2025/37

15.1.2025

UREDBA (EU) 2025/37 EVROPSKEGA PARLAMENTA IN SVETA

z dne 19. decembra 2024

o spremembi Uredbe (EU) 2019/881 glede upravljanih varnostnih storitev

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora ([1]),

po posvetovanju z Odborom regij,

v skladu z rednim zakonodajnim postopkom ([2]),

ob upoštevanju naslednjega:

(1) Z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta ([3]) je vzpostavljen okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za namen zagotavljanja ustrezne ravni kibernetske varnosti za proizvode informacijske in komunikacijske tehnologije (IKT), storitve IKT in postopke IKT v Uniji, pa tudi za namene preprečevanja razdrobljenosti notranjega trga v zvezi s certifikacijskimi shemami za kibernetsko varnost v Uniji.

(2) Da bi zagotovili odpornost Unije na kibernetske napade in preprečili morebitne ranljivosti na notranjem trgu, je namen te uredbe dopolniti horizontalni regulativni okvir, ki določa celovite zahteve glede kibernetske varnosti za izdelke z digitalnimi elementi na podlagi Uredbe (EU) 2024/2847 Evropskega parlamenta in Sveta ([4]) z določitvijo varnostnih ciljev za upravljane varnostne storitve ter uporabo in zanesljivost teh storitev.

(3) Upravljane varnostne storitve izvajajo ponudniki upravljanih varnostnih storitev, kakor so opredeljeni v členu 6, točka 40, Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta ([5]). Opredelitev pojma upravljanih varnostnih storitev v tej uredbi bi zato morala biti skladna z opredelitvijo pojma ponudnikov upravljanih varnostnih storitev iz Direktive (EU) 2022/2555. Te storitve vključujejo izvajanje dejavnosti, povezanih z obvladovanjem tveganj za kibernetsko varnost za stranke teh storitev, ali zagotavljanje pomoči pri takih dejavnostih ter postajajo vse pomembnejše pri preprečevanju in blaženju incidentov. Zato se ponudniki teh storitev štejejo za bistvene ali pomembne subjekte, ki spadajo v visoko kritični sektor na podlagi Direktive (EU) 2022/2555. Kot je navedeno v uvodni izjavi 86 navedene direktive, imajo ponudniki upravljanih varnostnih storitev na področjih, kot so odzivanje na incidente, penetracijsko testiranje, varnostne presoje in svetovanje, še posebej pomembno vlogo pri zagotavljanju pomoči subjektom pri njihovih prizadevanjih za preprečevanje in odkrivanje incidentov ter odzivanje nanje ali obnovitev po njih. Vendar so ponudniki upravljanih varnostnih storitev tudi sami tarča kibernetskih napadov in predstavljajo posebno tveganje, saj so tesno vključeni v delovanje svojih strank. Zato je pomembno, da so bistveni in pomembni subjekti v smislu Direktive (EU) 2022/2555 bolj skrbni pri izbiri ponudnikov upravljanih varnostnih storitev.

([1]) UL C 349, 29.9.2023, str. 167.
([2]) Stališče Evropskega parlamenta z dne 24. aprila 2024 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 2. decembra 2024.
([3]) Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).
([4]) Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80).

(4) Opredelitev pojma upravljanih varnostnih storitev iz te uredbe zajema neizčrpni seznam upravljanih varnostnih storitev, za katere bi lahko uvedli evropske certifikacijske sheme za kibernetsko varnost, kot so odzivanje na incidente, penetracijsko testiranje, varnostne presoje in svetovanje v zvezi s tehnično podporo. Upravljane varnostne storitve bi lahko vključevale storitve kibernetske varnosti, ki podpirajo pripravljenost na preprečevanje, odkrivanje, analizo in blaženje incidentov ter odzivanje nanje in obnovitve po njih. Za upravljane varnostne storitve bi se lahko štela tudi zagotavljanje obveščevalnih podatkov o kibernetskih grožnjah in ocenjevanje tveganja, povezano s tehnično podporo. Za različne upravljane varnostne storitve bi lahko obstajale ločene evropske certifikacijske sheme za kibernetsko varnost. Evropski certifikati kibernetske varnosti, izdani v skladu s takimi shemami, bi se morali nanašati na določene upravljane varnostne storitve določenega ponudnika teh storitev.

(5) Ponudniki upravljanih varnostnih storitev imajo lahko pomembno vlogo tudi pri ukrepih, s katerimi Unija podpira odzivanje in začetno obnovitev v primerih pomembnih kibernetskih incidentov in kibernetskih incidentov velikih razsežnosti, tako da se opira na storitve zaupanja vrednih zasebnih ponudnikov in na testiranje kritičnih subjektov na podlagi usklajenih ocen tveganja za varnost na ravni Unije, da bi ugotovila morebitne ranljivosti. Certificiranje upravljanih varnostnih storitev bi lahko imelo vlogo pri izbiri zaupanja vrednih ponudnikov upravljanih varnostnih storitev, kakor so opredeljeni v Uredbi (EU) 2025/38 ([6]) Evropskega parlamenta in Sveta.

(6) Certificiranje upravljanih varnostnih storitev ni pomembno le v postopku izbire za kibernetskovarnostno rezervo EU, vzpostavljeno z Uredbo (EU) 2025/38, temveč je tudi bistven kazalnik kakovosti za zasebne in javne subjekte, ki nameravajo kupiti take storitve. Glede na kritičnost upravljanih varnostnih storitev in občutljivost obdelanih podatkov bi lahko certificiranje potencialnim strankam zagotovilo pomembne usmeritve in zagotovila glede zanesljivosti teh storitev. Evropske certifikacijske sheme za kibernetsko varnost za upravljane varnostne storitve naj bi prispevale k preprečevanju razdrobljenosti notranjega trga. Namen te uredbe je torej izboljšati delovanje notranjega trga.

(7) Evropske certifikacijske sheme za kibernetsko varnost za upravljane varnostne storitve bi morale privesti do uporabe teh storitev in večje konkurence med ponudniki upravljanih varnostnih storitev. Brez poseganja v cilj zagotavljanja zadostne in ustrezne ravni ustreznega tehničnega znanja in poklicne integritete takih ponudnikov bi morale take certifikacijske sheme zato olajšati vstop na trg in ponudbo upravljanih varnostnih storitev, in sicer tako, da bi čim bolj poenostavili morebitna regulativna, upravna in finančna bremena, ki bi jih lahko imeli ponudniki, zlasti mala in srednja podjetja (MSP), vključno z mikro podjetji, pri ponudbi upravljanih varnostnih storitev. Poleg tega bi morali zato, da bi spodbudili uporabo upravljanih varnostnih storitev in povpraševanje po njih, z evropskimi certifikacijskimi shemami za kibernetsko varnost prispevati k dostopnosti teh storitev, zlasti za manjše akterje, kot so MSP, vključno z mikro podjetji, ter za lokalne in regionalne organe, ki imajo omejene zmogljivosti in vire, vendar so bolj izpostavljeni kršitvam kibernetske varnosti, te pa imajo finančne, pravne in operativne posledice ter škodujejo ugledu.

(8) MSP, vključno z mikro podjetji, je pomembno zagotoviti podporo pri izvajanju te uredbe ter zaposlovanju oseb s specializiranimi kibernetskovarnostnimi veščinami in strokovnim znanjem, potrebnimi za izvajanje upravljanih varnostnih storitev v skladu z zahtevami iz te uredbe. V programu Digitalna Evropa, vzpostavljenem z Uredbo (EU) 2021/649 Evropskega parlamenta in Sveta ([7]), in drugih ustreznih programih Unije je določeno, da Komisija vzpostavi finančno in tehnično podporo, ki tem podjetjem omogoča, da prispevajo k rasti gospodarstva Unije in okrepitvi skupne ravni kibernetske varnosti v Uniji, vključno z racionalizacijo finančne podpore iz programa Digitalna Evropa in drugih ustreznih programov Unije ter s podporo MSP, vključno z mikro podjetji.

(9) Evropske certifikacijske sheme za kibernetsko varnost za upravljane varnostne storitve bi morale prispevati k razpoložljivosti varnih in visokokakovostnih storitev, ki zagotavljajo varen digitalni prehod, in k doseganju ciljev iz programa politike Digitalno desetletje do leta 2030, vzpostavljenega s Sklepom (EU) 2022/2481 Evropskega parlamenta in Sveta ([8]), zlasti v zvezi s ciljem, da 75 % podjetij Unije začne uporabljati računalništvo v oblaku,

([6]) Uredba (EU) 2025/38 Evropskega parlamenta in Sveta z dne 19. decembra 2024 o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskih groženj in incidentov ter pripravo in odzivanje nanje ter spremembi Uredbe (EU) 2021/694 (Akt o kibernetski solidarnosti) (UL L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Uredba (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa Digitalna Evropa in razveljavitvi Sklepa (EU) 2015/2240 (UL L 166, 11.5.2021, str. 1).

([8]) Sklep (EU) 2022/2481 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o vzpostavitvi programa politike Digitalno desetletje do leta 2030 (UL L 323, 19.12.2022, str. 4).

velepodatke ali umetno inteligenco, da več kot 90 % MSP, vključno z mikro podjetji, doseže vsaj osnovno raven digitalne intenzivnosti in da postanejo ključne javne storitve dostopne na spletu.

(10) Upravljane varnostne storitve poleg uvajanja proizvodov IKT, storitev IKT ali postopkov IKT pogosto zagotavljajo dodatne storitvene funkcije, ki temeljijo na kompetencah, strokovnem znanju in izkušnjah osebja ponudnikov takih storitev. Zelo visoka raven teh kompetenc, strokovnega znanja in izkušenj ter ustrezni notranji postopki bi morali biti del varnostnih ciljev, da se zagotovi zelo visoka kakovost ponujenih upravljanih varnostnih storitev. Da bi se lahko vsi vidiki upravljanih varnostnih storitev vključili v namenske evropske certifikacijske sheme za kibernetsko varnost, je torej treba spremeniti Uredbo (EU) 2019/881. Pri tem bi bilo treba upoštevati rezultate in priporočila ocene in pregleda iz Uredbe (EU) 2019/881.

(11) Da bi spodbudili rast zanesljivega notranjega trga in hkrati ustvarili partnerstva s podobno mislečimi tretjimi državami, bi bilo treba postopek certificiranja, vzpostavljen v evropskem certifikacijskem okviru za kibernetsko varnost iz Uredbe (EU) 2019/881, izvajati tako, da bi olajšali njegovo mednarodno priznanje in uskladitev z mednarodnimi standardi.

(12) Unija se spoprijema z vrzeljo na področju strokovnjakov, za katero je značilno pomanjkanje usposobljenih strokovnjakov, in s hitro spreminjajočo se krajino groženj, kot je ugotovljeno v sporočilu Komisije z dne 18. aprila 2023 z naslovom „Zapolnitev vrzeli na področju strokovnjakov za kibernetsko varnost za povečanje konkurenčnosti, rasti in odpornosti EU (‚akademija za kibernetske veščine')“. Izobraževalni viri in oblike formalnega usposabljanja so različni, znanje pa je mogoče pridobiti na različne načine: formalno, na primer z univerzitetnimi programi ali tečaji, ali neformalno, na primer z usposabljanjem na delovnem mestu ali delovnimi izkušnjami na ustreznem področju. Da bi se visokokakovostne upravljane varnostne storitve lažje razvile in da bi imeli boljši pregled nad sestavo delovne sile Unije na področju kibernetske varnosti, je pomembno okrepiti sodelovanje med državami članicami, Komisijo, Agencijo Evropske unije za kibernetsko varnost, ustanovljeno z Uredbo (EU) 2019/881 (v nadaljnjem besedilu: agencija ENISA), in deležniki, vključno z zasebnim sektorjem in akademskimi krogi, in sicer z oblikovanjem javno-zasebnih partnerstev, podpiranjem pobud na področju raziskav in inovacij, razvojem in vzajemnim priznavanjem skupnih standardov ter certificiranjem kibernetskovarnostnih veščin, tudi prek evropskega okvira za kibernetskovarnostne veščine. Tako sodelovanje bi spodbudilo tudi mobilnost strokovnjakov za kibernetsko varnost v Uniji ter vključevanje znanja in usposabljanja o kibernetski varnosti v izobraževalne programe, hkrati pa bi omogočilo vajeništvo in pripravništvo mladim, tudi osebam, ki prebivajo v prikrajšanih regijah, kot so otoki ter redko poseljena, podeželska in oddaljena območja. Pomembno je, da je cilj takega sodelovanja privabiti k temu področju več žensk in deklet ter prispevati k odpravljanju razlik med spoloma na področju naravoslovja, tehnologije, inženirstva in matematike, ter da je cilj zasebnega sektorja zagotoviti usposabljanje na delovnem mestu, ki bo usmerjeno v najbolj iskana znanja in spretnosti, ter vključevalo javno upravo in zagonska podjetja, pa tudi MSP, vključno z mikro podjetji. Pomembno je tudi, da ponudniki in države članice sodelujejo in prispevajo k zbiranju podatkov o razmerah in razvoju na trgu dela na področju kibernetske varnosti.

(13) Agencija ENISA ima pomembno vlogo pri pripravi predlog za evropske certifikacijske sheme za kibernetsko varnost. Komisija bi morala pri pripravi predloga splošnega proračuna Unije v skladu s postopkom iz člena 29 Uredbe (EU) 2019/881 oceniti potrebna proračunska sredstva za kadrovski načrt agencije ENISA.

(14) Ta uredba določa ciljno usmerjene spremembe Uredbe (EU) 2019/881, da se omogoči vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za upravljane varnostne storitve. V njej so določene in pojasnjene tudi nekatere določbe navedene uredbe v zvezi s pripravo in delovanjem vseh evropskih certifikacijskih shem za kibernetsko varnost, da bi zagotovili njihovo preglednost in odprtost. Slednje spremembe, pri katerih gre le za podrobnejši opis ali pojasnitev Uredbe (EU) 2019/881, zlasti spremembe v zvezi z informacijami, ki jih mora agencija ENISA zagotoviti pri posredovanju predloge za shemo, ad hoc delovnimi skupinami, ustanovljenimi za vsako predlogo za shemo, ter obveščanjem in svetovanjem v zvezi z evropskimi certifikacijskimi shemami za kibernetsko varnost, nikakor ne bi smele vplivati na širšo oceno in pregled navedene uredbe, ki se zahtevata na podlagi člena 67 navedene uredbe, zlasti z oceno vpliva, učinkovitosti in uspešnosti naslova navedene uredbe v zvezi s certifikacijskim okvirom za kibernetsko varnost. Ocena in pregled v zvezi s tem naslovom bi morala temeljiti na obsežnem posvetovanju z deležniki ter na celoviti in temeljiti analizi zadevnih postopkov.

(15) Ker cilja te uredbe, in sicer omogočiti vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za upravljane varnostne storitve, države članice ne morejo zadovoljivo doseči, temveč se zaradi obsega in učinkov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(16) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([9]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 10. januarja 2024 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Spremembe Uredbe (EU) 2019/881

Uredba (EU) 2019/881 se spremeni:

(1) v členu 1(1), prvi pododstavek, se točka (b) nadomesti z naslednjim:

„(b) okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za namene zagotavljanja ustrezne ravni kibernetske varnosti za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve v Uniji, pa tudi za namene preprečevanja razdrobljenosti notranjega trga v zvezi s certifikacijskimi shemami za kibernetsko varnost v Uniji.“;

(2) člen 2 se spremeni:

(a) točke 9, 10 in 11 se nadomestijo z naslednjim:

„(9) ‚evropska certifikacijska shema za kibernetsko varnost‘ pomeni celovit sklop pravil, tehničnih zahtev, standardov in postopkov, ki so vzpostavljeni na ravni Unije in se uporabljajo za certificiranje ali ugotavljanje skladnosti posameznih proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev;

(10) ‚nacionalna certifikacijska shema za kibernetsko varnost‘ pomeni celovit sklop pravil, tehničnih zahtev, standardov in postopkov, ki so jih oblikovali in sprejeli nacionalni javni organi in se uporabljajo za certificiranje ali ugotavljanje skladnosti proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, ki spadajo na področje uporabe določene sheme;

(11) ‚evropski certifikat kibernetske varnosti‘ pomeni dokument, ki ga izda ustrezen organ in potrjuje, da je bil zadevni proizvod IKT, storitev IKT, postopek IKT ali upravljana varnostna storitev ocenjena glede skladnosti s posebnimi varnostnimi zahtevami, določenimi v evropski certifikacijski shemi za kibernetsko varnost;“;

(b) vstavi se naslednja točka:

„(14a) ‚upravljana varnostna storitev‘ pomeni storitev, ki se zagotavlja tretji osebi in vključuje izvajanje dejavnosti, povezanih z obvladovanjem tveganj za kibernetsko varnost, ali za zagotavljanje pomoči pri takih dejavnostih, kot so odzivanje na incidente, penetracijsko testiranje, varnostne presoje in svetovanje, vključno s strokovnim svetovanjem, povezanim s tehnično podporo;“;

(c) točke 20, 21 in 22 se nadomestijo z naslednjim:

„(20) ‚tehnična specifikacija‘ pomeni dokument, ki določa tehnične zahteve, ki jih mora izpolnjevati proizvod IKT, storitev IKT, postopek IKT ali upravljana varnostna storitev, ali postopke ugotavljanja skladnosti v zvezi s proizvodom IKT, storitvijo IKT, postopkom IKT ali upravljano varnostno storitvijo;

([9]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

(21) ‚raven zanesljivosti' pomeni podlago za zaupanje, da proizvod IKT, storitev IKT, postopek IKT ali upravljana varnostna storitev izpolnjuje varnostne zahteve določene evropske certifikacijske sheme za kibernetsko varnost, navaja pa tudi raven, na kateri je bil proizvod IKT, storitev IKT, postopek IKT ali upravljana varnostna storitev ocenjena, vendar kot taka ne meri varnosti zadevnega proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve;

(22) ‚samoocenjevanje skladnosti' pomeni dejavnost proizvajalca ali ponudnika proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, s katero se oceni, ali ti proizvodi IKT, storitve IKT, postopki IKT ali upravljane varnostne storitve izpolnjujejo zahteve iz določene evropske certifikacijske sheme za kibernetsko varnost.";

(3) v členu 4 se odstavek 6 nadomesti z naslednjim:

„6. Agencija ENISA spodbuja uporabo evropskega certificiranja na področju kibernetske varnosti, da se prepreči razdrobljenost notranjega trga. Agencija ENISA prispeva k vzpostavitvi in vzdrževanju evropskega certifikacijskega okvira za kibernetsko varnost v skladu z naslovom III te uredbe, da bi se izboljšala preglednost kibernetske varnosti proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev ter s tem okrepila zaupanje v digitalni notranji trg in njegova konkurenčnost.";

(4) člen 8 se spremeni:

(a) odstavek 1 se spremeni:

(i) uvodno besedilo se nadomesti z naslednjim:

„1. Agencija ENISA podpira in spodbuja oblikovanje in izvajanje politike Unije o certificiranju proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev glede kibernetske varnosti, kot je določeno v naslovu III te uredbe, in sicer s:";

(ii) točka (b) se nadomesti z naslednjim:

„(b) pripravo predlog za evropske certifikacijske sheme za kibernetsko varnost (v nadaljnjem besedilu: predloge za sheme) za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve v skladu s členom 49;";

(b) odstavek 3 se nadomesti z naslednjim:

„3. Agencija ENISA pripravi in objavi smernice ter razvije dobre prakse glede zahtev na področju kibernetske varnosti za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve v sodelovanju z nacionalnimi certifikacijskimi organi za kibernetsko varnost in industrijo na formalen, strukturiran in pregleden način.";

(c) odstavek 5 se nadomesti z naslednjim:

„5. Agencija ENISA omogoča lažjo vzpostavitev in uvedbo evropskih in mednarodnih standardov za obvladovanje tveganja in za varnost proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev.";

(5) člen 46 se nadomesti z naslednjim:

„*Člen 46*

Evropski certifikacijski okvir za kibernetsko varnost

1. Evropski certifikacijski okvir za kibernetsko varnost se vzpostavi za izboljšanje pogojev za delovanje notranjega trga z zvišanjem ravni kibernetske varnosti v Uniji in omogočanjem harmoniziranega pristopa na ravni Unije glede evropskih certifikacijskih shem za kibernetsko varnost, da bi se oblikoval enotni digitalni trg za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve.

2. Evropski certifikacijski okvir za kibernetsko varnost zagotavlja mehanizem za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost in za potrjevanje, da proizvodi IKT, storitve IKT in postopki IKT, ki so bili ocenjeni v skladu s takimi shemami, izpolnjujejo določene varnostne zahteve, da se zaščitijo razpoložljivost, pristnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali funkcij ali storitev, ki jih ti

proizvodi, storitve in postopki ponujajo ali so prek njih dostopni v celotnem življenjskem ciklu. Z njim se potrjuje tudi, da upravljane varnostne storitve, ki so bile ocenjene v skladu s takimi shemami, izpolnjujejo določene varnostne zahteve, da se zaščitijo razpoložljivost, pristnost, celovitost in zaupnost podatkov, do katerih se dostopa ali ki se obdelujejo, shranjujejo ali prenašajo v zvezi z izvajanjem teh storitev, ter da te storitve vedno izvaja osebje z ustreznimi kompetencami, strokovnim znanjem in izkušnjami ter zadostno in primerno ravnjo ustreznega tehničnega znanja in poklicne integritete.“;

(6) člen 47 se spremeni:

(a) odstavek 2 se nadomesti z naslednjim:

„2. Tekoči delovni program Unije vključuje predvsem seznam proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev ali njihovih kategorij, za katere je lahko koristno, če so vključeni v področje uporabe evropske certifikacijske sheme za kibernetsko varnost.“;

(b) odstavek 3 se spremeni:

(i) uvodno besedilo se nadomesti z naslednjim:

„3. Vključitev posameznih proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev ali njihovih kategorij v tekoči delovni program Unije se utemelji z enim ali več od naslednjih razlogov:“;

(ii) točka (a) se nadomesti z naslednjim:

„(a) razpoložljivost in oblikovanje nacionalnih certifikacijskih shem za kibernetsko varnost, ki zajemajo posamezno kategorijo proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, zlasti kar zadeva tveganje razdrobljenosti;“;

(iii) vstavi se naslednja točka:

„(ca) tehnološki razvoj ter razpoložljivost in razvoj mednarodnih certifikacijskih shem za kibernetsko varnost ter mednarodnih standardov in standardov, ki jih uporablja industrija;“;

(7) člen 49 se spremeni:

(a) odstavki 1do 4 se nadomestijo z naslednjim:

„1. Agencija ENISA na zahtevo Komisije na podlagi člena 48 pripravi predlogo za shemo, ki izpolnjuje veljavne zahteve iz členov 51, 51a, 52 in 54.

2. Agencija ENISA lahko na zahtevo evropske certifikacijske skupine za kibernetsko varnost na podlagi člena 48(2) pripravi predlogo za shemo, ki izpolnjuje veljavne zahteve iz členov 51, 51a, 52 in 54. Če agencija ENISA tako zahtevo zavrne, mora to obrazložiti. Vsako odločitev o zavrnitvi take zahteve sprejme upravni odbor.

3. Pri pripravi predloge za shemo se agencija ENISA pravočasno posvetuje z vsemi ustreznimi deležniki v okviru formalnega, odprtega, preglednega in vključujočega posvetovalnega postopka. Agencija ENISA pri posredovanju predloge za shemo Komisiji na podlagi odstavka 6 zagotovi informacije o tem, kako je ravnala v skladu s tem odstavkom.

4. Agencija ENISA za vsako predlogo za shemo ustanovi ad hoc delovno skupino v skladu s členom 20(4), da agenciji ENISA pomaga s specifičnimi nasveti ter strokovnim znanjem in izkušnjami. Te ad hoc delovne skupine, po potrebi in brez poseganja v postopke in diskrecijsko pravico iz člena 20(4) vključujejo strokovnjake iz javnih uprav držav članic, institucij, organov, uradov in agencij Unije ter iz zasebnega sektorja.“;

(b) odstavek 7 se nadomesti z naslednjim:

„7. Komisija lahko na podlagi predloge za shemo, ki jo pripravi agencija ENISA, sprejme izvedbene akte, ki določajo evropsko certifikacijsko shemo za kibernetsko varnost za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve, ki izpolnjujejo ustrezne zahteve iz členov 51, 51a, 52 in 54. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 66(2).“;

(8) vstavi se naslednji člen:

„Člen 49a

Informacije in posvetovanje o evropskih certifikacijskih shemah za kibernetsko varnost

1. Komisija javno objavi informacije o svoji zahtevi agenciji ENISA, naj pripravi predlogo za shemo ali pregleda obstoječo evropsko certifikacijsko shemo za kibernetsko varnost iz člena 48.

2. V času, ko agencija ENISA na podlagi člena 49 pripravlja predlogo za shemo, lahko Evropski parlament, Svet ali oba od Komisije kot predsedujoče evropski certifikacijski skupini za kibernetsko varnost (ECCG) in agencije ENISA zahtevata, naj vsako četrtletje predstavita ustrezne informacije o osnutku predloge. Agencija ENISA lahko na zahtevo Evropskega parlamenta ali Sveta v soglasju s Komisijo in brez poseganja v člen 27 Evropskemu parlamentu in Svetu da na voljo ustrezne dele osnutka predloge za shemo na način, ki ustreza zahtevani ravni zaupnosti, in, kadar je primerno, v omejenem obsegu.

3. Da bi se okrepil dialog med institucijami Unije ter da bi se izboljšal formalen, odprt, pregleden in vključujoč posvetovalni postopek, lahko Evropski parlament, Svet ali oba Komisijo in agencijo ENISA pozoveta k razpravi o zadevah v zvezi z delovanjem evropskih certifikacijskih shem za kibernetsko varnost za proizvode IKT, storitve IKT, postopke IKT ali upravljane varnostne storitve.

4. Kadar je primerno, Komisija pri ocenjevanju te uredbe na podlagi člena 67 upošteva elemente, ki izhajajo iz stališč Evropskega parlamenta in stališč Sveta o zadevah iz odstavka 3 tega člena.“;

(9) člen 51 se spremeni:

(a) naslov se nadomesti z naslednjim:

„Varnostni cilji evropskih certifikacijskih shem za kibernetsko varnost za proizvode IKT, storitve IKT in postopke IKT“;

(b) uvodni stavek se nadomesti z naslednjim:

„Evropska certifikacijska shema za kibernetsko varnost za proizvode IKT, storitve IKT ali postopke IKT je oblikovana tako, da se ustrezno dosežejo najmanj naslednji varnostni cilji:“;

(10) vstavi se naslednji člen:

„Člen 51a

Varnostni cilji evropskih certifikacijskih shem za kibernetsko varnost za upravljane varnostne storitve

Evropska certifikacijska shema za kibernetsko varnost za upravljane varnostne storitve je oblikovana tako, da se ustrezno dosežejo najmanj naslednji varnostni cilji:

(a) da se upravljane varnostne storitve izvajajo z ustreznimi kompetencami, strokovnim znanjem in izkušnjami, vključno s tem, da ima osebje, odgovorno za izvajanje teh storitev, zadostno in ustrezno raven tehničnega znanja in kompetenc na določenem področju, zadostne in ustrezne izkušnje ter najvišjo stopnjo poklicne integritete;

(b) da ima ponudnik vzpostavljene ustrezne notranje postopke za zagotovitev, da se upravljane varnostne storitve vedno izvajajo na zadostni in ustrezni ravni kakovosti;

(c) da se zaščitijo podatki, do katerih se dostopa ali ki se shranjujejo, prenašajo ali kako drugače obdelujejo v zvezi z izvajanjem upravljanih varnostnih storitev pred naključnim ali nepooblaščenim dostopom, hrambo, razkritjem, uničenjem, drugo obdelavo ali izgubo ali spremembo ali slabo razpoložljivostjo;

(d) da se v primeru fizičnega ali tehničnega incidenta zagotovi pravočasna povrnitev razpoložljivosti in dostopa do podatkov, storitev in funkcij;

(e) da imajo pooblaščene osebe, programi ali stroji dostop zgolj do podatkov, storitev ali funkcij, na katere se nanašajo njihove pravice do dostopa;

(f) da se evidentira in omogoči ocena, do katerih podatkov, storitev ali funkcij se je dostopalo ali kateri podatki, storitve ali funkcije so se uporabljali oziroma kako drugače obdelovali ter kdaj in kdo je do njih dostopal oziroma jih je uporabljal ali obdeloval;

(g) da so proizvodi IKT, storitve IKT in postopki IKT, ki se uporabljajo pri zagotavljanju upravljanih varnostnih storitev, razviti v skladu z načelom privzete in vgrajene varnosti, ter, kadar je ustrezno, vključujejo najnovejše varnostne posodobitve in ne vsebujejo javno znanih šibkih točk.“;

(11) člen 52 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Evropska certifikacijska shema za kibernetsko varnost lahko določa eno ali več naslednjih ravni zanesljivosti za proizvode IKT, storitve IKT in postopke IKT ter upravljane varnostne storitve: ‚osnovno‘, ‚znatno‘ ali ‚visoko‘. Raven zanesljivosti ustreza stopnji tveganja, povezani s predvideno uporabo proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve v smislu verjetnosti in vpliva incidenta.“;

(b) odstavek 3 se nadomesti z naslednjim:

„3. Varnostne zahteve, ki ustrezajo vsaki ravni zanesljivosti, so določene v ustrezni evropski certifikacijski shemi za kibernetsko varnost, vključno z ustreznimi varnostnimi funkcionalnostmi in ustrezno strogostjo in obsegom ocenjevanja, ki se izvede za proizvod IKT, storitev IKT, postopek IKT ali upravljano varnostno storitev.“;

(c) odstavki 5, 6 in 7 se nadomestijo z naslednjim:

„5. Evropski certifikat kibernetske varnosti ali izjava EU o skladnosti, ki se nanaša na ‚osnovno‘ raven zanesljivost, zagotavlja, da proizvodi IKT, storitve IKT, postopki IKT ali upravljane varnostne storitve, za katere se izda ta certifikat ali ta izjava EU o skladnosti, izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni na ravni za kar najbolj zmanjšana znana osnovna tveganja incidentov in kibernetskih napadov. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo vsaj pregled tehnične dokumentacije. Kadar tak pregled ni primeren, se izvedejo nadomestne ocenjevalne dejavnosti z enakovrednim učinkom.

6. Evropski certifikat kibernetske varnosti, ki se nanaša na ‚znatno‘ raven zanesljivosti, zagotavlja, da proizvodi IKT, storitve IKT, postopki IKT ali upravljane varnostne storitve, za katere se izda ta certifikat, izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni na ravni za kar najbolj zmanjšana znana kibernetska tveganja ter tveganja incidentov in kibernetskih napadov, ki jih izvajajo akterji z omejenim znanjem in viri. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo najmanj naslednje: pregled za dokazovanje, da se javno znane šibke točke ne pojavljajo, in testiranje za dokazovanje, da se pri proizvodih IKT, storitvah IKT, postopkih IKT ali upravljanih varnostnih storitev pravilno izvajajo potrebne varnostne funkcionalnosti. Kadar katera izmed takih ocenjevalnih dejavnosti ni primerna, se izvedejo nadomestne ocenjevalne dejavnosti z enakovrednim učinkom.

7. Evropski certifikat kibernetske varnosti, ki se nanaša na ‚visoko‘ raven zanesljivosti, zagotavlja, da proizvodi IKT, storitve IKT, postopki IKT ali upravljane varnostne storitve, za katere se izda ta certifikat, izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni na ravni za kar najbolj zmanjšano tveganje naprednih kibernetskih napadov, ki jih izvajajo akterji z obsežnim znanjem in viri. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo najmanj naslednje: pregled za dokazovanje, da se javno znane šibke točke ne pojavljajo; testiranje za dokazovanje, da se pri proizvodih IKT, storitvah IKT, postopkih IKT ali upravljanih varnostnih storitvah pravilno izvajajo potrebne najsodobnejše varnostne funkcionalnosti, ter ocenjevanje njihove odpornosti proti izurjenim napadalcem z uporabo penetracijskega testiranja. Kadar katera izmed takih ocenjevalnih dejavnosti ni primerna, se izvedejo nadomestne dejavnosti z enakovrednim učinkom.“;

(12) v členu 53 se odstavki 1, 2 in 3 nadomestijo z naslednjim:

„1. V okviru evropske certifikacijske sheme za kibernetsko varnost se lahko dopusti samoocenjevanje skladnosti, za katero je v celoti odgovoren proizvajalec ali ponudnik proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev. Samoocenjevanje skladnosti se dopusti samo v zvezi s proizvodi IKT, storitvami IKT, postopki IKT ali upravljanimi varnostnimi storitvami, ki predstavljajo nizko tveganje, ki ustreza ‚osnovni' ravni zanesljivosti.

2. Proizvajalec ali ponudnik proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev lahko izda izjavo EU o skladnosti, v kateri je navedeno, da je dokazano izpolnjevanje zahtev iz sheme. Z izdajo take izjave proizvajalec ali ponudnik proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev prevzame odgovornost za skladnost proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve z zahtevami iz te sheme.

3. Proizvajalec ali ponudnik proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev za obdobje, določeno v ustrezni evropski certifikacijski shemi za kibernetsko varnost, nacionalnemu certifikacijskemu organu za kibernetsko varnost, imenovanemu na podlagi člena 58, da na voljo izjavo EU o skladnosti, tehnično dokumentacijo in vse druge ustrezne informacije, ki se nanašajo na skladnost proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev s shemo. Kopija izjave EU o skladnosti se predloži nacionalnemu certifikacijskemu organu za kibernetsko varnost in agenciji ENISA.";

(13) v členu 54 se odstavek 1 spremeni:

(a) točka (a) se nadomesti z naslednjim:

„(a) predmet urejanja in področje uporabe certifikacijske sheme, vključno z vrsto ali kategorijami zajetih proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev;";

(b) točka (g) se nadomesti z naslednjim:

„(g) posebna merila in metode za ocenjevanje, vključno z vrstami ocene, ki se uporabljajo za dokazovanje, da so veljavni varnostni cilji iz členov 51 in 51a doseženi;";

(c) točka (j) se nadomesti z naslednjim:

„(j) pravila za spremljanje skladnosti proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev z zahtevami evropskih certifikatov kibernetske varnosti ali izjave EU o skladnosti, vključno z mehanizmi za dokazovanje stalnega izpolnjevanja določenih zahtev glede kibernetske varnosti;";

(d) točka (l) se nadomesti z naslednjim:

„(l) pravila glede posledic za proizvode IKT, storitve IKT, postopke IKT ali upravljane varnostne storitve, ki so bili certificirani ali za katere se je izdala izjava EU o skladnosti, vendar niso skladni z zahtevami sheme;";

(e) točka (o) se nadomesti z naslednjim:

„(o) opredelitev nacionalnih ali mednarodnih certifikacijskih shem za kibernetsko varnost, ki zadeva isto vrsto ali kategorije proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, varnostnih zahtev, meril in metod za ocenjevanje ter ravni zanesljivosti;";

(f) točka (q) se nadomesti z naslednjim:

„(q) obdobje razpoložljivosti izjave EU o skladnosti, tehnične dokumentacije in vseh drugih ustreznih informacij, ki jih da na voljo proizvajalec ali ponudnik proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev;";

(14) člen 56 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. Za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve, ki so bili certificirani na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi člena 49, se domneva, da so skladni z zahtevami take sheme.";

(b) odstavek 3 se spremeni:

(i) prvi pododstavek se nadomesti z naslednjim:

„Komisija redno ocenjuje učinkovitost in uporabo sprejetih evropskih certifikacijskih shem za kibernetsko varnost ter ali bi morala posamezna evropska certifikacijska shema za kibernetsko varnost postati obvezna na podlagi ustreznega prava Unije, da bi zagotovili ustrezno raven kibernetske varnosti proizvodov IKT, storitev IKT, postopkov IKT in od 4. februarja 2025 upravljanih varnostnih storitev v Uniji ter izboljšali delovanje notranjega trga. Prva taka ocena se izvede do 31. decembra 2023, poznejše ocene pa se izvedejo vsaj vsaki dve leti po tem. Komisija na podlagi rezultatov teh ocen opredeli proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve, zajete v obstoječi certifikacijski shemi, ki bi morali biti zajeti v obvezni certifikacijski shemi.“;

(ii) tretji pododstavek se spremeni:

— točka (a) se nadomesti z naslednjim:

„(a) upošteva učinek ukrepov na proizvajalce ali ponudnike takih proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev ter na uporabnike v smislu stroška teh ukrepov, pa tudi družbene ali gospodarske koristi zaradi pričakovane višje ravni varnosti ciljnih proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev;“;

— točka (d) se nadomesti z naslednjim:

„(d) upošteva roke za izvajanje, prehodne ukrepe in obdobja, zlasti glede morebitnega učinka ukrepov na proizvajalce ali ponudnike proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, tudi s posebnimi interesi in potrebami MSP, vključno z mikro podjetji;“;

(c) odstavka 7 in 8 se nadomestita z naslednjim:

„7. Fizična ali pravna oseba, ki predloži proizvode IKT, storitve IKT, postopke IKT ali upravljane varnostne storitve za certifikacijo, nacionalnemu certifikacijskemu organu za kibernetsko varnost, imenovanim na podlagi člena 58, kadar je to organ, ki je izdal evropski certifikat kibernetske varnosti, ali organu za ugotavljanje skladnosti iz člena 60 da na voljo vse informacije, ki so potrebne za izvedbo certifikacije.

8. Imetnik evropskega certifikata kibernetske varnosti obvesti nacionalni certifikacijski organ za kibernetsko varnost ali organ za ugotavljanje skladnosti iz odstavka 7 o vseh pozneje odkritih šibkih točkah ali nepravilnostih v zvezi z varnostjo certificiranega proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve, ki bi lahko vplivale na njegovo skladnost z zahtevami, povezanimi s certifikacijo. Navedeni organ te informacije brez nepotrebnega odlašanja posreduje zadevnemu nacionalnemu certifikacijskemu organu za kibernetsko varnost.“;

(15) v členu 57 se odstavka 1 in 2 nadomestita z naslednjim:

„1. Brez poseganja v odstavek 3 tega člena nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve, ki so zajeti v evropski certifikacijski shemi za kibernetsko varnost, prenehajo učinkovati z datumom, določenim v izvedbenem aktu, sprejetem na podlagi člena 49(7). Nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve, ki niso zajeti v evropski certifikacijski shemi za kibernetsko varnost, še naprej obstajajo.

2. Države članice ne uvedejo novih nacionalnih certifikacijskih shem za kibernetsko varnost za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve, ki so že zajeti v veljavni evropski certifikacijski shemi za kibernetsko varnost.“;

(16) člen 58 se spremeni:

(a) odstavek 7 se spremeni:

(i) točki (a) in (b) se nadomestita z naslednjim:

„(a) nadzirajo in uveljavljajo pravila iz evropskih certifikacijskih shem za kibernetsko varnost na podlagi člena 54(1), točka (j), za spremljanje skladnosti proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev z zahtevami evropskih certifikatov kibernetske varnosti, ki so bili izdani na njihovem ozemlju, v sodelovanju z drugimi zadevnimi organi za nadzor trga;

(b) spremljajo izpolnjevanje obveznosti proizvajalcev ali ponudnikov proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, ki imajo sedež na njihovem ozemlju in izvajajo samoocenjevanje skladnosti, in jih izvršujejo, ter zlasti spremljajo izpolnjevanje obveznosti takih proizvajalcev ali ponudnikov, določenih v členu 53(2) in (3) in v ustrezni evropski certifikacijski shemi za kibernetsko varnost, in jih izvršujejo;“;

(ii) točka (h) se nadomesti z naslednjim:

„(h) sodelujejo z drugimi nacionalnimi certifikacijskimi organi za kibernetsko varnost ali drugimi javnimi organi, vključno z izmenjavo informacij o morebitni neskladnosti proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev z zahtevami iz te uredbe ali z zahtevami posameznih evropskih certifikacijskih shem za kibernetsko varnost, ter“;

(b) odstavek 9 se nadomesti z naslednjim:

„9. Nacionalni certifikacijski organi za kibernetsko varnost sodelujejo med seboj in s Komisijo, zlasti z izmenjavo informacij, izkušenj in dobrih praks glede certificiranja kibernetske varnosti in tehničnih vprašanj, ki zadevajo kibernetsko varnost proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev.“;

(17) v členu 59(3) se točki (b) in (c) nadomestita z naslednjim:

„(b) postopke za nadziranje in uveljavljanje pravil za spremljanje skladnosti proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev z evropskimi certifikati kibernetske varnosti na podlagi člena 58(7), točka (a);

(c) postopke za spremljanje in izvrševanje obveznosti proizvajalcev ali ponudnikov proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev na podlagi člena 58(7), točka (b);“;

(18) v členu 67 se odstavka 2 in 3 nadomestita z naslednjim:

„2. Oceni se tudi vpliv, učinkovitost in uspešnost določb naslova III te uredbe – vključno s postopki za uvedbo evropskih certifikacijskih shem za kibernetsko varnost in njihovih evidenčnih baz – glede ciljev zagotavljanja ustrezne ravni kibernetske varnosti proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev v Uniji ter izboljšanja delovanja notranjega trga.

3. Med ocenjevanjem se presodi, ali so za dostop do notranjega trga potrebne bistvene zahteve glede kibernetske varnosti, da se prepreči vstop proizvodov IKT, storitev IKT, postopkov IKT in upravljanih varnostnih storitev, ki ne izpolnjujejo osnovnih zahtev glede kibernetske varnosti, na notranji trg.“;

(19) Priloga se spremeni v skladu s Prilogo k tej Uredbi.

Člen 2

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 19. decembra 2024

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*
R. METSOLA	BÓKA J.

PRILOGA

Priloga k Uredbi (EU) 2019/881 se spremeni:

(1) točke 2 do 5 se nadomestijo z naslednjim:

„2. Organ za ugotavljanje skladnosti je organ tretje strani, neodvisen od organizacije ali proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, katerih skladnost ugotavlja.

3. Organ, ki je del poslovnega združenja ali strokovne zveze, ki zastopa podjetja, vključena v zasnovo, proizvodnjo, dobavo oziroma opravljanje, sestavljanje, uporabo ali vzdrževanje proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, katerih skladnost ugotavlja, se lahko šteje kot organ za ugotavljanje skladnosti, če je zagotovljena njegova neodvisnost in ni nasprotja interesov.

4. Organi za ugotavljanje skladnosti, njihovo najvišje vodstvo in osebe, odgovorne za izvajanje nalog ugotavljanja skladnosti, niso snovalci, proizvajalci, dobavitelji oziroma ponudniki, monterji, kupci, lastniki, uporabniki ali vzdrževalci proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve, katerih skladnost ugotavljajo, niti niso pooblaščeni zastopniki katere koli od navedenih strani. Ta prepoved ne onemogoča uporabe proizvodov IKT, za katere se ugotavlja skladnost in ki so nujno potrebni za delovanje organa za ugotavljanje skladnosti, ali uporabe takih proizvodov IKT za osebne namene.

5. Organi za ugotavljanje skladnosti, njihovo najvišje vodstvo in osebe, odgovorne za izvajanje nalog ugotavljanja skladnosti, ne sodelujejo neposredno pri snovanju, proizvodnji ali izdelavi, dobavi, trženju, montaži, uporabi ali vzdrževanju proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev, katerih skladnost ugotavljajo, niti ne zastopajo strani, ki sodelujejo pri teh dejavnostih. Organi za ugotavljanje skladnosti, njihovo najvišje vodstvo in osebe, odgovorne za izvajanje nalog ugotavljanja skladnosti, ne sodelujejo pri nobenih dejavnostih, ki bi lahko bile v nasprotju z njihovo neodvisno presojo ali integriteto v zvezi z njihovimi dejavnostmi za ugotavljanje skladnosti. Ta prepoved velja zlasti za svetovalne storitve.“;

(2) točka 10 se spremeni:

(a) uvodno besedilo se nadomesti z naslednjim:

„10. Vedno ter za vsak postopek ugotavljanja skladnosti in vsako vrsto, kategorijo ali podkategorijo proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve ima organ za ugotavljanje skladnosti na razpolago:“;

(b) točka (c) se nadomesti z naslednjim:

„(c) postopke za izvajanje dejavnosti, pri katerih je ustrezno upoštevana velikost podjetja, sektor, v katerem deluje, njegova struktura, stopnja zahtevnosti tehnologije proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve in masovna ali serijska narava proizvodnega postopka.“;

(3) točki 19 in 20 se nadomestita z naslednjim:

„19. Organi za ugotavljanje skladnosti izpolnjujejo zahteve ustreznega harmoniziranega standarda, kakor je opredeljen v členu 2, točka 9, Uredbe (ES) št. 765/2008, za akreditacijo organov za ugotavljanje skladnosti, ki izvajajo certificiranje proizvodov IKT, storitev IKT, postopkov IKT ali upravljanih varnostnih storitev.

20. Organi za ugotavljanje skladnosti zagotovijo, da preskuševalni laboratoriji, v katerih se izvaja ugotavljanje skladnosti, izpolnjujejo zahteve ustreznega harmoniziranega standarda, kakor je opredeljen v členu 2, točka 9, Uredbe (ES) št. 765/2008, za akreditacijo laboratorijev, ki izvajajo preskuse.“.

V zvezi s tem aktom je bila podana izjava, ki je na voljo v UL C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.