2025/37

15.1.2025.

UREDBA (EU) 2025/37 EUROPSKOG PARLAMENTA I VIJEĆA

od 19. prosinca 2024.

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 ([1]),

nakon savjetovanja s Odborom regija,

u skladu s redovnim zakonodavnim postupkom ([2]),

budući da:

(1) Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća ([3]) 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.

(2) Kako bi se osigurala otpornost Unije na kibernapade i spriječile eventualne ranjivosti na unutarnjem tržištu, ovom se Uredbom namjerava dopuniti horizontalni regulatorni okvir kojim se utvrđuju sveobuhvatni kibersigurnosni zahtjevi za proizvode s digitalnim elementima u skladu s Uredbom (EU) 2024/2847 Europskog parlamenta i Vijeća ([4]), kojom se utvrđuju sigurnosni ciljevi za upravljane usluge kao i primjenu i pouzdanost tih usluga.

(3) Upravljane sigurnosne usluge pružaju pružatelji upravljanih sigurnosnih usluga kako su definirani u članku 6. točki 40. Direktive (EU) 2022/2555 Europskog parlamenta i Vijeća ([5]). Stoga bi definicija upravljanih sigurnosnih usluga u ovoj Uredbi trebala biti u skladu s definicijom pružatelja upravljanih sigurnosnih usluga iz Direktive (EU) 2022/2555. Te usluge sastoje se od obavljanja aktivnosti povezanih s upravljanjem kibersigurnosnim rizicima klijenata ili pružanja pomoći za te aktivnosti i sve su važnije u sprečavanju i ublažavanju incidenata. Zbog toga se pružatelji tih usluga smatraju ključnim ili važnim subjektima koji pripadaju sektoru visoke kritičnosti u skladu s Direktivom (EU) 2022/2555. Kako je navedeno u uvodnoj izjavi 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 predstavljaju poseban kibersigurnosni rizik zbog svoje bliske integracije u rad svojih klijenata. Važno je, stoga, da ključni i važni subjekti u smislu Direktive (EU) 2022/2555 postupaju s većom pažnjom pri odabiru pružatelja upravljanih sigurnosnih usluga.

([1]) SL C 349, 29.9.2023., str. 167.
([2]) Stajalište Europskog parlamenta od 24. travnja 2024. (još nije objavljeno u Službenom listu) i odluka Vijeća od 2. prosinca 2024.
([3]) 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.).
([4]) Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni Uredaba (EU) br. 168/2013 i (EU) 2019/1020 i Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti) (SL L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) 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.).

(4) Definicija upravljanih sigurnosnih usluga na temelju ove Uredbe uključuje neiscrpan popis upravljanih sigurnosnih usluga koje bi mogle biti prihvatljive za europske programe kibersigurnosne certifikacije, kao što su rješavanje incidenata, penetracijsko testiranje, revizije sigurnosti i savjetovanje povezano s tehničkom potporom. Upravljane sigurnosne usluge mogle bi obuhvaćati kibersigurnosne usluge kojima se podupiru pripravnost za, sprečavanje, otkrivanje, analiza i ublažavanje, odgovor na kiberincidente i oporavak od njih. Pružanje obavještajnih podataka o kiberprijetnjama i procjena rizika u vezi s tehničkom potporom također bi se mogli smatrati upravljanim sigurnosnim uslugama. Za različite upravljane sigurnosne usluge mogli bi postojati zasebni europski programi kibersigurnosne certifikacije. Europski kibersigurnosni certifikati izdani u skladu s takvim programima trebali bi se odnositi na posebne upravljane sigurnosne usluge određenog pružatelja tih usluga.

(5) Pružatelji upravljanih sigurnosnih usluga mogu također imati važnu ulogu u vezi s mjerama Unije kojima se podupiru odgovor i početni oporavak u slučajevima značajnih incidenata i kibersigurnosnih incidenata velikih razmjera, oslanjajući se na usluge pouzdanih privatnih pružatelja usluga i testiranje kritičnih subjekata na potencijalne ranjivosti na temelju koordiniranih procjena sigurnosnih rizika na razini Unije. Certifikacija upravljanih sigurnosnih usluga mogla bi imati ulogu u odabiru pouzdanih pružatelja upravljanih sigurnosnih usluga kako su definirani u Uredbi (EU) 2025/38 Europskog parlamenta i Vijeća ([6]).

(6) Certifikacija upravljanih sigurnosnih usluga nije važna samo za postupak odabira za pričuvu EU-a za kibernetičku sigurnost uspostavljenu Uredbom (EU) 2025/38, nego je i ključan pokazatelj kvalitete privatnim i javnim subjektima koji namjeravaju kupovati takve usluge. S obzirom na kritičnost upravljanih sigurnosnih usluga i osjetljivost obrađenih podataka, certifikacija bi potencijalnim klijentima mogla biti važan pokazatelj i jamstvo pouzdanosti tih usluga. Svrha europskih programa kibersigurnosne certifikacije za upravljane sigurnosne usluge jest da doprinose izbjegavanju fragmentacije unutarnjeg tržišta. Stoga je cilj ove Uredbe poboljšanje funkcioniranja unutarnjeg tržišta.

(7) Europski programi kibersigurnosne certifikacije za upravljane sigurnosne usluge trebali bi dovesti do uvođenja tih usluga i do povećanja tržišnog natjecanja među pružateljima upravljanih sigurnosnih usluga. Ne dovodeći u pitanje cilj osiguravanja dostatnih i odgovarajućih razina relevantnog tehničkog znanja i profesionalnog integriteta takvih pružatelja, takvi programi certifikacije trebali bi stoga olakšati ulazak na tržište i ponudu upravljanih sigurnosnih usluga pojednostavnjenjem, u mjeri u kojoj je to moguće, potencijalnog regulatornog, administrativnog i financijskog opterećenja s kojim bi se pružatelji, posebno mala i srednja poduzeća (MSP-ovi), uključujući mikropoduzeća, mogli suočiti prilikom pružanja upravljanih sigurnosnih usluga. Osim toga, kako bi se potaknulo uvođenje upravljanih sigurnosnih usluga i potražnja za njima, europskim programima kibersigurnosne certifikacije trebalo bi doprinijeti njihovoj pristupačnosti, posebno za manje aktere, kao što su MSP-ovi, uključujući mikropoduzeća, te lokalne i regionalne vlasti koje imaju ograničene kapacitete i resurse, ali koje su sklonije povredama kibersigurnosti s financijskim, pravnim, reputacijskim i operativnim posljedicama.

(8) Važno je pružiti potporu MSP-ovima, uključujući mikropoduzeća, u provedbi ove Uredbe i privlačenju specijaliziranih vještina i stručnog znanja u području kibersigurnosti potrebnih za pružanje upravljanih sigurnosnih usluga u skladu sa zahtjevima utvrđenima u ovoj Uredbi. Programom Digitalna Europa uspostavljenim Uredbom (EU) 2021/694 Europskog parlamenta i Vijeća ([7]) i drugim relevantnim programima Unije predviđa se da bi Komisija trebala uspostaviti financijsku i tehničku potporu kojom se tim poduzećima omogućuje da doprinesu rastu gospodarstva Unije i jačanju zajedničke razine kibersigurnosti u Uniji, među ostalim pojednostavnjenjem financijske potpore iz programa Digitalna Europa i drugih relevantnih programa Unije te podupiranjem MSP-ova, uključujući mikropoduzeća.

(9) Europskim programima kibersigurnosne certifikacije za upravljane sigurnosne usluge trebalo bi se doprinijeti dostupnosti sigurnih i visokokvalitetnih usluga kojima se jamči sigurna digitalna tranzicija i postizanju ciljeva utvrđenih u programu politike za digitalno desetljeće do 2030. uspostavljenom Odlukom (EU) 2022/2481 Europskog parlamenta i Vijeća ([8]), posebno u pogledu cilja da 75 % poduzeća iz Unije počne upotrebljavati usluge

([6]) Uredba (EU) 2025/38 Europskog parlamenta i Vijeća od 19. prosinca 2024. o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih te izmjeni Uredbe (EU) 2021/694 (Akt o kibernetičkoj solidarnosti) (SL L, 2025/38, 15.1.2025., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Uredba (EU) 2021/694 Europskog parlamenta i Vijeća od 29. travnja 2021. o uspostavi programa Digitalna Europa te o stavljanju izvan snage Odluke (EU) 2015/2240 (SL L 166, 11.5.2021., str. 1.).

([8]) Odluka (EU) 2022/2481 Europskog parlamenta i Vijeća od 14. prosinca 2022. o uspostavi programa politike za digitalno desetljeće do 2030. (SL L 323, 19.12.2022., str. 4.).

računalstva u oblaku, velike količine podataka ili umjetnu inteligenciju, da više od 90 % MSP-ova, uključujući mikropoduzeća, dosegne barem osnovnu razinu digitalne intenzivnosti te da ključne javne usluge budu dostupne na internetu.

(10) Uz primjenu IKT proizvoda, IKT usluga ili IKT procesa, upravljane sigurnosne usluge često nude dodatne mogućnosti koje se oslanjaju na kompetencije, stručnost i iskustvo osoblja pružatelja takvih usluga. 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 europskim programima kibersigurnosne certifikacije obuhvate svi aspekti upravljanih sigurnosnih usluga, potrebno je izmijeniti Uredbu (EU) 2019/881. U obzir bi trebalo uzeti rezultate i preporuke evaluacije i preispitivanja predviđenih Uredbom (EU) 2019/881.

(11) Kako bi se olakšao rast pouzdanog unutarnjeg tržišta i istodobno stvorila partnerstva s trećim zemljama istomišljenicama, postupak certifikacije uspostavljen okvirom europskog programa kibersigurnosne certifikacije iz Uredbe (EU) 2019/881 trebalo bi provesti na način kojim bi se omogućilo međunarodno priznavanje i usklađenost s međunarodnim standardima.

(12) Kako je potvrđeno u Komunikaciji Komisije od 18. travnja 2023. naslovljenoj Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije („Akademija za vještine u području kibersigurnosti”), Unija se suočava s nedostatkom talenata, koji karakterizira manjak kvalificiranih stručnjaka, i s prijetećom situacijom koja se brzo mijenja. Obrazovni sadržaji i formalno osposobljavanje razlikuju se, a znanje se može steći na različite načine: formalno, na primjer na sveučilištima ili tečajevima ili neformalno, na primjer osposobljavanjem na radnome mjestu ili radnim iskustvom u relevantnom području. Stoga bi, kako bi se olakšala pojava visokokvalitetnih upravljanih sigurnosnih usluga i kako bi se dobio bolji pregled sastava radne snage Unije u području kibersigurnosti, bilo važno ojačati suradnju između država članica, Komisije, Agencije Europske unije za kibersigurnost osnovane Uredbom (EU) 2019/881 (ENISA) i dionika, uključujući iz privatnog sektora i akademske zajednice, 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. Takvom bi se suradnjom olakšala mobilnost stručnjaka u području kibersigurnosti unutar Unije te integracija znanja i osposobljavanja u području kibersigurnosti u obrazovne programe, te istodobno osigurao 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. Važno je da se takvom suradnjom nastoji privući više žena i djevojčica u tom području i doprinijeti uklanjanju rodnog jaza u znanosti, tehnologiji, inženjerstvu i matematici te da je privatni sektor usmjeren na osposobljavanje na radnome mjestu koje obuhvaća najtraženije vještine, uključujući javnu upravu i novoosnovana poduzeća te MSP-ove, uključujući mikropoduzeća. Osim toga, važno je da pružatelji tih usluga i države članice surađuju i doprinose prikupljanju podataka o stanju tržišta rada u području kibersigurnosti i njegovu razvoju.

(13) ENISA ima važnu ulogu u pripremi prijedloga europskih programa certifikacije. Komisija bi pri pripremi nacrta općeg proračuna Unije trebala ocijeniti potrebna proračunska sredstva za plan radnih mjesta ENISA-e u skladu s postupkom utvrđenim u članku 29. Uredbe (EU) 2019/881.

(14) Ovom se Uredbom predviđaju ciljane izmjene Uredbe (EU) 2019/881 kako bi se omogućila uspostava europskih programa kibersigurnosne certifikacije za upravljane sigurnosne usluge. Pritom se utvrđuju i pojašnjavaju određene odredbe te uredbe o pripremi i funkcioniranju svih europskih programa kibersigurnosne certifikacije kako bi se osigurala njihova transparentnost i otvorenost. Potonje izmjene, koje su ograničene na specifikaciju ili pojašnjenje Uredbe (EU) 2019/881, posebno izmjene koje se odnose na informacije koje ENISA treba pružati pri podnošenju prijedloga programa, *ad hoc* radne skupine osnovane za svaki prijedlog programa, te informacije i savjetovanja u pogledu europskih programa kibersigurnosne certifikacije, ni na koji način ne bi trebale prejudicirati širu evaluaciju i preispitivanje te uredbe, što se zahtijeva na temelju članka 67. te uredbe, posebno evaluaciju učinka, djelotvornosti i učinkovitosti glave te uredbe koja se odnosi na okvir kibersigurnosne certifikacije. Evaluacija i preispitivanje u pogledu te glave trebali bi se temeljiti na opsežnom savjetovanju s dionicima te potpunoj i temeljitoj analizi uključenih postupaka.

(15) S obzirom na to da cilj ove Uredbe, to jest omogućiti uspostavu europskih programa kibersigurnosne certifikacije za upravljane sigurnosne usluge, ne mogu dostatno ostvariti države članice, nego se zbog njegova opsega i učinaka on na bolji način može 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 utvrđenim u tom članku, ova Uredba ne prelazi ono što je potrebno za ostvarivanje tih ciljeva.

(16) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([9]) te je on dao mišljenje 10. siječnja 2024.,

DONIJELI SU OVU UREDBU:

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 ili 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 te se sastoji od obavljanja aktivnosti povezanih s upravljanjem kibersigurnosnim rizicima, kao što su rješavanje incidenata, penetracijska testiranja, revizije sigurnosti i savjetovanje, uključujući stručno savjetovanje, povezano s tehničkom potporom, ili pružanje pomoći u obavljanju tih aktivnosti;”;

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

„20. ‚tehnička specifikacija’ 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;

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

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 ocjenjuje 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. mijenja se kako slijedi:

i. uvodni tekst 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:";

ii. točka (b) zamjenjuje se sljedećim:

„(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.;";

(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. članak 46. zamjenjuje se sljedećim:

„Članak 46

Europski okvir za kibersigurnosnu certifikaciju

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

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

usluga i procesa ili kojima se s pomoću njih može pristupiti tijekom njihova cijelog životnog ciklusa. 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 dostatnom i odgovarajućom razinom relevantnog tehničkog znanja i profesionalnog integriteta.”;

6. članak 47. mijenja se kako slijedi:

(a) stavak 2. zamjenjuje se sljedećim:

„2. Kontinuirani program rada Unije osobito 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.”;

(b) stavak 3. mijenja se kako slijedi:

i. uvodni dio zamjenjuje se sljedećim:

„3. Uključivanje kontinuiranog programa rada Unije određenih IKT proizvoda, IKT usluga, IKT procesa i upravljanih sigurnosnih usluga, ili njihovih kategorija u opravdano je na temelju jednog ili više od sljedećih razloga:”;

ii. točka (a) zamjenjuje se sljedećim:

„(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;”;

iii. umeće se sljedeća točka:

„(ca) tehnološkog razvoja te dostupnosti i razvoja međunarodnih programa kibersigurnosne certifikacije te međunarodnih normi i normi koje upotrebljava industrija;”;

7. članak 49. mijenja se kako slijedi:

(a) stavci od 1. do 4. zamjenjuju se sljedećim:

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

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

3. Pri izradi prijedloga programa certifikacije ENISA se pravodobno savjetuje sa svim relevantnim dionicima putem formalnih, otvorenih, transparentnih i uključivih postupaka savjetovanja. Pri prosljeđivanju prijedloga programa certifikacije Komisiji, u skladu sa stavkom 6., ENISA dostavlja informacije o tome kako je postupila u skladu s ovim stavkom.

4. Za svaki prijedlog programa certifikacije ENISA uspostavlja *ad hoc* radnu skupinu u skladu s člankom 20. stavkom 4. radi pružanja posebnih savjeta i stručnog znanja ENISA-i. Te *ad hoc* radne skupine, prema potrebi i ne dovodeći u pitanje postupke i diskrecijsko pravo iz članka 20. stavka 4., uključuju stručnjake iz javnih uprava država članica, institucija, tijela, ureda i agencija Unije te privatnog sektora.”;

(b) stavak 7. zamjenjuje se sljedećim:

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

8. umeće se sljedeći članak:

„Članak 49.a

Informacije i savjetovanje o europskim programima kibersigurnosne certifikacije

1. Komisija objavljuje informacije o svojem zahtjevu ENISA-i da izradi prijedlog programa certifikacije ili da preispita postojeći europski program kibersigurnosne certifikacije iz članka 48.

2. Tijekom izrade prijedloga programa certifikacije koji provodi ENISA na temelju članka 49. Europski parlament, Vijeće, ili oboje mogu zatražiti od Komisije u svojstvu predsjednika ECCG-a i ENISA-e da svaka tri mjeseca dostave relevantne informacije o nacrtu prijedloga programa certifikacije. Na zahtjev Europskog parlamenta ili Vijeća, ENISA može, u dogovoru s Komisijom i ne dovodeći u pitanje članak 27., staviti na raspolaganje Europskom parlamentu i Vijeću relevantne dijelove nacrta prijedloga programa certifikacije na način primjeren potrebnoj razini povjerljivosti i, prema potrebi, na ograničen način.

3. Kako bi se poboljšao dijalog među institucijama Unije i doprinijelo formalnom, otvorenom, transparentnom i uključivom postupku savjetovanja, Europski parlament, Vijeće, ili oboje, mogu pozvati Komisiju i ENISA-u da rasprave o pitanjima u vezi s funkcioniranjem europskih programa kibersigurnosne certifikacije za IKT proizvode, IKT usluge, IKT procese ili upravljane sigurnosne usluge.

4. Komisija prema potrebi uzima u obzir elemente koji proizlaze iz stajališta Europskog parlamenta i iz stajališta Vijeća o pitanjima iz stavka 3. ovog članka pri evaluaciji ove Uredbe na temelju članka 67.";

9. 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:"

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

(b) da pružatelj ima uspostavljene primjerene interne postupke kojima jamči da se upravljane sigurnosne usluge u svakom trenutku pružaju na dostatnoj i odgovarajućoj razini kvalitete;

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

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

(f) da se vodi evidencija podataka, usluga ili funkcija kojima se pristupilo, koje su se koristile ili na drugi način obrađivale, u koje vrijeme i od strane koga, te da je dostupna za procjenu;

(g) da su IKT proizvodi, IKT usluge i IKT procesi koji se koriste za pružanje upravljanih sigurnosnih usluga sigurni dizajnom i po zadanim postavkama i da, prema potrebi, imaju najnovija sigurnosna ažuriranja te da ne sadrže poznate ranjivosti.”;

11. 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 ili 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 ili 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.”;

12. 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 ili 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, IKT procesa ili upravljanih sigurnosnih usluga s programom stavlja na raspolaganje nacionalnom tijelu za kibersigurnosnu certifikaciju imenovano na temelju članka 58. za razdoblje utvrđeno u odgovarajućem europskom programu kibersigurnosne certifikacije. Preslika EU izjave o sukladnosti podnosi se nacionalnom tijelu za kibersigurnosnu certifikaciju i ENISA-i.";

13. 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 ili upravljanih sigurnosnih usluga;";

(b) točka (g) zamjenjuje se sljedećim:

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

(c) točka (j) zamjenjuje se sljedećim:

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

(d) točka (l) zamjenjuje se sljedećim:

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

(e) 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 ili upravljanih sigurnosnih usluga, sigurnosne zahtjeve, kriterije i metode evaluacije te jamstvene razine;";

(f) 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;";

14. 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, IKT procesa i, od 4. veljače 2025., upravljanih sigurnosnih usluga 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:

— 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;”;

— 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 MSP-ova, uključujući mikropoduzeća;”;

(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 imenovanom na temelju 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.”;

15. 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 provedbenom 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.”;

16. 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.";

17. 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);";

18. u članku 67. stavci 2. i 3. zamjenjuju se sljedećim:

„2. Ocjenjivanjem se procjenjuje i učinak, djelotvornost i učinkovitost odredaba iz glave III. ove Uredbe, uključujući postupke koji dovode do donošenja europskih programa kibersigurnosne certifikacije i njihove baze dokaza, 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. Ocjenjivanjem se procjenjuje jesu li ključni zahtjevi kibersigurnosti za pristup unutarnjem tržištu potrebni kako bi se spriječilo da IKT proizvodi, IKT usluge, IKT procesi i upravljane sigurnosne usluge koji ne ispunjavaju temeljne zahtjeve u pogledu kibersigurnosti uđu na unutarnje tržište.".

19. Prilog se mijenja u skladu s Prilogom ovoj Uredbi.

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 Bruxellesu 19. prosinca 2024.

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*
R. METSOLA	BÓKA J.

PRILOG

Prilog Uredbi (EU) 2019/881 mijenja se kako slijedi:

1. točke od 2. do 5. zamjenjuju se sljedećim:

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

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

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

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

2. točka 10. mijenja se kako slijedi:

(a) uvodni dio zamjenjuje se sljedećim:

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

(b) točka (c) zamjenjuje se sljedećim:

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

3. točke 19. i 20. zamjenjuju se sljedećim:

„19. Tijela za ocjenjivanje sukladnosti ispunjavaju zahtjeve relevantne usklađene norme kako je definirana u članku 2. točki 9. Uredbe (EZ) br. 765/2008 za akreditaciju tijela za ocjenjivanje sukladnosti koja obavljaju certifikaciju IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga.

20. Tijela za ocjenjivanje sukladnosti osiguravaju da ispitni laboratoriji koji se upotrebljavaju za potrebe ocjenjivanja sukladnosti ispunjavaju zahtjeve relevantne usklađene norme kako je definirana u članku 2. točki 9. Uredbe (EZ) br. 765/2008 za akreditaciju laboratorija koji obavljaju ispitivanje.”.

U pogledu ovog akta dana je izjava koja se može pronaći u SL C, C/2025/307, 15.1.2025., ELI: http://data.europa.eu/eli/C/2025/307/oj.