonositi ostvarenju prethodno navedenih ciljeva na sljedeće načine:

pojačanom potporom izradi politika – pružanjem savjeta i smjernica Komisiji i državama članicama u cilju ažuriranja i razvoja holističkog normativnog okvira u području kibersigurnosti te sektorskih politika i zakonodavnih inicijativa kada je riječ o pitanjima kibersigurnosti; doprinošenjem radu Skupine za suradnju (članak 11. Direktive (EU) 2016/1148) pružanjem stručnih savjeta i pomoći; podupiranjem razvoja politike i provedbe u području elektroničke identifikacije i usluga povjerenja; promicanjem razmjene najbolje prakse među nadležnim tijelima;

pojačanom potporom izgradnji kapaciteta – pružanjem potpore državama članicama, institucijama, tijelima, uredima i agencijama Unije u razvoju i poboljšanju sprječavanja, otkrivanja, analize i kapaciteta za odgovor na probleme i incidente u području kibersigurnosti; pružanjem pomoći državama članicama, na zahtjev, u razvoju nacionalnih CSIRT-ova, nacionalnih strategija za kibersigurnost; pružanjem pomoći institucijama Unije u razvoju i preispitivanju Unijinih strategija za kibersigurnost; pružanjem osposobljavanja u području kibersigurnosti; pomaganjem državama članicama u okviru Skupine za suradnju u razmjeni najbolje prakse; olakšavanjem uspostave sektorskih centara za razmjenu informacija i analizu (ISAC);

operativnom suradnjom i potporom za upravljanje krizama – podupiranjem suradnje nadležnih javnih tijela i dionika uspostavom sustavne suradnje s institucijama, tijelima, uredima i agencijama Unije koja se bave pitanjima kibersigurnosti, kiberkriminala i zaštite privatnosti i osobnih podataka; osiguravanjem tajništva mreže CSIRT-ova (članak 12. stavak 2. Direktive (EU) 2016/1148) i pridonošenjem operativnoj suradnji unutar mreže pružanjem, u suradnji s CERT-EU-om, potpore državama članicama, na zahtjev: organiziranjemi redovitih kibersigurnosnih vježbi; pridonošenjem razvoju usklađenog odgovora na prekogranične kiberincidente i kiberkrize velikih razmjera; provedbom, u suradnji s mrežom CSIRT-ova, *ex-post* tehničke istrage značajnih incidenata i izdavanjem naknadnih preporuka;

zadaćama povezanima s tržištem (normizacija, certifikacija) – obavljanjem niza funkcija kojima se posebno podupire unutarnje tržište: „tržišni opservatorij" za kibersigurnost, analizom relevantnih trendova na kibersigurnosnom tržištu radi boljeg usklađivanja ponude i potražnje; podupiranjem i promicanjem razvoja i provedbe politike Unije o kibersigurnosnoj certifikaciji IKT proizvoda i usluga izradom prijedloga europskih programa kibersigurnosne certifikacije za IKT proizvode i usluge, osiguravanjem tajništva za Skupinu Unije za kibersigurnosnu certifikaciju, pružanjem smjernica i dobre prakse o sigurnosnim zahtjevima za IKT proizvode i usluge u suradnji s nacionalnim tijelima za nadzor certifikacije i industrijom; **pojačanom potporom povećanju znanja, informiranosti i razine osviještenosti –** pružanjem pomoći i savjeta Komisiji i državama članicama u cilju stjecanja visoke razine znanja u cijeloj Uniji o pitanjima povezanima s NIS-om i njegovoj primjeni na industrijske dionike. To podrazumijeva i prikupljanje, organiziranje i objavu na posebnom portalu informacija o sigurnosti mrežnih i informacijskih sustava [ili kibersigurnosti]. Još jedan važan element jesu aktivnosti podizanja razine osviještenosti i informativne kampanje o kibersigurnosnim rizicima usmjerene na opću javnost.

pojačanom potporom istraživanju i inovacijama – pružanjem savjeta o potrebama u području istraživanja i utvrđivanjem prioriteta u području kibersigurnosti;

---

[44] Transparentnost kibersigurnosnog jamstva znači pružanje korisnicima dovoljno informacija o kibersigurnosnim značajkama s pomoću kojih mogu objektivno utvrditi razinu sigurnosti određenog IKT proizvoda, usluge ili postupka.

podupiranjem međunarodne suradnje – potporom nastojanjima Unije da uspostavi suradnju s trećim zemljama i međunarodnim organizacijama u cilju poticanja međunarodne suradnje u području kibersigurnosti.

CERTIFIKACIJA

Okvirom za certifikaciju pridonijet će se ostvarenju ciljeva jer će se povećati opća transparentnost kibersigurnosnog jamstva[45] IKT proizvoda i usluga, a tako i povjerenje u jedinstveno digitalno tržište i digitalne inovacije. Time bi se trebalo pridonijeti i izbjegavanju rascjepkanosti programa certificiranja u EU-u i povezanih sigurnosnih zahtjeva i kriterija za ocjenjivanje po državama članicama i sektorima.

1.4.3. Očekivani rezultat/rezultati i utjecaj

Navesti učinke koje bi prijedlog/inicijativa trebali imati na ciljane korisnike/skupine.

Očekuje se da će se jačanjem ENISA-e (podupiranjem sposobnosti, sprječavanja, suradnje i osviještenosti na razini EU-a, čime će se povećati ukupna kiberotpornost EU-a) te podupiranjem okvira EU-a za certifikaciju IKT proizvoda i usluga ostvariti sljedeći učinci (otvoren popis):

Ukupni učinak

– ukupan pozitivan učinak na unutarnje tržište zahvaljujući manjoj rascjepkanosti tržišta i izgradnji povjerenja u digitalne tehnologije s pomoću bolje suradnje, usklađenijih pristupa politikama kibersigurnosti EU-a i povećanim sposobnostima na razini EU-a. To bi trebalo imati pozitivan gospodarski učinak jer bi se smanjili troškovi incidenata povezanih s kibersigurnošću/kiberkriminalom, za koje procijenjeni gospodarski učinak u Uniji iznosi 0,41 % BDP-a EU-a (tj. otprilike 55 milijardi EUR).

Posebni rezultati:

Veće sposobnosti i pripravnost država članica i poduzeća u području kibersigurnosti

– veće sposobnosti i pripravnost država članica u području kibersigurnosti (zahvaljujući dugoročnoj strateškoj analizi kiberprijetnji i kiberincidenata, smjernicama i izvješćima, razmjeni iskustva i dobre prakse, dostupnosti osposobljavanja i materijala za osposobljavanje, pojačanim vježbama CyberEurope),

– veće sposobnosti privatnih dionika zahvaljujući potpori za uspostavu centara za razmjenu informacija i analizu (ISAC) u različitim sektorima,

– bolja pripravnost EU-a i država članica u području kibersigurnosti zahvaljujući dostupnosti dobro uvježbanih i dogovorenih planova u slučaju prekograničnog kiberincidenta velikih razmjera testiranih u vježbama CyberEurope.

Bolja suradnja i koordinacija među državama članicama i institucijama, agencijama i tijelima EU-a

– bolja suradnja unutar javnog i privatnog sektora i između njih,

– bolja prekogranična i međusektorska usklađenost pristupa provedbi Direktive NIS,

[45] Transparentnost kibersigurnosnog jamstva znači pružanje korisnicima dovoljno informacija o kibersigurnosnim značajkama s pomoću kojih mogu objektivno utvrditi razinu sigurnosti određenog IKT proizvoda, usluge ili postupka.

– bolja suradnja u području certifikacije zahvaljujući institucionalnom okviru kojim se omogućuje razvoj europskih programa kibersigurnosne certifikacije i razvoj zajedničke politike u tom području.

Veće sposobnosti na razini EU-a za dopunu djelovanja država članica

– bolji „operativni kapacitet EU-a” za dopunu djelovanja država članica i njihovo podupiranje, na zahtjev, u odnosu na ograničene i unaprijed definirane usluge. Očekuje se da će one pozitivno utjecati na uspješno sprječavanje incidenata te na otkrivanje i odgovore na razini države članice i Unije;

Veća osviještenost građana i poduzeća o pitanjima kibersigurnosti

– veća opća osviještenost građana i poduzeća o pitanjima kibersigurnosti,

– poboljšana sposobnost donošenja utemeljenih odluka povezanih s IKT proizvodima i uslugama zahvaljujući kibersigurnosnoj certifikaciji

Veće povjerenje u jedinstveno digitalno tržište i u digitalne inovacije povećanjem transparentnosti kibersigurnosnog jamstva IKT proizvoda i usluga

– veća transparentnost kibersigurnosnog jamstva[46] IKT proizvoda i usluga zahvaljujući pojednostavnjenju postupaka sigurnosnog certificiranja s pomoću okvira za cijeli EU

– veća razina jamstva za sigurnosne značajke IKT proizvoda i usluga

– veće prihvaćanje sigurnosnog certificiranja potaknuto pojednostavnjenim postupcima, nižim troškovima i mogućim poslovnim prilikama u cijelom EU-u koje ne onemogućava rascjepkanost tržišta

– bolja konkurentnost na kibersigurnosnom tržištu EU-a zbog nižih troškova i manjeg administrativnog opterećenja MSP-ova i uklanjanja mogućih prepreka ulasku na tržište uzrokovanih brojnim nacionalnim sustavima certifikacije

Ostalo

– ne očekuje se da će ijedan od ciljeva imati znatan utjecaj na okoliš,

– u odnosu na proračun EU-a može se očekivati veća učinkovitost zbog bolje suradnje i koordinacije aktivnosti među institucijama, agencijama i tijelima EU-a.

1.4.4. Pokazatelji rezultata i utjecaja

Navesti pokazatelje koji omogućuju praćenje provedbe prijedloga/inicijative.

(a)

Cilj: jačanje sposobnosti i pripravnosti država članica i poduzeća

- broj osposobljavanja koje je organizirala ENISA
- zemljopisna pokrivenost (broj zemalja i područja) izravne pomoći koju je pružila ENISA
- razina pripravnosti koju su postigle države članice u pogledu zrelosti CSIRT-ova i nadzora regulatornih mjera povezanih s kibersigurnošću

[46] Transparentnost kibersigurnosnog jamstva znači pružanje korisnicima dovoljno informacija o značajkama kibersigurnosti s pomoću kojih mogu objektivno utvrditi razinu sigurnosti određenog IKT proizvoda, usluge ili postupka.

- broj dobre prakse u cijelom EU-u u pogledu ključnih infrastruktura koju osigurava ENISA
- količina dobre prakse u cijelom EU-u koju za MSP-ove osigurava ENISA
- godišnje strateške analize kiberprijetnji i kiberincidenata u cilju otkrivanja novih kretanja koje objavljuje ENISA
- redovito pridonošenje ENISA-e radu radnih skupina za kibersigurnost europskih organizacija za normizaciju (ESO).

Cilj: bolja suradnja i koordinacija među državama članicama i institucijama, agencijama i tijelima EU-a:

- broj država članica koje su iskoristile preporuke i mišljenja ENISA-e u svojem postupku izrade politika
- broj institucija, agencija i tijela EU-a koji su iskoristili preporuke i mišljenja ENISA-e u svojem postupku izrade politika
- redovita provedba programa rada mreže CSIRT-ova i dobro funkcioniranje IT infrastrukture i komunikacijskih kanala mreže CSIRT-ova
- broj tehničkih izvješća koja su dostavljena Skupini za suradnju i koja je ona upotrijebila
- dosljedan pristup prekograničnoj i međusektorskoj provedbi Direktive NIS
- broj regulatornih procjena sukladnosti koje je provela ENISA
- broj uspostavljenih ISACS-ova u različitim sektorima, posebno za ključne infrastrukture
- uspostava i redovito održavanje informativne platforme za širenje informacija o kibersigurnosti koje potječu od institucija, agencija i tijela EU-a
- redoviti doprinos izradi EU-ovih programa rada u području istraživanja i inovacija
- uspostavljen sporazum o suradnji između ENISA-e, EC3-a i CERT-EU-a
- broj programa certificiranja koji su uključeni u okvir i razvijeni unutar njega

Cilj: jačanje sposobnosti na razini EU-a za dopunu djelovanja država članica, posebno u slučaju prekograničnih kiberkriza:

- godišnje strateške analize kiberprijetnji i kiberincidenata u cilju otkrivanja novih trendova koje objavljuje ENISA
- objavljivanje objedinjenih informacija o incidentima koje je ENISA prijavila u skladu s Direktivom NIS
- broj paneuropskih vježbi koje je koordinirala Agencija i broj država članica i organizacija koje su u njima sudjelovale
- broj zahtjeva za podupiranje hitnih odgovora koje su države članice podnijele ENISA-i i koje je Agencija izvršila
- broj analiza ranjivosti, tragova i incidenata koje je izvršila ENISA u suradnji s CERT-EU-om
- dostupnost izvješća o stanju u cijelom EU-u koja se temelje na informacijama koje su države članice i drugi subjekti dostavili ENISA-i u slučaju prekograničnog kiberincidenta velikih razmjera.

Cilj: povećanje osviještenosti građana i poduzeća o pitanjima kibersigurnosti:

- redovito provođenje kampanja podizanja razine osviještenosti u EU-u i na nacionalnoj razini i redovito informiranje o temama u skladu s novim potrebama za učenjem
- povećanje kiberosviještenosti među građanima EU-a
- redovito provođenje ispitivanja osviještenosti o kibersigurnosti i postupno povećanje postotka točnih odgovora
- redovito objavljivanje dobre prakse u području kibersigurnosti i kiberhigijene usmjerene na zaposlenike i organizacije.

Cilj: jačanje povjerenja u jedinstveno digitalno tržište i u digitalne inovacije povećanjem opće transparentnosti kibersigurnosnog jamstva[47] IKT proizvoda i usluga:

- broj programa uključenih u okvir EU-a
- manji troškovi pribavljanja certifikata o sigurnosti IKT-a
- broj tijela za ocjenjivanje sukladnosti specijaliziranih za certifikaciju u području IKT-a, u svim državama članicama
- osnivanje Europske skupine za kibersigurnosnu certifikaciju i organiziranje redovitih sastanaka
- donesene smjernice za certificiranje u skladu s okvirom EU-a
- redovita objava analiza glavnih trendova na kibersigurnosnom tržištu EU-a
- broj certificiranih IKT proizvoda i usluga u skladu s pravilima europskog okvira za sigurnosno certificiranje u području IKT-a
- veći broj krajnjih korisnika koji su svjesni sigurnosnih značajki IKT proizvoda i usluga

(b)

1.4.5. Zahtjev/zahtjevi koje je potrebno kratkoročno ili dugoročno ispuniti

Uzimajući u obzir regulatorne zahtjeve i dinamičan razvoj kiberprijetnji, treba preispitati mandat ENISA-e kako bi se utvrdio obnovljeni skup zadaća i funkcija u cilju djelotvornog i učinkovitog podupiranja nastojanja država članica, institucija EU-a i drugih dionika da osiguraju sigurni kiberprostor u Europskoj uniji. Opisan je predloženi opseg mandata uz jačanje područja u kojima je agencija pokazala jasnu dodanu vrijednost i dodavanje novih područja u kojima je potrebna potpora zbog novih prioriteta politike i instrumenata, posebno Direktive NIS, revizije Strategije EU-a za kibersigurnost, novog Plana EU-a u području kibersigurnosti za suradnju u kiberkrizama i sigurnosno certificiranje u području IKT-a. Novim predloženim mandatom Agenciji se nastoji omogućiti snažnija i važnija uloga koja će posebno uključivati aktivnije podupiranje država članica u borbi protiv posebnih prijetnji (operativni kapacitet) i pretvaranje Agencije u stručni centar za pomoć državama članicama i Komisiji u postupku kibersigurnosne certifikacije.

Istodobno se prijedlozima uspostavlja okvir za kibersigurnosnu certifikaciju IKT proizvoda

[47] Transparentnost kibersigurnosnog jamstva znači pružanje korisnicima dovoljno informacija o kibersigurnosnim značajkama s pomoću kojih mogu objektivno utvrditi razinu sigurnosti određenog IKT proizvoda, usluge ili postupka.

i usluga i opisuju se osnovne funkcije i zadaće ENISA-e u području kibersigurnosne certifikacije. Okvirom se propisuju zajedničke odredbe i postupci kojima se omogućuje stvaranje programa kibersigurnosne certifikacije za određene IKT proizvode/usluge ili kibersigurnosne rizike u cijelom EU-u. Stvaranjem europskih programa kibersigurnosne certifikacije u skladu s Okvirom omogućit će se da certifikati izdani u okviru tih programa budu važeći i priznati u svim državama članicama te će se riješiti postojeći problem rascjepkanosti tržišta.

1.4.6. Dodana vrijednost sudjelovanja Unije

Kibersigurnost je globalno pitanje prekogranične prirode koje sve više postaje međusektorsko pitanje zbog međuovisnosti između mreža i informacijskih sustava. Povećava se broj, složenost i razmjer kiberincidenata i njihov učinak na gospodarstvo i društvo i očekuje se da će i dalje rasti usporedno s tehnološkim napretkom, primjerice širenjem interneta stvari. To znači da su potrebni veći zajednički napori država članica, institucija EU-a i privatnih dionika usmjereni na suzbijanje kiberprijetnji za koje se ne može očekivati da će se u budućnosti smanjiti.

Od osnivanja ENISA-e 2004. njezin cilj bio je poticati suradnju među državama članicama i dionicima u području NIS-a, uključujući javno-privatnu suradnju. Ta potpora suradnji uključivala je tehničke aktivnosti usmjerene na izradu prikaza okruženja prijetnji u cijelom EU-u, osnivanje stručnih skupina i organizaciju paneuropskih vježbi za suzbijanje kiberincidenata i upravljanje krizama za javni i privatni sektor (posebno „Cyber Europe"). Direktivom NIS ENISA-i su povjerene dodatne zadaće, među ostalim uloga tajništva mreže CSIRT-ova za operativnu suradnju država članica.

Dodana vrijednost djelovanja na razini EU-a, posebno u cilju jačanja suradnje među državama članicama, ali i između zajednica u području mrežne i informacijske sigurnosti, priznata je u Zaključcima vijeća iz 2016.[48] i jasno proizlazi iz ocjene ENISA-e iz 2017. u kojoj je prikazano da dodana vrijednost Agencije poglavito proizlazi iz njezine sposobnosti za jačanje suradnje tih dionika. Na razini EU-a ne postoji nijedan drugi akter koji podupire suradnju toliko velikog broja različitih dionika u području mrežne i informacijske sigurnosti.

Dodana vrijednosti ENISA-a u smislu okupljanja zajednica i dionika u području kibersigurnosti odnosi se i na područje certifikacije. Zbog rasta kiberkriminaliteta i sigurnosnih prijetnji uspostavljene su nacionalne inicijative kojima se uvode strogi kibersigurnosni zahtjevi i zahtjevi u pogledu certifikacije komponenata IKT-a koje se upotrebljavaju u tradicionalnoj infrastrukturi. Iako su te inicijative važne, one mogu uzrokovati rascjepkanost jedinstvenog tržišta i prepreke interoperabilnosti. Prodavač IKT-a možda će morati proći nekoliko postupaka certifikacije da bi mogao prodavati u nekoliko država članica. Nedjelotvornost/neučinkovitost postojećih programa certificiranja vjerojatno se neće moći riješiti bez intervencije EU-a. Rascjepkanost tržišta vrlo će se vjerojatno bez intervencije povećati u vrlo kratkom roku (sljedećih 5 – 10 godina) zbog uvođenja novih programa certificiranja. Zbog nepostojanja koordinacije i interoperabilnosti među tim programimasmanjuje se potencijal jedinstvenog digitalnog tržišta. To dokazuje dodanu vrijednost uspostave europskog okvira za kibersigurnosnu certifikaciju IKT proizvoda i usluga kojim će se uspostaviti potrebni uvjeti za učinkovito rješavanje problema povezanih sa supostojanjem višestrukih postupaka certifikacije u

[48] Zaključci Vijeća o jačanju europskog sustava kiberotpornosti i poticanju konkurentne i inovativne industrije kibersigurnosti – 15. studenoga 2016.

različitim državama članicama, smanjiti troškovi certifikacije i na taj način povećati privlačnost certifikacije u EU-u s komercijalnog gledišta i gledišta tržišnog natjecanja.

1.4.7. Pouke iz prijašnjih sličnih iskustava

U skladu s pravnom osnovom za ENISA-u Komisija je izvršila ocjenjivanje Agencije koje je uključivalo neovisno istraživanje i javno savjetovanje. Zaključak je ocjenjivanja da su ciljevi ENISA-e i dalje relevantni. U kontekstu tehnološkog razvoja i novih prijetnji kao i znatne potrebe za većom mrežnom i informacijskom sigurnošću (NIS) u EU-u, potrebna je tehnička stručnost za razvoj pitanja mrežne i informacijske sigurnosti. U državama članicama treba jačati kapacitete za razumijevanje prijetnji i za odgovor na prijetnje i dionici moraju surađivati u svim tematskim područjima i sa svim institucijama.

Agencija uspješno pridonosi mrežnoj i informacijskoj sigurnosti u Europi zahvaljujući pružanju mogućnosti za jačanje kapaciteta u 28 država članica, jačanju suradnje među državama članicama i dionicima u području mrežne i informacije sigurnosti, pružanju stručnih savjeta i jačanju zajedništva te podupiranju politike.

ENISA je uspjela ostvariti utjecaj, barem u određenoj mjeri, u širokom području mrežne i informacijske sigurnosti, ali nije u potpunosti uspjela razviti prepoznatljivost i dostatnu vidljivost da bi bila priznata kao „najbolji" stručni centar u Europi. To se može objasniti širokim mandatom ENISA-e za koji joj nisu osigurani razmjerno dostatni resursi. Nadalje, ENISA je jedina agencija EU-a s vremenski ograničenim mandatom zbog čega je ograničena njezina sposobnost za razvoj dugoročne vizije i održive potpore dionicima. To je i u suprotnosti s odredbama Direktive NIS kojom se ENISA-i povjeravaju zadaće koje nisu ograničenog trajanja.

Trenutačno ne postoji europski okvir za kibersigurnosnu certifikaciju IKT proizvoda i usluga. Međutim, zbog rasta kiberkriminala i sigurnosnih prijetnji nastale su nacionalne inicijative, koje uzrokuju rizik od fragmentacije jedinstvenog tržišta.

1.4.8. Usklađenost i moguća sinergija s drugim odgovarajućim instrumentima

Inicijativa je u velikoj mjeri u skladu s postojećim politikama, posebno u području unutarnjeg tržišta. Oblikovana je u skladu s općim pristupom kibersigurnosti koji je definiran u preispitivanju Strategije jedinstvenog digitalnog tržišta u cilju dopune sveobuhvatnog skupa mjera, primjerice preispitivanja strategije EU-a za kibersigurnost, plana za suradnju u slučaju kiberkriza i inicijativa za suzbijanje kiberkriminaliteta. Njome bi se osigurala usklađenost s odredbama postojećeg zakonodavstva u području kibersigurnosti, posebno s Direktivom NIS, u cilju daljnjeg razvoja kiberotpornosti EU-a s pomoću pojačanih sposobnosti, suradnje, upravljanja rizikom i osviještenosti o kiberprijetnjama.

Predloženim mjerama certifikacije trebao bi se riješiti mogući problem rascjepkanosti uzrokovane postojećim i novim nacionalnim programima certificiranja, čime bi se pridonijelo razvoju jedinstvenog digitalnog tržišta. Inicijativom se podupire i dopunjuje provedba Direktive NIS na način da se poduzećima na koja se primjenjuje Direktiva osigurava vrlo koristan alat za dokazivanje usklađenosti sa zahtjevima mrežne i informacijske sigurnosti u cijeloj Uniji.

Predloženim europskim okvirom za kibersigurnosnu certifikaciju u području IKT-a ne dovodi se u pitanje Opća uredba o zaštiti podataka[49], a posebno relevantne odredbe o certifikaciji[50] kako se primjenjuju na sigurnost obrade osobnih podataka. Naposljetku, ali ne i najmanje važno, predloženi programi u budućem europskom okviru trebali bi se što više oslanjati na međunarodne norme kao način za izbjegavanje stvaranja prepreka trgovini i osiguravanje usklađenosti s međunarodnim inicijativama.

[49] Uredba (EU) 2016/679 od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

[50] Na primjer članci 42. (Certificiranje) i 43. (Certifikacijska tijela) te članci 57., 58. i 70. posebno u pogledu relevantnih zadaća i ovlasti neovisnih nadzornih tijela i zadaća Europskog odbora za zaštitu podataka.

1.5. Trajanje i financijski utjecaj

☐ Prijedlog/inicijativa **ograničenog trajanja**

– ☐ prijedlog/inicijativa na snazi od [DD/MM]GGGG do [DD/MM]GGGG

– ☐ Financijski utjecaj od GGGG do GGGG

☒ Prijedlog/inicijativa **neograničenog trajanja**

– Provedba s razdobljem uspostave od 2019. do 2020.

– nakon čega slijedi redovna provedba.

1.6. Predviđene metode upravljanja[51]

☒ **Izravno upravljanje** Komisije (Glava III. – Certifikacija)

– ☐ izvršne agencije

☐ **Podijeljeno upravljanje** s državama članicama

☒ **Neizravno upravljanje** delegiranjem zadaća proračunske provedbe:

☐ međunarodnim organizacijama i njihovim agencijama (navesti);

☐ EIB-u i Europskom investicijskom fondu;

☒ tijelima na koja se upućuje u člancima 208. i 209. (Glava II. – ENISA)

☐ tijelima javnog prava;

☐ tijelima uređenima privatnim pravom koja pružaju javne usluge u mjeri u kojoj daju odgovarajuća financijska jamstva;

☐ tijelima uređenima privatnim pravom države članice kojima je povjerena provedba javno-privatnog partnerstva i koja daju odgovarajuća financijska jamstva;

☐ osobama kojima je povjerena provedba posebnih aktivnosti u ZVSP-u u skladu s glavom V. UEU-a i koje su navedene u odgovarajućem temeljnom aktu.

Napomene

Ova Uredba obuhvaća sljedeće: – u glavi II. predložene Uredbe preispituje se mandat Agencije Europske unije za sigurnost mrežnih i informacijskih sustava (ENISA) i daje joj se važna uloga u postupku certificiranja – u glavi III. uspostavlja se okvir za stvaranje europskih programa kibersigurnosne certifikacije IKT proizvoda i usluga u kojima ENISA ima ključnu ulogu.

[51] Informacije o načinima upravljanja i upućivanju na Financijsku uredbu dostupne su na internetskim stranicama BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

Navesti učestalost i uvjete.

Praćenje će početi odmah nakon donošenja pravnog instrumenta i bit će usmjereno na njegovu primjenu. Komisija će organizirati sastanke s ENISA-om, predstavnicima država članica (npr. skupinama stručnjaka) i relevantnim dionicima posebno kako bi olakšala provedbu pravila o certifikaciji, kao što je osnivanje Odbora.

Prvo ocjenjivanje trebalo bi provesti 5 godina nakon stupanja na snagu pravnog instrumenta, ako dovoljno podataka bude na raspolaganju. U pravni instrument uključena je izričita klauzula o ocjenjivanju i reviziji [članak XXX.] u skladu s kojom će Komisija provesti neovisno ocjenjivanje. Komisija će Europskom parlamentu i Vijeću dostaviti izvješće o svojem ocjenjivanju prema potrebi popraćeno prijedlogom o reviziji, u cilju mjerenja učinka Uredbe i njezine dodane vrijednosti. Daljnja ocjenjivanja trebalo bi provoditi svakih pet godina. Tijekom ocjenjivanja Komisija će primjenjivati svoju metodologiju bolje regulative. Ocjenjivanja će se provoditi uz pomoć ciljanih, stručnih rasprava, istraživanja i savjetovanja s različitim dionicima.

Izvršni direktor ENISA-e trebao bi svake dvije godine dostaviti Upravljačkom odboru *ex-post* ocjenu aktivnosti ENISA-e. Agencija bi trebala izraditi i akcijski plan na temelju zaključaka ocjena i svake dvije godine Komisiju izvješćivati o napretku. Upravljački odbor trebao bi biti odgovoran nadzirati provedbu odgovarajućih mjera na temelju tih zaključaka.

Navodne nepravilnosti u radu Agencije istražuje Europski ombudsman u skladu s odredbama članka 228. Ugovora.

Izvori podataka za planirano praćenje bili bi poglavito ENISA, Europska skupina za kibercertifikaciju, Skupina za suradnju, mreža CSIRT-ova i tijela država članica. Osim podataka iz izvješća (uključujući godišnja izvješća o radu) ENISA-e, Europske skupine za kibercertifikaciju, Skupine za suradnju i mreže CSIRT-ova, upotrebljavat će se, prema potrebi, posebni alati za prikupljanje podataka (na primjer ankete koje se provode među nacionalnim tijelima, Eurobarometar i izvješća o kampanji Mjesec kibersigurnosti i paneuropskim vježbama).

2.2. Sustav upravljanja i kontrole

2.2.1. Utvrđeni rizik/rizici

Utvrđeni su rizici ograničeni: agencija Unije već postoji i njezin će se mandat odrediti na način da se veći naglasak stavi na područja u kojima je agencija pokazala jasnu dodanu vrijednost i uključe nova područja u kojima je potrebna potpora zbog novih prioriteta politike i instrumenata, posebno Direktive NIS, revizije Strategije EU-a za kibersigurnost, novog Plana EU-a u području kibersigurnosti za suradnju u kiberkrizama i sigurnosno certificiranje u području IKT-a.

U prijedlogu se stoga podrobno opisuju funkcije Agencije i povećava njezina učinkovitost. Povećanje operativnih sposobnosti i zadaća nije stvaran rizik jer bi se njima dopunjavala i

podupirala djelovanja država članica, na zahtjev i u odnosu na ograničene i unaprijed utvrđene usluge.

Nadalje, predloženim modelom agencije, u skladu sa zajedničkim pristupom, osigurala bi se dostatna kontrola kako bi se osiguralo da ENISA djeluje u smjeru postizanja svojih ciljeva. Čini se da su operativni i financijski rizici predloženih promjena ograničeni.

Istodobno je nužno osigurati odgovarajuće financijske resurse kako bi ENISA mogla izvršavati zadaće koje su joj povjerene novim mandatom, među ostalim u području certifikacije.

2.2.2. Predviđene metode kontrole

Financijski izvještaji agencije podnosit će se na odobrenje Revizorskom sudu i podlijegat će postupku davanja razrješnice, a predviđene su i revizije.

Isto tako, djelovanje agencije podliježe nadzoru Europskog ombudsmana u skladu s odredbama članka 228. Ugovora.

Vidjeti prethodne točke 2.1. i 2.2.1.

2.3. Mjere za sprječavanje prijevara i nepravilnosti

Navesti postojeće ili predviđene mjere za sprečavanje i zaštitu.

Primjenjivale bi se ENISA-ine mjere za sprečavanje i zaštitu od prijevara, posebno:

– osoblje agencije provjerava plaćanja za sve zatražene usluge ili studije prije izvršavanja plaćanja, uzimajući u obzir ugovorne obveze, ekonomska načela i dobru financijsku ili upravljačku praksu. Odredbe o sprečavanju prijevara (nadzor, zahtjevi u smislu izvješćivanja itd.) bit će uključene u sve sporazume i ugovore koje agencija sklapa s primateljima plaćanja,

– u cilju borbe protiv prijevara, korupcije i ostalih nezakonitih aktivnosti, odredbe Uredbe (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća od 11. rujna 2013. o istragama koje provodi Europski ured za borbu protiv prijevara (OLAF), primjenjuju se bez ograničenja,

– Agencija u roku od šest mjeseci od stupanja na snagu ove Uredbe pristupa Međuinstitucionalnom sporazumu od 25. svibnja 1999. između Europskog parlamenta, Vijeća Europske unije i Komisije Europskih zajednica u vezi s internim istragama koje provodi Europski ured za borbu protiv prijevara (OLAF), te bez odgode donosi odgovarajuće odredbe koje se primjenjuju na sve zaposlenike agencije.

3. PROCIJENJENI FINANCIJSKI UTJECAJ PRIJEDLOGA/INICIJATIVE

3.1. Naslov/naslovi višegodišnjeg financijskog okvira i proračunska linija/linije u okviru rashoda na koje se prijedlog/inicijativa odnosi

- Postojeće proračunske linije

Prema redoslijedu naslova višegodišnjeg financijskog okvira i proračunskih linija.

Naslov višegodišnjeg financijskog okvira:	Proračunska linija	Vrsta rashoda	Doprinos			
		Dif./nedif.[52].	zemalja EFTA-e[53]	zemalja kandidatkinja[54]	trećih zemalja	u smislu članka 21. stavka 2. točke (b) Financijske uredbe
1a Konkurentnost za rast i zapošljavanje	09.0203 ENISA i sigurnosna certifikacija u području informacijske i komunikacijske tehnologije	Dif.	DA	NE	NE	NE
5 Administrativni rashodi]	09.0101 – Rashodi koji se odnose na osoblje u aktivnoj službi u području politike komunikacijskih mreža, sadržaja i tehnologija 09.0102 – Rashodi koji se odnose na vanjsko osoblje u aktivnoj službi u području politike komunikacijskih mreža,	Nedif.	NE	NE	NE	NE

52 Dif. = diferencirana odobrena sredstva / nedif. = nediferencirana odobrena sredstva.

53 EFTA: Europsko udruženje slobodne trgovine

54 Zemlje kandidatkinje i, ako je primjenjivo, potencijalne zemlje kandidatkinje sa zapadnog Balkana.

	sadržaja i tehnologija 09.010211 – Ostali rashodi upravljanja					

3.2. Procijenjeni utjecaj na rashode

3.2.1. Sažetak procijenjenog utjecaja na rashode

u milijunima EUR (do tri decimalna mjesta)

Naslov višegodišnjeg financijskog okvira	1a	Konkurentnost za rast i zapošljavanje

ENISA			**Polazna vrijednost** **2017. (31.12.2016.)**		**2019.** ***(od 01.7. 2019.)***	**2020.**	**2021.**	**2022.**	**UKUPNO**
Glava 1.: Rashodi za osoblje *(uključujući rashode povezane sa zapošljavanjem, osposobljavanjem, sociomedicinskom infrastrukturom i vanjskim uslugama)*	Preuzete obveze	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Plaćanja	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Glava 2: Infrastrukturni i operativni troškovi	Preuzete obveze	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Plaćanja	(2a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Glava 3: Operativni rashodi	Preuzete obveze	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Plaćanja	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
UKUPNA odobrena sredstva za ENISA-u	Preuzete obveze	=1+1a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Plaćanja	=2+2a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Naslov višegodišnjeg financijskog okvira	**5**	„Administrativni rashodi”

u milijunima EUR (do tri decimalna mjesta)

		2019. *(od 01.7. 2019.)*	**2020.**	**2021.**	**2022.**	**UKUPNO**
GU: CNECT						
• Ljudski resursi		0,216	0,846	0,846	0,846	**2,754**
• Ostali administrativni rashodi		0,102	0,235	0,238	0,242	**0,817**
UKUPNO GU CNECT	Odobrena sredstva	0,318	1,081	1,084	1,088	**3,571**

Troškovi osoblja izračunani su u skladu s planiranim datumom zapošljavanja (zapošljavanje je predviđeno od 1. srpnja 2019.)

Planirana sredstva nakon 2020. okvirna su i njima se ne dovode u pitanje prijedlozi Komisije za višegodišnji financijski okvir nakon 2020.

UKUPNA odobrena sredstva iz NASLOVA 5 višegodišnjeg financijskog okvira	(Ukupne preuzete obveze = ukupna plaćanja)	0,318	1,081	1,084	1,088	**3,571**

u milijunima EUR (do tri decimalna mjesta)

	2019.	**2020.**	**2021.**	**2022.**	**UKUPNO**

UKUPNA odobrena sredstva iz NASLOVA 1. – 5. višegodišnjeg financijskog okvira	Preuzete obveze	16,868	21,727	23,332	24,11	**86,038**
	Plaćanja	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Procijenjeni utjecaj na odobrena sredstva Agencije

– ☐ Za prijedlog/inicijativu nisu potrebna odobrena sredstva za poslovanje

– ☒ Za prijedlog/inicijativu potrebna su odobrena sredstva za poslovanje kako je navedeno u nastavku:

Odobrena sredstva za preuzete obveze u milijunima EUR (do tri decimalna mjesta)

Navesti ciljeve i rezultate[55] ⇩	**2019.**	**2020.**	**2021.**	**2022.**	**UKUPNO**
Jačanje sposobnosti i pripravnosti država članica i poduzeća	1,408	1,900	1,931	1,969	7,208
Poboljšanje suradnje i koordinacija među državama članicama i institucijama, agencijama i tijelima EU-a	0,939	1,266	1,288	1,313	4,806
Jačanje sposobnosti na razini EU-a za dopunu djelovanja država članica, posebno u slučaju prekograničnih kiberkriza	0,704	0,950	0,965	0,985	3,604
Povećanje osviještenosti građana i poduzeća o pitanjima kibersigurnosti	0,704	0,950	0,965	0,985	3,604
Jačanje povjerenja u jedinstveno digitalno tržište i u digitalne inovacije povećanjem opće transparentnosti kibersigurnosnog jamstva IKT proizvoda i usluga	0,939	1,266	1,288	1,313	4,806
UKUPNI TROŠAK	4,694	6,332	6,437	6,565	24,028

[55] U ovoj su tablici prikazani samo rashodi poslovanja za glavu 3.

3.2.3. Procijenjen utjecaj na ljudske resurse Agencije

3.2.3.1. Sažetak

– ☐ Za prijedlog/inicijativu nisu potrebna odobrena administrativna sredstva

– ☒ Za prijedlog/inicijativu potrebna su sljedeća odobrena administrativna sredstva:

u milijunima EUR (do tri decimalna mjesta)

	T3/4 2019.	**2020.**	**2021.**	**2022.**
Privremeni dužnosnici (razred AD)	4,242	5,695	6,381	6,709
Privremeni dužnosnici (razred AST)	1,601	1,998	2,217	2,217
Ugovorni djelatnici	2,041	2,041	2,041	2,041
Upućeni nacionalni stručnjaci	0,306	0,447	0,656	0,796
UKUPNO	**8,190**	**10,181**	**11,295**	**11,763**

Troškovi osoblja izračunani su u skladu s planiranim datumom zapošljavanja (za sadašnje zaposlenike ENISA-e puno zaposlenje predviđa se od 1. siječnja 2019.) U pogledu novih zaposlenika predviđeno je postupno zapošljavanje počevši od 1. srpnja 2019. do potpune zaposlenosti 2022. Planirana sredstva nakon 2020. okvirna su i njima se ne dovode u pitanje prijedlozi Komisije za višegodišnji financijski okvir nakon 2020.

Očekivani utjecaj na osoblje (dodatni ekvivalenti punog radnog vremena) – plan radnih mjesta

Funkcijska skupina i razred	2017. **Postojeća ENISA**	T3/4 2019.	2020.	2021.	2022.
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					

AD ukupno	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST ukupno	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
AST/SC ukupno					
SVEUKUPNO	48	12	10	7	3

Zadaće dodatnih zaposlenika razreda AD/AST za ostvarivanje ciljeva instrumenta opisanih u odjeljku 1.4.2.:

Zadaće	AD	AST	UNS	Ukupno
Politika i jačanje kapaciteta	8	1		9
Operativna suradnja	8	1	7	16
Certificiranje (zadaće povezane s tržištem)	9	3	2	14
Znanje, informiranje i podizanje razine osviještenosti	1	1		2
UKUPNO	26	6	9	41

Opis zadaća koje treba obaviti:

Zadaće	**Potrebna dodatna sredstva**
Razvoj i provedba politike EU-a i jačanje kapaciteta	Zadaće bi uključivale pomaganje Skupini za suradnju, podupiranje dosljedne prekogranične provedbe mrežne i informacijske sigurnosti, redovito izvješćivanje o stanju provedbe pravnog okvira EU-a; savjetovanje i koordinaciju sektorskih kibersigurnosnih inicijativa, uključujući u području energetike, prometa (npr. zrakoplovni /cestovni /pomorski /povezana

	vozila), zdravstva, financija; pružanje potpore za uspostavu centara za razmjenu informacija i analizu (ISAC) u različitim sektorima.
Operativna suradnja i upravljanje krizama	**Zadaće bi uključivale sljedeće:** osiguravanje tajništva za mrežu CSIRT-ova osiguravanjem, među ostalim, dobrog funkcioniranja IT infrastrukture i komunikacijskih kanala mreže CSIRT-ova; osiguravanje strukturirane suradnje s CERT-EU-om, EC3-om i ostalim relevantnim tijelima EU-a; organiziranje **vježbi Cyber Europe**[56] – zadaće povezane s povećanjem učestalosti vježbe, koja bi se umjesto svake dvije godine održavala svake godine, i osiguravanjem da se tijekom vježbe incident promatra od početka do kraja; **tehničku pomoć –** zadaće bi uključivale strukturiranu suradnju s CERT-EU-om u cilju pružanja tehničke pomoći u slučaju znatnih incidenata i podupiranja analize incidenata. To bi uključivalo pružanje pomoći državama članicama za rješavanje incidenata i analizu ranjivosti, tragova i incidenata. Olakšavanje suradnje među pojedinim državama članicama u slučaju hitnih odgovora analizom i objedinjavanjem nacionalnih izvješća o stanju na temelju informacija koje joj dobrovoljno dostavljaju države članice i ostali subjekti; **plan za koordinirani odgovor na prekogranične kiberincidente velikih razmjera –** Agencija će pridonijeti razvoju usklađenog odgovora, na razini Unije i država članica, na prekogranične incidente ili krize velikih razmjera povezane s kibersigurnošću s pomoću niza zadaća koje uključuju sve od doprinosa informiranosti o stanju na razini Unije do testiranja planova suradnje u slučaju incidenata. ***ex post* tehničke istrage incidenata** – provoditi *ex post* tehničke istrage incidenata ili im pridonositi u suradnji s mrežom CSIRT-ova u cilju izdavanja preporuka i jačanja sposobnosti u obliku javnih izvješća kako bi se budući incidenti mogli lakše spriječiti.

[56] Cyber Europe najveća je i najsveobuhvatnija vježba EU-a u području kibersigurnosti u kojoj sudjeluje više od 700 stručnjaka za kibersigurnost iz svih 28 država članica. Održava se svake dvije godine. U ocjeni ENISA-e i u strategiji EU-a za kibersigurnost iz 2013. ističe se da mnogi dionici zbog brzog razvoja kiberprijetnji zagovaraju povećanje učestalosti vježbe Cyber Europe s jednom u dvije godine na jednom svake godine. Međutim, to trenutačno nije moguće jer Agencija ima ograničena sredstva.

Zadaće povezane s tržištem (normizacija, certifikacija):	Zadaće bi uključivale aktivno podupiranje aktivnosti unutar okvira za certifikaciju, uključujući pružanje tehničkih savjeta u izradi prijedloga europskih programa kibersigurnosne certifikacije. Zadaće će uključivati i potporu razvoju i provedbi politika Unije u području normizacije, certifikacije i opservatorija tržišta – to će zahtijevati olakšavanje prihvaćanja normi za upravljanje rizikom elektroničkih proizvoda, mreža i usluga i savjetovanje operatora ključnih usluga i pružatelja digitalnih usluga o zahtjevima u pogledu tehničke sigurnosti. Zadaće će uključivati i analizu glavnih trendova na kibersigurnosnom tržištu.
znanje i informacije, podizanje razine osviještenosti:	Kako bi se osigurao lakši pristup bolje strukturiranim informacijama o kibersigurnosnim rizicima i mogućim mjerama za njihovo uklanjanje, prijedlogom se Agenciji dodjeljuje nova zadaća razvoja i održavanja „informativnog centra" Unije. Zadaće bi uključivale prikupljanje, analizu i objavu, na posebnom portalu, informacija o sigurnosti mrežnih i informacijskih sustava, posebno o kibersigurnosti, koje pružaju institucije, agencije i tijela EU-a. Zadaće bi uključivale i podupiranje aktivnosti ENISA-e u području podizanja razine osviještenosti kako bi se Agenciji omogućilo da pojača svoje napore.

3.2.3.2. Procjena potrebnih ljudskih resursa za matičnu glavnu upravu

– ☐ Za prijedlog/inicijativu nisu potrebni ljudski resursi.

– ☒ Za prijedlog/inicijativu potrebni su sljedeći ljudski resursi:

Procjenu treba izraziti u cijelom iznosu (ili najviše s jednim decimalnim mjestom)

		Dodatno osoblje			
	Početno stanje 2017.	T3/4 2019.	2020.	2021.	2020.
• **Radna mjesta prema planu radnih mjesta (dužnosnici i privremeni djelatnici)**					
09 01 01 01 (Sjedište i predstavništva Komisije)	1	2	3		
• **Vanjsko osoblje (u ekvivalentu punog radnog vremena: EPRV)**[57]					
09 01 02 01 (UO, UNS, UsO iz „globalne omotnice")	1	2			
UKUPNO		**4**	**3**		

Opis zadaća koje treba obaviti:

Dužnosnici i privremeno osoblje	predstavljanje Komisije u Upravljačkom odboru Agencije; izrada mišljenja Komisije o jedinstvenom programskom dokumentu BEREC-a i praćenje njegove provedbe; nadzor pripreme proračuna agencije i praćenje njegova izvršenja; pružanje pomoći Agenciji u razvoju aktivnosti u skladu s politikama Unije, među ostalim sudjelovanjem na relevantnim sastancima; nadzor provedbe okvira za europske programe kibersigurnosne certifikacije IKT proizvoda i usluga; održavanje kontakata s državama članicama i ostalim važnim dionicima u pogledu napora u području certificiranja; suradnja s ENISA-om u pogledu prijedloga programa; izrada prijedloga europskih programa kibersigurnosti.
Vanjsko osoblje	Isto kao gore navedeno.

[57] UO = ugovorno osoblje; LO = lokalno osoblje; UNS = upućeni nacionalni stručnjaci; UsO = ustupljeno osoblje; MSD = mladi stručnjaci u delegacijama.

3.2.4. Usklađenost s važećim višegodišnjim financijskim okvirom

– ☐ Prijedlog/inicijativa u skladu je s postojećim višegodišnjim financijskim okvirom.

– ☒ Prijedlog/inicijativa povlači za sobom reprogramiranje relevantnog naslova višegodišnjeg financijskog okvira.

Prijedlog će zahtijevati reprogramiranje članka 09 02 03 zbog revizije mandata ENISA-e kojom se Agenciji dodjeljuju nove zadaće povezane, među ostalim, s provedbom Direktive NIS i europskim okvirom za kibersigurnosnu certifikaciju. Odgovarajući iznosi:

Godina	Predviđeno	Zahtjev
2019.	10,739	16,550
2020.	10,954	20,646
2021.	Nije primjenjivo	22,248*
2022.	Nije primjenjivo	23,023*

* Ovo je procjena. Financiranje EU-a nakon 2020. ispitat će se u kontekstu rasprave u Komisiji o svim prijedlozima za razdoblje nakon 2020. To znači da će Komisija nakon što podnese prijedlog sljedećeg višegodišnjeg financijskog okvira predstaviti izmijenjeni zakonodavni financijski izvještaj uzimajući u obzir zaključke procjene učinka[58].

– ☐ Za prijedlog/inicijativu potrebna je primjena instrumenta za financijsku fleksibilnost ili revizija višegodišnjeg financijskog okvira[59].

3.2.5. Doprinosi trećih strana

– ☐ Prijedlogom/inicijativom ne predviđa se sudjelovanje trećih strana u financiranju.

– ☒ Prijedlogom/inicijativom predviđa se sufinanciranje prema sljedećoj procjeni:

	Godina **2019.**	Godina **2020.**	Godina **2021.**	Godina **2022.**
EFTA	p.m[60].	p.m.	p.m.	p.m.

58 Poveznica na stranicu s procjenom učinka.

59 Vidjeti članke 11. i 17. Uredbe Vijeća (EU, Euratom) br. 1311/2013 kojom se uspostavlja višegodišnji financijski okvir za razdoblje 2014. - 2020.

60 Točan iznos za sljedeće godine bit će poznat nakon utvrđivanja faktora proporcionalnosti za EFTA-u za predmetnu godinu.

3.3. Procijenjeni utjecaj na prihode

– ☒ Prijedlog/inicijativa nema financijski utjecaj na prihode.

– ☐ Prijedlog/inicijativa ima sljedeći financijski utjecaj:

  – ☐ na vlastita sredstva

  – ☐ na razno

EUROPSKA
KOMISIJA

Bruxelles, 13.9.2017.
COM(2017) 477 final

ANNEX 1

PRILOG

PRIJEDLOGU 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”)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

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 moraju ispuniti zahtjeve norme EN ISO/IEC 17065:2012.

17. Tijela za ocjenjivanje sukladnosti moraju osigurati da ispitni laboratoriji koji se upotrebljavaju za ocjenjivanje sukladnosti ispunjavaju zahtjeve norme EN ISO/IEC 17025:2005.