Europski parlament
2019-2024

Dokument s plenarne sjednice

A9-0307/2023

26.10.2023.

***I
IZVJEŠĆE

o Prijedlogu uredbe Europskog parlamenta i Vijeća o izmjeni Uredbe (EU) 2019/881 u pogledu upravljanih sigurnosnih usluga (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Odbor za industriju, istraživanje i energetiku

Izvjestiteljica: Josianne Cutajar

Oznake postupaka

*	Postupak savjetovanja
***	Postupak suglasnosti
***I	Redovni zakonodavni postupak (prvo čitanje)
***II	Redovni zakonodavni postupak (drugo čitanje)
***III	Redovni zakonodavni postupak (treće čitanje)

(Navedeni se postupak temelji na pravnoj osnovi predloženoj u nacrtu akta.)

Izmjene nacrta akta

Amandmani Parlamenta u obliku dvaju stupaca

Brisanja su označena ***podebljanim kurzivom*** u lijevom stupcu. Izmjene su označene ***podebljanim kurzivom*** u obama stupcima. Novi tekst označen je ***podebljanim kurzivom*** u desnom stupcu.

U prvom i drugom retku zaglavlja svakog amandmana naznačen je predmetni odlomak iz nacrta akta koji se razmatra. Ako se amandman odnosi na postojeći akt koji se želi izmijeniti nacrtom akta, zaglavlje sadrži i treći redak u kojem se navodi postojeći akt te četvrti redak u kojem se navodi odredba akta na koju se izmjena odnosi.

Amandmani Parlamenta u obliku pročišćenog teksta

Novi dijelovi teksta označuju se ***podebljanim kurzivom***. Brisani dijelovi teksta označuju se oznakom ▌ ili su precrtani. Izmjene se naznačuju tako da se novi tekst označi ***podebljanim kurzivom***, a da se zamijenjeni tekst izbriše ili precrta.
Iznimno, izmjene strogo tehničke prirode koje unesu nadležne službe prilikom izrade konačnog teksta ne označuju se.

SADRŽAJ

Stranica

NACRT ZAKONODAVNE REZOLUCIJE EUROPSKOG PARLAMENTA

o Prijedlogu uredbe Europskog parlamenta i Vijeća o izmjeni Uredbe (EU) 2019/881 u pogledu upravljanih sigurnosnih usluga

(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Redovni zakonodavni postupak: prvo čitanje)

Europski parlament,

– uzimajući u obzir Prijedlog Komisije upućen Europskom parlamentu i Vijeću (COM(2023)0208),

– uzimajući u obzir članak 294. stavak 2. i članak 114. Ugovora o funkcioniranju Europske unije, u skladu s kojima je Komisija podnijela Prijedlog Parlamentu (C9-0137/2023),

– uzimajući u obzir članak 294. stavak 3. Ugovora o funkcioniranju Europske unije,

– uzimajući u obzir mišljenje Europskog gospodarskog i socijalnog odbora od 13. srpnja 2023.[1],

– uzimajući u obzir članak 59. Poslovnika,

– uzimajući u obzir pismo Odbora za unutarnje tržište i zaštitu potrošača,

– uzimajući u obzir izvješće Odbora za industriju, istraživanje i energetiku (A9-0307/2023),

1. usvaja sljedeće stajalište u prvom čitanju;

2. poziva Komisiju da predmet ponovno uputi Parlamentu ako zamijeni, bitno izmijeni ili namjerava bitno izmijeniti svoj Prijedlog;

3. nalaže svojoj predsjednici da stajalište Parlamenta proslijedi Vijeću, Komisiji i nacionalnim parlamentima.

[1] SL C 349, 29.9.2023., str. 167.

Amandman 1

AMANDMANI EUROPSKOG PARLAMENTA*

na prijedlog Komisije

2023/0108 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o izmjeni Uredbe (EU) 2019/881 u pogledu upravljanih sigurnosnih usluga

(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[2],

uzimajući u obzir mišljenje Odbora regija,

u skladu s redovnim zakonodavnim postupkom[3],

---

* Amandmani: novi ili izmijenjeni tekst označava se podebljanim kurzivom; a brisani tekst oznakom ▌.

2 ***SL C 349, 29.9.2023., str. 167.***

3 ***Stajalište Europskog parlamenta od ... (još nije objavljeno u Službenom listu) i odluka Vijeća od ....***

budući da:

(1) Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća[4] utvrđen je okvir za uspostavu europskih programa kibersigurnosne certifikacije za potrebe osiguranja prikladne razine kibersigurnosti proizvoda, usluga i procesa ***informacijske i komunikacijske tehnologije (***IKT***)*** u Uniji kao i za potrebe izbjegavanja fragmentacije unutarnjeg tržišta u pogledu programâ kibersigurnosne certifikacije u Uniji.

(1a) Kako bi se osigurala otpornost Unije na kibernapade i spriječile eventualne ranjivosti na tržištu Unije, ovom se Uredbom namjerava dopuniti horizontalni regulatorni okvir kojim se utvrđuju sveobuhvatni kibersigurnosni zahtjevi za sve proizvode s digitalnim elementima u skladu s Uredbom (EU) .../... Europskog parlamenta i Vijeća[5] (2022/0272(COD)), kojom se utvrđuju osnovni zahtjevi za upravljane kibersigurnosne usluge, njihovu primjenu i pouzdanost.

(2) Upravljane sigurnosne usluge, odnosno usluge koje se sastoje od obavljanja aktivnosti povezanih s upravljanjem kibersigurnosnim rizicima klijenata ili pružanja pomoći za te aktivnosti, ***uključujući otkrivanje, odgovor na incidente ili oporavak od njih,*** sve su važnije u sprečavanju i ublažavanju kibersigurnosnih incidenata. ***Aktivnosti pružatelja upravljanih sigurnosnih usluga sastoje se od usluga koje se odnose na sprečavanje, identifikaciju, zaštitu, otkrivanje, analizu, zaustavljanje, odgovor i oporavak, uključujući, među ostalim, pružanje obavještajnih podataka o kiberprijetnjama, praćenje prijetnji u stvarnom vremenu s pomoću proaktivnih tehnika, uključujući integriranu sigurnost, procjenu rizika, prošireno otkrivanje, ispravljanje i odgovor.*** Zbog toga se pružatelji tih usluga smatraju ključnim ili važnim subjektima koji pripadaju sektoru visoke kritičnosti u skladu s Direktivom (EU) 2022/2555 Europskog parlamenta i Vijeća[6]. U skladu s uvodnom

---

4 Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

5 Uredba (EU) .../... Europskog parlamenta i Vijeća od ... o ... (SL L, …, ELI: …).

6 Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

izjavom 86. te direktive, u područjima kao što su odgovor na incidente, penetracijska testiranja, revizije sigurnosti i savjetovanje, pružatelji upravljanih sigurnosnih usluga imaju posebno važnu ulogu u pomaganju subjektima u njihovim nastojanjima da spriječe i otkriju incidente te odgovore na njih ili se oporave od njih. Pružatelji upravljanih sigurnosnih usluga i sami su, međutim, bili meta kibernapada te zbog svoje bliske integracije u rad svojih klijenata predstavljaju poseban rizik. Ključni i važni subjekti u smislu Direktive (EU) 2022/2555 stoga bi trebali postupati s većom pažnjom pri odabiru pružatelja upravljanih sigurnosnih usluga.

(3) Osim toga, pružatelji upravljanih sigurnosnih usluga imaju važnu ulogu u kibersigurnosnoj pričuvi EU-a, čija je postupna uspostava omogućena u Uredbi (EU) …/… [o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih]. Kibersigurnosna pričuva EU-a koristit će se kao potpora mjerama odgovora i hitnog oporavka u slučaju značajnih kibersigurnosnih incidenata i kibersigurnosnih incidenata velikih razmjera. U Uredbi (EU) .../... [o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih] utvrđen je postupak odabira pružatelja koji čine kibersigurnosnu pričuvu EU-a i u njemu bi se, među ostalim, trebalo uzeti u obzir je li dotični pružatelj prošao europsku ili nacionalnu kibersigurnosnu certifikaciju. Relevantne usluge koje pružaju pouzdani pružatelji u skladu s Uredbom (EU) …/… [o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih] odgovaraju upravljanim sigurnosnim uslugama u skladu s ovom Uredbom.

(4) Certifikacija upravljanih sigurnosnih usluga nije važna samo za postupak odabira za kibersigurnosnu pričuvu EU-a, nego je i ključan pokazatelj kvalitete privatnim i javnim subjektima koji namjeravaju kupovati takve usluge. S obzirom na kritičnost upravljanih sigurnosnih usluga i osjetljivost podataka koji se u njima obrađuju, certifikacija bi potencijalnim klijentima mogla biti važan pokazatelj i jamstvo pouzdanosti tih usluga. Europski programi certifikacije za upravljane sigurnosne usluge doprinose izbjegavanju fragmentacije jedinstvenog tržišta. Stoga je cilj ove Uredbe poboljšanje funkcioniranja unutarnjeg tržišta.

(4a) Europski programi certifikacije za upravljane sigurnosne usluge trebali bi rezultirati prihvaćanjem tih usluga i jačanjem tržišnog natjecanja u tom području, uzimajući u obzir posebne potrebe pružatelja i korisnika. Tim bi se programima stoga trebala postići ravnoteža između njihova cilja i mogućeg regulatornog, administrativnog i financijskog opterećenja s kojim bi se mogli suočiti pružatelji, posebno mikropoduzeća ili mala i srednja poduzeća (MSP-ovi). Osim toga, programima bi se trebala potaknuti upotreba certificiranih upravljanih sigurnosnih usluga na način da doprinesu njihovoj pristupačnosti, posebno za manje aktere, kao što su mikropoduzeća i MSP-ovi, te lokalne i regionalne vlasti koje imaju ograničene kapacitete i resurse, ali koje su sklonije povredama kibersigurnosti s financijskim, pravnim, reputacijskim i operativnim posljedicama.

(4b) Unijinim programom certifikacije za upravljane sigurnosne usluge trebala bi se osigurati dostupnost sigurnih i visokokvalitetnih usluga kojima se jamči sigurna digitalna tranzicija i doprinosi postizanju ciljeva utvrđenih u programu politike za digitalno desetljeće, posebno u pogledu cilja da 75 % poduzeća iz EU-a počne upotrebljavati računalstvo u oblaku, umjetnu inteligenciju ili velike količine podataka, da više od 90 % mikropoduzeća i MSP-ova dosegne barem osnovnu razinu digitalne intenzivnosti te da se ključne javne usluge nude na internetu.

(4c) Ponuda obrazovnih sadržaja i formalnog osposobljavanja u digitalnom i tehnološkom okruženju koje se trenutačno brzo razvija se razlikuje, a znanje se može steći na različite načine, odnosno formalnim i neformalnim putem; na sveučilištima ili tečajevima i primjerice osposobljavanjem na radnom mjestu ili dugotrajnim radnim iskustvom u relevantnom području.

(5) Uz primjenu IKT proizvoda, IKT usluga ili IKT procesa, upravljane sigurnosne usluge često nude dodatne mogućnosti koje se oslanjaju na kompetencije, stručnost i iskustvo njihova osoblja. Kako bi se osigurala vrlo visoka kvaliteta pruženih upravljanih sigurnosnih usluga, među sigurnosne ciljeve trebalo bi uvrstiti vrlo visoku razinu tih kompetencija, stručnosti i iskustva te odgovarajuće unutarnje postupke. Kako bi se omogućilo da se ciljanim programom certifikacije obuhvate svi aspekti ***upravljane*** sigurnosne usluge, potrebno je izmijeniti Uredbu (EU) 2019/881. ***Pri razvoju programa certifikacije uspostavljenog u skladu s ovom Uredbom***

trebali bi se uzeti u obzir i rezultati i preporuke ocjenjivanja i revizija koji se njome predviđaju.

(5a) Kako bi se olakšao rast pouzdanog tržišta Unije i istodobno stvorila partnerstva s trećim zemljama istomišljenicama, među ostalim s obzirom na odredbe Uredbe (EU) .../... Europskog parlamenta i Vijeća[7] (2023/0109(COD)) u pogledu pristupa kibersigurnosnoj pričuvi EU-a, postupak certifikacije uspostavljen okvirom iz ove Uredbe trebalo bi pojednostavniti kako bi se osiguralo međunarodno priznavanje i usklađenost s međunarodnim standardima.

(5b) Kako bi se osigurao razvoj pouzdanog tržišta Unije za upravljane sigurnosne usluge, pružatelji tih usluga i države članice trebali bi surađivati i doprinositi prikupljanju podataka o stanju tržišta rada u području kibersigurnosti i njegovu razvoju.

(5c) Koordinirani pristup na razini Unije za jačanje otpornosti ključne infrastrukture temelji se na izgradnji kapaciteta država članica. Međutim, Unija se suočava s nedostatkom talenata, koji karakterizira manjak kvalificiranih stručnjaka, i s prijetnjama koje se brzo mijenjaju, kako je potvrđeno u Komunikaciji Komisije od 18. travnja 2023. o Akademiji za vještine u području kibersigurnosti. Stoga bi, kako bi se olakšala pojava visokokvalitetnih osnovnih upravljanih sigurnosnih usluga i kako bi se dobio bolji pregled sastava radne snage Unije u području kibersigurnosti, trebalo ojačati suradnju između država članica, Komisije, ENISA-e i dionika, uključujući privatni sektor i akademsku zajednicu, razvojem javno-privatnih partnerstava, podupiranjem inicijativa za istraživanje i inovacije, razvojem i uzajamnim priznavanjem zajedničkih standarda i certifikacijom vještina u području kibersigurnosti, među ostalim putem Europskog okvira vještina za kibersigurnost. Time bi se također trebala olakšati mobilnost stručnjaka u području kibersigurnosti unutar Unije te integracija znanja i osposobljavanja u području kibersigurnosti u obrazovne programe, te istodobno osigurati pristup naukovanju i pripravništvu za mlade, uključujući osobe koje žive u regijama u nepovoljnom položaju, kao što su otoci, rijetko naseljena, ruralna i udaljena područja. Tim mjerama ujedno bi trebalo privući veći broj žena i djevojaka u to

---

7 Uredba (EU) .../... Europskog parlamenta i Vijeća od ... o ... (SL L, …, ELI: …).

područje te doprinijeti uklanjanju rodnog jaza u znanosti, tehnologiji, inženjerstvu i matematici. Privatni sektor trebao bi biti usmjeren i na osposobljavanje na radnom mjestu koje obuhvaća najtraženije vještine, uključujući javnu upravu i start-up poduzeća, mikropoduzeća i MSP-ove.

(5d) Trebalo bi osigurati odgovarajuća financijska sredstva i resurse za potrebe dodatnih zadaća povjerenih ENISA-i izmjenama Uredbe (EU) 2019/881 koje su uvedene ovom Uredbom.

(5e) Kako bi se dopunili određeni elementi ove Uredbe koji nisu ključni, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. Ugovora o funkcioniranju Europske unije kako bi se osigurao europski program kibersigurnosne certifikacije za IKT proizvode, IKT usluge, IKT procese i upravljane sigurnosne usluge. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.[8] Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.

(5e) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća te je on dao mišljenje [DD.MM.GGGG.][9],

DONIJELI SU OVU UREDBU:

---

8 SL L 123, 12.5.2016., str. 1.

9 SL C .../...

Članak 1.

Izmjene Uredbe (EU) 2019/881

Uredba (EU) 2019/881 mijenja se kako slijedi:

(1) u članku 1. stavku 1. prvom podstavku točka (b) zamjenjuje se sljedećim:

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

(2) Članak 2. mijenja se kako slijedi:

(a) točke (9.), (10.) i (11.) zamjenjuju se sljedećim:

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

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

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

(b) umeće se sljedeća točka:

„(14.a) „upravljana sigurnosna usluga” znači usluga koja se ***pruža trećoj strani, a sastoji se*** od obavljanja aktivnosti povezanih s upravljanjem

kibersigurnosnim rizicima, uključujući ***odgovor na incidente***, penetracijska testiranja, revizije sigurnosti i savjetovanje, ili od pružanja pomoći ***ili savjeta u vezi s tim aktivnostima***;”;

(c) točke ***(***20.***)***, ***(***21.***)*** i ***(***22.***)*** zamjenjuju se sljedećim:

„(20.)„tehničke specifikacije” znači dokument kojim se propisuju tehnički zahtjevi koje IKT proizvod, IKT usluga, IKT proces ili upravljana sigurnosna usluga trebaju ispunjavati ili postupci ocjenjivanja sukladnosti koji se na njih odnose;

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

(22) „samoocjenjivanje sukladnosti” znači djelovanje koje provodi proizvođač ili pružatelj IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga kojim se evaluira ispunjavaju li ti IKT proizvodi, IKT usluge, IKT procesi ili upravljane sigurnosne usluge zahtjeve utvrđene u određenom europskom programu kibersigurnosne certifikacije.”***;***

(3) u članku 4. stavak 6. zamjenjuje se sljedećim:

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

(4) članak 8. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

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

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

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

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

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

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

(b) stavak 3. zamjenjuje se sljedećim:

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

(c) stavak 5. zamjenjuje se sljedećim:

„5. ENISA olakšava uspostavu i prihvaćanje europskih i međunarodnih normi za upravljanje rizikom i za sigurnost IKT proizvoda, IKT usluga, IKT procesa i upravljanih sigurnosnih usluga.”;

(5) u članku 46. stavci 1. i 2. zamjenjuju se sljedećim:

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

2. Europskim okvirom za kibersigurnosnu certifikaciju pruža se mehanizam za uspostavu europskih programa kibersigurnosne certifikacije. Njime se potvrđuje da IKT proizvodi, IKT usluge i IKT procesi koji su evaluirani u skladu s takvim programima ispunjavaju utvrđene sigurnosne zahtjeve za potrebe zaštite dostupnosti, izvornosti, cjelovitosti i povjerljivosti pohranjenih, prenesenih ili obrađenih podataka ili funkcija ili usluga koje se nude s pomoću tih proizvoda, usluga i procesa ili kojima se s pomoću njih može pristupiti tijekom njihova cijelog životnog ciklusa. Uz to, njime se potvrđuje da upravljane sigurnosne usluge koje su evaluirane u skladu s takvim programima ispunjavaju utvrđene sigurnosne zahtjeve za potrebe zaštite dostupnosti, izvornosti, cjelovitosti i povjerljivosti podataka kojima se pristupa ili koji se obrađuju, pohranjuju ili prenose u vezi s pružanjem tih usluga te se potvrđuje da te usluge na potrebnoj razini kompetentnosti, stručnosti i iskustva kontinuirano pruža osoblje s vrlo visokom razinom relevantnog tehničkog znanja i profesionalnog integriteta.”;

(6) u članku 47. stavci 2. i 3. zamjenjuju se sljedećim:

„2. Kontinuirani program rada Unije konkretno uključuje popis IKT proizvoda, IKT usluga i IKT procesa ili njihovih kategorija, te upravljanih sigurnosnih usluga, koji mogu imati koristi od uključivanja u područje primjene europskog programa kibersigurnosne certifikacije. ***U tom kontekstu Komisija može uključiti detaljnu procjenu postojećih načina osposobljavanja kako bi se premostio utvrđeni nedostatak vještina te popis prijedloga za ispunjavanje potreba za kvalificiranim zaposlenicima i vrstama vještina.***

3. Uključivanje određenih IKT proizvoda, IKT usluga i IKT procesa ili njihovih kategorija, odnosno upravljanih sigurnosnih usluga, u kontinuirani program

rada Unije opravdano je na temelju jednog ili više od sljedećih razloga:

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

(b) relevantnog prava ili politika Unije ili država članica;

tržišne potražnje;

(ca) tehnološkog razvoja te dostupnosti i razvoja međunarodnih programa kibersigurnosne certifikacije te međunarodnih i industrijskih standarda.

(d) razvoja kiberprijetnji;

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

(7) članak 49. ***mijenja se kako slijedi***:

(a) stavak 7. zamjenjuje se sljedećim:

„7. Komisija ***je***, na temelju prijedloga programa certifikacije koji je izradila ENISA, ***ovlaštena donijeti delegirane*** akte ***u skladu s člankom 65.a kojim se ova Uredba dopunjuje i*** kojim se predviđaju europski programi kibersigurnosne certifikacije za IKT proizvode, IKT usluge, IKT procese i upravljane sigurnosne usluge koji ispunjavaju zahtjeve određene u člancima 51., 52. i 54.***";***

(b) umeće se sljedeći stavak:

„7.a Prije donošenja takvih delegiranih akata Komisija u suradnji s ENISA-om provodi i objavljuje procjenu učinka predloženog europskog programa kibersigurnosne certifikacije. Tijekom pripreme procjene učinka Komisija provodi javna savjetovanja i savjetovanja s Interesnom skupinom za kibersigurnosnu certifikaciju (SCCG) i Europskom skupinom za kibersigurnosnu certifikaciju (ECCG)";

(8) Članak 51. mijenja se kako slijedi:

(a) naslov se zamjenjuje sljedećim:

„Sigurnosni ciljevi europskih programa kibersigurnosne certifikacije za IKT proizvode, IKT usluge i IKT procese”

(b) uvodna rečenica zamjenjuje se sljedećim:

„Europski program kibersigurnosne certifikacije za IKT proizvode, IKT usluge ili IKT procese mora se oblikovati tako da se njime postignu, ovisno o slučaju, barem sljedeći sigurnosni ciljevi:”***;***

(9) umeće se sljedeći članak:

„Članak 51.a Sigurnosni ciljevi europskih programa kibersigurnosne certifikacije za upravljane sigurnosne usluge

Europski program kibersigurnosne certifikacije za upravljane sigurnosne usluge mora se oblikovati tako da se njime postignu, ovisno o slučaju, barem sljedeći sigurnosni ciljevi:

(a) osigurati da se upravljane sigurnosne usluge pružaju na potrebnoj razini kompetentnosti, stručnosti i iskustva, među ostalim da osoblje zaduženo za pružanje tih usluga ima vrlo visoku razinu tehničkog znanja i stručnosti u tom području, dostatno i primjereno iskustvo te najviši stupanj profesionalnog integriteta;

(b) osigurati da pružatelj ima primjerene interne postupke kojima jamči da se upravljane sigurnosne usluge u svakom trenutku pružaju na vrlo visokoj razini kvalitete;

(c) zaštita podataka kojima se pristupa ili koji se pohranjuju, šalju ili na drugi način obrađuju u vezi s pružanjem upravljanih sigurnosnih usluga od slučajnog ili neovlaštenog pristupa, pohranjivanja, objave, uništavanja, druge obrade, gubitka, izmjene ili nedostatka dostupnosti;

(d) osigurati da podaci, usluge i funkcije te pristup podacima, uslugama i funkcijama pravodobno budu ponovno dostupni u slučaju fizičkog ili tehničkog incidenta;

(e) osigurati da ovlaštene osobe, programi ili strojevi mogu pristupati isključivo

podacima, uslugama ili funkcijama na koje se odnose njihova prava pristupa;

(f) evidentiranje i mogućnost provjere kojim je podacima tko i kad pristupio, koristio ih ili ih na drugi način obrađivao;

(g) osigurati da su IKT proizvodi, IKT usluge i IKT procesi koji se koriste za pružanje upravljanih sigurnosnih usluga sigurni po zadanim postavkama i dizajnom ***i da imaju osiguran ažuriran softver i hardver,*** da ne sadrže poznate ranjivosti te da imaju najnovija sigurnosna ažuriranja;”

(10) Članak 52. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

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

(b) stavak 3. zamjenjuje se sljedećim:

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

(c) stavci 5., 6. i 7. zamjenjuju se sljedećim:

„5. Europskim kibersigurnosnim certifikatom ili EU izjavom o sukladnosti koji se odnose na ‚osnovnu’ jamstvenu razinu pruža se jamstvo da IKT proizvodi, IKT usluge, IKT procesi i upravljane sigurnosne usluge za koje su taj certifikat ili ta EU izjava o sukladnosti izdani ispunjavaju odgovarajuće sigurnosne zahtjeve, uključujući sigurnosne funkcionalnosti, te da su bili podvrgnuti evaluaciji na razini čija je svrha

svođenje na najmanju moguću mjeru poznatih osnovnih rizika za incidente i kibernapade. Aktivnosti evaluacije koje treba poduzeti obuhvaćaju barem preispitivanje tehničke dokumentacije. Ako takvo preispitivanje nije odgovarajuće, poduzimaju se zamjenske aktivnosti evaluacije s istovjetnim učinkom.

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

7. Europskim kibersigurnosnim certifikatom koji se odnosi na ‚visoku' jamstvenu razinu pruža se jamstvo da IKT proizvodi, IKT usluge, IKT procesi i upravljane sigurnosne usluge za koje je taj certifikat izdan ispunjavaju odgovarajuće sigurnosne zahtjeve, uključujući sigurnosne funkcionalnosti, te da su bili podvrgnuti evaluaciji na razini čija je svrha svođenje na najmanju moguću mjeru rizika od najsuvremenijih kibernapada koje provode subjekti znatnih vještina i resursa. Aktivnosti evaluacije koje treba poduzeti obuhvaćaju barem sljedeće: preispitivanje radi dokazivanja nepostojanja javno poznatih ranjivosti; testiranje radi dokazivanja da IKT proizvodi, IKT usluge, IKT procesi ili upravljane sigurnosne usluge na ispravan način i na najsuvremenijoj razini primjenjuju potrebne sigurnosne funkcionalnosti; procjenu njihove otpornosti na napad vještih napadača, za koju se koristi penetracijsko

testiranje. Ako bilo koja od tih aktivnosti evaluacije nije odgovarajuća, poduzimaju se zamjenske aktivnosti s istovjetnim učinkom.”;

(11) u članku 53. stavci 1., 2. i 3. zamjenjuju se sljedećim:

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

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

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

(12) u članku 54. stavak 1. mijenja se kako slijedi:

(a) točka (a) zamjenjuje se sljedećim:

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

(b) točka (j) zamjenjuje se sljedećim:

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

(c) točka (l) zamjenjuje se sljedećim:

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

(d) točka (o) zamjenjuje se sljedećim:

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

(e) točka (q) zamjenjuje se sljedećim:

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

(13) članak 56. mijenja se kako slijedi:

(a) stavak 1. zamjenjuje se sljedećim:

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

(b) stavak 3. mijenja se kako slijedi:

i. prvi podstavak zamjenjuje se sljedećim:

Komisija redovito ocjenjuje učinkovitost i upotrebu donesenih europskih

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

ii. treći podstavak mijenja se kako slijedi:

(aa) točka (a) zamjenjuje se sljedećim:

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

(bb) točka (d) zamjenjuje se sljedećim:

„(d) uzima u obzir sve rokove za provedbu, prijelazne mjere i razdoblja, posebno vodeći računa o mogućem učinku mjere na proizvođače ili pružatelje IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga, uključujući ***posebne interese i potrebe mikropoduzeća te MSP-ova***;”**;**

iii. dodaje se sljedeći podstavak:

„S obzirom na treći podstavak točku (d) ovog članka, Komisija osigurava odgovarajuću financijsku potporu u regulatornom okviru postojećih programa Unije, posebno kako bi se smanjilo financijsko opterećenje za mikropoduzeća i MSP-ove, uključujući start-up poduzeća koja djeluju u području upravljanih sigurnosnih usluga.”;

(c) stavci 7. i 8. zamjenjuju se sljedećim:

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

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

(14) u članku 57. stavci 1. i 2. zamjenjuju se sljedećim:

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

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

(15) članak 58. mijenja se kako slijedi:

(a) stavak 7. mijenja se kako slijedi:

i. točke (a) i (b) zamjenjuju se sljedećim:

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

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

ii. točka (h) zamjenjuje se sljedećim:

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

(b) stavak 9. zamjenjuje se sljedećim:

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

(16) u članku 59. stavku 3. točke (b) i (c) zamjenjuju se sljedećim:

„(b) postupaka za nadzor i provedbu pravila o praćenju sukladnosti IKT proizvoda,

IKT usluga, IKT procesa i upravljanih sigurnosnih usluga s europskim kibersigurnosnim certifikatima na temelju članka 58. stavka 7. točke (a);

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

(16a) umeće se sljedeći članak:

„Članak 65.a
Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

2. Ovlast za donošenje delegiranih akata iz članka 49. stavka 7. dodjeljuje se Komisiji na razdoblje od pet godina počevši od ... [datum stupanja na snagu izmijenjene Uredbe]. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 49. stavka 7. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u Službenom listu Europske unije ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

6. Delegirani akt donesen na temelju članka 49. stavka 7. stupa na snagu samo

ako ni Europski parlament ni Vijeće u roku od dva mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za [dva mjeseca] na inicijativu Europskog parlamenta ili Vijeća.;"

(17) Članak 67. zamjenjuje se sljedećim:

„Članak 67.

Ocjenjivanje i revizija

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

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

3. Ocjenjuje se i:

(a) učinkovitost i djelotvornost postupaka koji prethode savjetovanju, pripremi i donošenju europskih programa kibersigurnosne certifikacije, kao i načini za poboljšanje i ubrzavanje tih postupaka;

(b) jesu li ključni zahtjevi kibersigurnosti za pristup unutarnjem tržištu nužni kako bi se spriječio ulazak na tržište Unije IKT proizvoda, IKT usluga, IKT procesa i upravljanih sigurnosnih usluga koji ne ispunjavaju temeljne zahtjeve u pogledu kibersigurnosti.

4. Do 28. lipnja 2024., a nakon toga svake tri godine Komisija Europskom parlamentu, Vijeću i Upravljačkom odboru prosljeđuje izvješće o

ocjenjivanju zajedno sa svojim zaključcima. Nalazi tog izvješća javno se obznanjuju."

Članak 2.

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

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

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*

OBRAZLOŽENJE

Izvjestiteljica podržava Prijedlog uredbe Europskog parlamenta i Vijeća o izmjeni Uredbe (EU) 2019/811 u pogledu upravljanih sigurnosnih usluga i uviđa da je potrebno ažurirati i ojačati europski program kibersigurnosne certifikacije tako da se njime obuhvate važne i rastuće industrijske usluge. S obzirom na to da su pojedine države članice već počele donositi programe certificiranja za upravljane sigurnosne usluge, izvjestiteljica smatra da je ova izmjena Akta o kibersigurnosti ključna kako bi se spriječile znatne razlike u nacionalnim programima, što bi dovelo do određene fragmentacije tržišta, koja je protivna gospodarskim te ujedno strateškim interesima Unije.

U tom je pogledu jasno da se ovim prijedlogom namjerava dopuniti Akt o kibersolidarnosti, a posebno će proširenje europskog programa kibersigurnosne certifikacije omogućiti da upravljane sigurnosne usluge, koje odgovaraju „pouzdanim pružateljima” u Aktu o kibersolidarnosti, imaju važnu ulogu u budućoj kibersigurnosnoj pričuvi EU-a. Stoga je ovaj prijedlog vrlo važan i za poticanje širih kapaciteta Unije u području kibersigurnosti, što je ključno za suzbijanje potencijalnih prijetnji u promjenjivoj geopolitičkoj situaciji.

U okviru prijedloga Komisije cilj je izvjestiteljice konsolidirati i dodatno pojasniti tu ciljanu izmjenu Akta o kibersigurnosti. To je vidljivo iz izvjestiteljičinih izmjena definicije upravljanih sigurnosnih usluga, u kojoj se pojašnjava da su one „eksternalizirane”, dok se istodobno detaljnije objašnjava što se može uključiti u tu definiciju. Predloženim izmjenama u pogledu priznavanja međunarodnih kibersigurnosnih standarda nastoji se potaknuti veća razina povjerenja te istovremeno nastaviti s razvojem sveobuhvatnih pravila EU-a.

U ovom nacrtu izvješća veći se naglasak stavlja na rješavanje problema nedostatka vještina te potporu mikropoduzećima, malim i srednjim poduzećima. Podnesene izmjene temelje se na već implicitnoj potrebi za vještinama u programu kibersigurnosne certifikacije s obzirom na „potrebn[u] razin[u] kompetentnosti, stručnosti i iskustva […] osoblj[a] s vrlo visokom razinom relevantnog tehničkog znanja i profesionalnog integriteta.”. Izvjestiteljica smatra da, uz istodobno poticanje suradnje među svim uključenim akterima te između država članica, privatnog sektora, akademske zajednice i istraživačkih institucija, europski program certifikacije mora biti pokretač novog plana za osposobljavanje i osnaživanje radne snage, uz

prikupljanje više podataka o potrebnim vještinama i doprinos uklanjanju rodnog jaza u području STEM-a.

Istodobno bi mikropoduzeća te mala i srednja poduzeća, koja čine okosnicu europskog gospodarstva i svakako imaju pozitivnu ulogu u industriji kibersigurnosti, trebala dobiti odgovarajuću financijsku potporu u regulatornom okviru postojećih programa Unije kako bi se smanjilo svako nerazmjerno financijsko opterećenje koje bi mogla osjećati.

21.9.2023.

PISMO ODBORA ZA UNUTARNJE TRŽIŠTE I ZAŠTITU POTROŠAČA

g. Cristian-Silviu Buşoi
Predsjednik
Odbor za industriju, istraživanje i energetiku
BRUXELLES

Predmet: Mišljenje o Prijedlogu uredbe Europskog parlamenta i Vijeća o izmjeni Uredbe (EU) 2019/881 u pogledu upravljanih sigurnosnih usluga (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Poštovani g. predsjedniče,

u okviru navedenog predmeta, Odbor za unutarnje tržište i zaštitu potrošača zadužen je za podnošenje mišljenja Vašem odboru. Na svojoj sjednici od 23. svibnja 2023. to je mišljenje odlučio podnijeti u obliku pisma. Odbor je pitanje razmotrio na svojoj sjednici od 19. rujna 2023. te je na toj istoj sjednici usvojio mišljenje.

Za vrijeme te iste sjednice[10], Odbor je odlučio pozvati Odbor za industriju, istraživanje i energetiku (ITRE) da kao nadležni odbor u svojem zakonodavnom izvješću uzme u obzir sljedeća zapažanja.

S poštovanjem,

Anna Cavazzini

PRIJEDLOZI

Odbor za unutarnje tržište i zaštitu potrošača poziva Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće prijedloge:

A. budući da je Komisija 18. travnja 2023. objavila zakonodavni prijedlog o upravljanim sigurnosnim uslugama koji uključuje ciljane izmjene Akta EU-a o kibersigurnosti[11];

B. budući da je o zakonodavnom prijedlogu Akta EU-a o kibersigurnosti

[10] Na konačnom glasovanju nazočni su bili: Anna Cavazzini (predsjednica), Andrus Ansip (potpredsjednik), Krzysztof Hetman (potpredsjednik), Alex Agius Saliba, João Albuquerque, Pablo Arias Echeverría, Laura Ballarín Cereza, Alessandra Basso, Brando Benifei, Biljana Borzan, Vlad Marius Botoş, Deirdre Clune, Dita Charanzová, David Cormand, Carlo Fidanza, Malte Gallée, Sandro Gozi, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Beata Mazurek, Leszek Miller, Anne Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Tom Vandenkendelaere, Kim Van Sparrentak.
[11] https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:52023PC0208

(2017/0225(COD))[12] Odbor za unutarnje tržište i zaštitu potrošača (IMCO) u skladu s bivšim člankom 54. Poslovnika podnio mišljenje nadležnom Odboru za industriju, istraživanje i energetiku (ITRE) sa zajedničkim nadležnostima u vezi s okvirom za kibersigurnosnu certifikaciju, s obzirom na jasnu nadležnost odbora IMCO u pogledu programa certifikacije i, općenito, normizacije, nadzora tržišta i provedbe jedinstvenog digitalnog tržišta;

C. budući da se Aktom EU-a o kibersigurnosti[13] nastoji postići 1) visoka razina kibersigurnosti, kiberotpornosti i povjerenja u EU utvrđivanjem ciljeva, zadaća i organizacijskih pitanja za ojačanu i preimenovanu Agenciju Europske unije za kibersigurnost (ENISA), s novim trajnim mandatom, i 2) okvir za dobrovoljne europske programe kibersigurnosne certifikacije za proizvode, usluge i procese informacijske i komunikacijske tehnologije (IKT);

D. budući da se predloženim ciljanim izmjenama u područje primjene Akta EU-a o kibersigurnosti žele uključiti upravljane sigurnosne usluge i dodati definicija tih usluga koja je usko usklađena s definicijom iz Direktive NIS 2[14]; budući da bi izmjene omogućile Komisiji da provedbenim aktima donese europski program kibersigurnosne certifikacije za upravljane sigurnosne usluge, što je Aktom o kibersigurnosti već omogućeno za proizvode informacijske i komunikacijske tehnologije (IKT proizvodi), IKT usluge i IKT procese.

E. budući da upravljane sigurnosne usluge imaju sve važniju ulogu u sprečavanju i ublažavanju kibersigurnosnih incidenata;

1. potvrđuje da je Vijeće 23. svibnja 2022.[15] pozvalo na povećanje ukupne razine kibersigurnosti u EU-u olakšavanjem pojave i razvoja pouzdanih pružatelja kibersigurnosnih usluga; smatra da su, među ostalim, rat u Ukrajini, trenutačni geopolitički kontekst i stalne prijetnje režima trećih zemalja, kao i stalno rastuće tržište digitalnih tehnologija i digitalna transformacija procesa općenito doveli do potrebe za višom razinom kibersigurnosti u EU-u i njegovim državama članicama; preporučuje Komisiji da poduzme proaktivne mjere za potporu razvoju pouzdanih pružatelja kibersigurnosnih usluga, kao što su financiranje istraživanja i razvoja, programi osposobljavanja za izgradnju vještina u području kibersigurnosti i poticaji za poduzeća da ulažu u kibersigurnost; predlaže da EU ojača suradnju s NATO-om i drugim međunarodnim partnerima kako bi odgovorio na kiberprijetnje režima trećih zemalja, uključujući razmjenu obavještajnih podataka o prijetnjama, zajedničke vježbe i koordinirane odgovore na kibernapade;

2. naglašava da je certificiranje upravljanih sigurnosnih usluga, koje se temelji na nediskriminirajućim pravilima i odražava europske i međunarodne standarde, ključno za izgradnju i jamčenje povjerenja u kvalitetu tih usluga, posebno u cilju postizanja visoke razine zaštite potrošača; napominje da su neke države članice već donijele programe certifikacije za upravljane sigurnosne usluge i da je stoga ključno izbjeći rascjepkanost na unutarnjem tržištu i nedosljednosti, koje mogu utjecati na industriju i poduzeća u

[12] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225(OLP)
[13] SL L 151, 7.6.2019., str. 15.
[14] SL L 333/810, 27.12.2022.
[15] 9364/22

području kibersigurnosti, te omogućiti usklađen pristup stvaranjem europskog programa kibersigurnosne certifikacije za takve usluge; traži da se u okvir za kibersigurnosnu certifikaciju uključe najbolje prakse iz postojećih nacionalnih programa certifikacije i da se on razvije uz savjetovanje s ključnim dionicima u industriji kibersigurnosti;

3. ističe da u područjima kao što su odgovor na incidente, penetracijska testiranja, revizije sigurnosti i savjetovanje, pružatelji upravljane sigurnosne usluge imaju važnu ulogu među pružateljima usluga u pomaganju subjektima u njihovim nastojanjima da spriječe i otkriju kiberincidente te odgovore na njih ili se oporave od njih. smatra da se, s obzirom na to da sve više poduzeća ima poteškoća s održavanjem različitih složenih softverskih sustava i međusobno povezanih korporativnih mreža, nužno oslanjaju na pružatelje upravljanih sigurnosnih usluga te bi se stoga takvi pružatelji trebali smatrati ključnim elementom u kibersigurnosnom ekosustavu EU-a; primjećuje, međutim, da su pružatelji upravljanih sigurnosnih usluga i sami bili meta kibernapada te zbog svoje bliske integracije u rad svojih klijenata predstavljaju poseban kibersigurnosni rizik;

4. podsjeća na važnost nedavno donesene Direktive NIS 2 kako bi se osigurala veća razina kiberotpornosti u cijeloj Uniji; poziva na brzo donošenje i provedbu provedbenih akata u skladu s tom Direktivom kako bi se osiguralo da pružatelji upravljanih sigurnosnih usluga poštuju zahtjeve Direktive o mjerama upravljanja kibersigurnosnim rizicima;

5. preporučuje da se od pružatelja upravljanih sigurnosnih usluga zahtijeva da se pridržavaju relevantnih kibersigurnosnih standarda i da se podvrgavaju redovitim revizijama kako bi se osiguralo da su njihovi sustavi sigurni i da štite ne samo same pružatelje nego i subjekte kojima služe; smatra da bi se takvim revizijama trebalo ocijeniti poštuju li pružatelji usluga okvir za kibersigurnosnu certifikaciju na razini EU-a i njihovu sposobnost da zaštite svoje sustave i sustave svojih klijenata od kiberprijetnji;

6. pozdravlja zakonodavni prijedlog o upravljanim sigurnosnim uslugama, čiji je cilj poboljšati kvalitetu upravljanih sigurnosnih usluga i povećati njihovu usporedivost u korist pravilnog funkcioniranja unutarnjeg tržišta i provedbe jedinstvenog digitalnog tržišta; naglašava da certifikacija upravljanih sigurnosnih usluga nije važna samo za postupak odabira za kibersigurnosnu pričuvu EU-a, nego je i ključan pokazatelj kvalitete i povjerenja za privatne i javne subjekte koji namjeravaju kupovati takve usluge.

7. napominje da se prijedlogom jača uloga ENISA-e, koja bi trebala podupirati i promicati razvoj i provedbu politike Unije o kibersigurnosnoj certifikaciji IKT proizvoda, usluga, procesa i upravljanih sigurnosnih usluga redovitim praćenjem razvoja u povezanim područjima normizacije i predlaganjem tehničkih specifikacija ako norme nisu dostupne; predlaže da se ENISA-i dodijele dodatna sredstva i ovlasti za izvršavanje njezine proširene uloge, uključujući financiranje istraživanja i razvoja, te jasan mandat za koordinaciju s nacionalnim agencijama za kibersigurnost i dionicima iz industrije; ističe ključnu ulogu timova za odgovor na računalne sigurnosne incidente (CSIRT-ovi) u postizanju predvidljivog i sigurnog digitalnog prostora za poduzeća i građane;

8. poziva Komisiju i ENISA-u da podrže i osiguraju dosljednu provedbu europskog programa kibersigurnosne certifikacije koji se temelji na nediskriminirajućim pravilima i odražava europske i međunarodne norme za samoocjenu sukladnosti koju provodi proizvođač ili pružatelj IKT proizvoda, usluga, procesa ili upravljanih sigurnosnih usluga,

u skladu s Aktom EU-a o kibersigurnosti; smatra da bi se provedbom trebali nadoknaditi troškovi akreditacije i potaknuti veći broj proizvođača ili pružatelja usluga na sudjelovanje u programu;

9. ističe da bi svaki program certifikacije trebao biti osmišljen tako da stimulira i potiče sve dionike uključene u predmetni sektor da razvijaju i usvajaju redovno ažurirane sigurnosne standarde, tehničke norme i načela integrirane sigurnosti i privatnosti u svim fazama životnog vijeka proizvoda ili usluge; ističe da pri razvoju takvih načela na sustavniji način treba uzeti u obzir doprinos civilnog društva i neovisnih istraživača u području sigurnosti; smatra da bi programi certifikacije trebali biti usklađeni s drugim europskim programima kibersigurnosne certifikacije donesenima u skladu s Aktom EU-a o kibersigurnosti te da bi se njima trebalo izbjegavati nerazmjerno opterećenje za pružatelje; preporučuje da programi certifikacije uključuju jasne i detaljne smjernice o tome kako provesti načela integrirane sigurnosti i integrirane privatnosti, ako su takve smjernice u skladu s odredbama kojima se utvrđuje okvir za europske programe kibersigurnosti u Aktu EU-a o kibersigurnosti; predlaže da se, ako je to potrebno i razmjerno, programi certificiranja sastoje od mehanizma za stalno poboljšanje, kao što su redovita preispitivanja i ažuriranja sigurnosnih standarda i tehničkih normi; smatra da bi se mehanizmom trebala uzeti u obzir najnovija kretanja u području kibersigurnosnih prijetnji i tehnologija; potiče da se u svaki program certificiranja uključe mjere za promicanje transparentnosti i odgovornosti, kao što su javno objavljivanje rezultata certificiranja i kazne za neusklađenost;

10. poziva na uvođenje dobrovoljne oznake povjerenja EU-a za certificirane IKT proizvode, usluge, procese i upravljane sigurnosne usluge; u tom pogledu ističe da bi oznaka mogla pomoći u poboljšanju informiranosti o kibersigurnosti na cijelom unutarnjem tržištu i dati konkurentsku prednost poduzećima s dobrim kibersigurnosnim kvalifikacijama; predlaže da se oznaka povjerenja EU-a osmisli tako da bude lako prepoznatljiva i razumljiva potrošačima i poduzećima;

11. preporučuje Komisiji i ENISA-i da uspostave poseban program istraživanja i razvoja za kibersigurnost; preporučuje da Komisija i ENISA uspostave okvir za procjenu kibersigurnosnih rizika za poduzeća koji bi sadržavao smjernice o tome kako utvrditi, procijeniti i ublažiti kibersigurnosne rizike i koji bi mogao biti prilagođen različitim sektorima i veličinama poduzeća; predlaže da Komisija i ENISA pruže pomoć i podršku državama članicama u uspostavi mehanizma za izvješćivanje o kibersigurnosnim incidentima za potrošače i poduzeća kako bi se olakšalo prikupljanje podataka o kiberincidentima, koji bi se mogli upotrijebiti za poboljšanje kibersigurnosnih politika i praksi.

POSTUPAK U NADLEŽNOM ODBORU

Naslov	Izmjena Uredbe (EU) 2019/881 u pogledu upravljanih sigurnosnih usluga
Referentni dokumenti	COM(2023)0208 – C9-0137/2023 – 2023/0108(COD)
Datum podnošenja EP-u	19.4.2023.
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 1.6.2023.
Odbori koji daju mišljenje Datum objave na plenarnoj sjednici	IMCO LIBE 1.6.2023. 1.6.2023.
Odbori koji nisu dali mišljenje Datum odluke	LIBE 30.5.2023.
Izvjestitelji Datum imenovanja	Josianne Cutajar 2.5.2023.
Razmatranje u odboru	19.7.2023. 19.9.2023.
Datum usvajanja	25.10.2023.
Rezultat konačnog glasovanja	+: 57 –: 0 0: 2
Zastupnici nazočni na konačnom glasovanju	Matteo Adinolfi, Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Michael Bloss, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, Henrike Hahn, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Thierry Mariani, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Sara Skyttedal, Riho Terras, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Zamjenici nazočni na konačnom glasovanju	Pascal Arimont, Tiziana Beghin, Franc Bogovič, Damien Carême, Martina Dlabajová, Francesca Donato, Matthias Ecke, Nicolás González Casares, Ladislav Ilčić, Luděk Niedermayer, Emma Wiesner
Zamjenici nazočni na konačnom glasovanju prema čl. 209. st. 7.	Asim Ademov, Aušra Maldeikienė, Irène Tolleret
Datum podnošenja	26.10.2023.

POIMENIČNO KONAČNO GLASOVANJE U NADLEŽNOM ODBORU

57	+
ECR	Ladislav Ilčić
ID	Matteo Adinolfi, Paolo Borchia, Marie Dauchy, Thierry Mariani
NI	Tiziana Beghin, Francesca Donato, Clara Ponsatí Obiols
PPE	Asim Ademov, Pascal Arimont, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Aušra Maldeikienė, Luděk Niedermayer, Markus Pieper, Sara Skyttedal, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Irène Tolleret, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia, Carlos Zorrinho
The Left	Marc Botenga, Marina Mesure
Verts/ALE	Michael Bloss, Damien Carême, Ciarán Cuffe, Henrike Hahn, Niklas Nienass, Ville Niinistö, Manuela Ripa

0	-

2	0
ECR	Johan Nissinen
ID	Markus Buchheit

Korišteni znakovi:
+ : za
- : protiv
0 : suzdržani