15.4.2024 A9-0307/2

Predlog spremembe 2
Cristian-Silviu Buşoi
v imenu Odbora za industrijo, raziskave in energetiko

Poročilo **A9-0307/2023**
Josianne Cutajar
Upravljane varnostne storitve
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Predlog uredbe
–

PREDLOGI SPREMEMB EVROPSKEGA PARLAMENTA*

k predlogu Komisije

UREDBA (EU) 2024/...
EVROPSKEGA PARLAMENTA IN SVETA

z dne ...

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,

* Spremembe: krepki ležeči tisk označuje novo ali spremenjeno besedilo, simbol ▌ pa tiste dele besedila, ki so bili črtani.

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

po posvetovanju z Odborom regij,

v skladu z rednim zakonodajnim postopkom[2],

[1] ***UL L 349, 29.9.2023, str. 167.***

[2] ***Stališče Evropskega parlamenta z dne … [(UL …)/(še ni objavljeno v Uradnem listu)] in sklep Sveta z dne …***

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 namene 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 bila Unija odporna proti kibernetskim napadom in da njen trg ne bi postal ranljiv, naj bi ta uredba dopolnila horizontalni regulativni okvir, ki določa zahteve glede kibernetske varnosti za vse izdelke z digitalnimi elementi v skladu z Uredbo (EU) …/… Evropskega parlamenta in Sveta[4] (2022/0272(COD)), in sicer so v njej določene bistvene zahteve za upravljane kibernetskovarnostne storitve, njihovo uporabo in zanesljivost.

---

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) .../... Evropskega parlamenta in Sveta z dne ... o … (UL L …, ELI: …).***

(3) Upravljane varnostne storitve ***so storitve, ki jih izvajajo ponudniki upravljanih varnostnih storitev, kot so opredeljeni v členu 6, točka (40), Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta***[5]. ***Zato bi morala biti opredelitev upravljanih varnostnih storitev v tej uredbi skladna z opredelitvijo 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 kibernetskovarnostnih incidentov. Zato se ponudniki navedenih storitev štejejo za bistvene ali pomembne subjekte, ki spadajo v visoko kritični sektor v skladu z Direktivo (EU) 2022/2555 ▌. V skladu z uvodno izjavo 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 okrevanje 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. Bistveni in pomembni subjekti v smislu Direktive (EU) 2022/2555 bi zato morali biti bolj skrbni pri izbiri ponudnika upravljanih varnostnih storitev.

---

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 upravljanih varnostnih storitev iz te uredbe zajema neizčrpni seznam upravljanih varnostnih storitev, za katere bi lahko uvedli sheme certificiranja, 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, preprečevanje, odkrivanje, analizo in zmanjševanje tveganja kibernetskih incidentov ter odzivanje nanje in okrevanje 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 lahko obstajajo ločene evropske certifikacijske sheme za kibernetsko varnost. Evropski certifikati kibernetske varnosti, izdani v skladu s temi 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 ***takojšnje okrevanje*** v primeru 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 ocen tveganja EU, da bi ugotovila morebitne ranljivosti. Pri izbiri*** zaupanja ***vrednih ponudnikov ima lahko vlogo certificiranje upravljanih varnostnih storitev***.

(6) Certificiranje upravljanih varnostnih storitev ni pomembno le v postopku izbire za kibernetskovarnostno rezervo EU, temveč je tudi bistven kazalnik kakovosti za zasebne in javne subjekte, ki nameravajo kupiti take storitve. Glede na kritičnost upravljanih varnostnih storitev in občutljivost podatkov, ki se obdelujejo v okviru teh storitev, bi lahko certificiranje potencialnim strankam zagotovilo pomembne smernice in zagotovila glede zanesljivosti teh storitev. Evropske certifikacijske sheme za upravljane varnostne storitve prispevajo k preprečevanju razdrobljenosti enotnega trga. Namen te uredbe je zato izboljšati delovanje notranjega trga.

(7) Uvedba evropskih certifikacijskih shem za upravljane varnostne storitve bi morala privesti do uporabe teh storitev in večje konkurence med njihovimi ponudniki. S certifikacijskami shemami bi morali zato olajšati vstop na trg in ponudbo upravljanih varnostnih storitev, in sicer tako, da bi čim bolj poenostavili morebitne regulativne, upravne in finančne obveznosti, ki bi jih ponudniki, zlasti mikro podjetja ali mala in srednja podjetja (MSP), lahko imeli pri ponudbi teh storitev, pri tem pa ne bi smeli ogrožati cilja, da bodo imeli ti ponudniki zadostno in ustrezno raven zadevnega tehničnega znanja in poklicne integritete. Poleg tega bi morali zato, da bi spodbudili uporabo upravljanih varnostnih storitev in povpraševanje po njih, s temi shemami prispevati k dostopnosti teh storitev, zlasti za manjše akterje, kot so mikro podjetja ter MSP, 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) Mikro podjetja ter MSP je treba podpirati pri izvajanju te uredbe ter zaposlovanju oseb s specializiranimi veščinami in strokovnim znanjem na področju kibernetske varnosti, ki so potrebne, da bi njihove upravljane varnostne storitve izpolnjevale zahteve iz te uredbe. V programu Digitalna Evropa in drugih ustreznih programih Unije je določeno, da Komisija poskrbi za finančno in tehnično podporo – tudi z racionalizacijo finančne podpore iz omenjenih programov ter s podpiranjem mikro podjetij in MSP –, da bi omenjena podjetja lahko prispevala k rasti evropskega gospodarstva in višji skupni ravni evropske kibernetske varnosti v okolju EU.

(9) Z uvedbo certifikacijske sheme Unije za upravljane varnostne storitve bi morale postati bolj razpoložljive varne in visokokakovostne storitve, ki bodo zagotavljale varen digitalni prehod in doseganje ciljev, določenih v programu politike digitalnega desetletja, zlasti v zvezi s ciljem, da 75 % podjetij Unije začne uporabljati računalništvo v oblaku, umetno inteligenco in velepodatke, da več kot 90 % mikro podjetij ter MSP 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 teh 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 upravljanih varnostnih storitev. Da bi se lahko vsi vidiki upravljanih varnostnih storitev vključili v ***namenske certifikacijske sheme***, 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 trga Unije in hkrati vzpostavili partnerstva s podobno mislečimi tretjimi državami, bi bilo treba postopek certificiranja, določen v okviru, vzpostavljenem s to uredbo, racionalizirati, da bi olajšali njegovo mednarodno priznanje in uskladitev z mednarodnimi standardi.

(12) Unija se spoprijema z vrzeljo na področju strokovnjakov, za katero je značilno primanjkovanje usposobljenih delavcev, pa tudi s hitro spreminjajočo se krajino groženj, kot je priznala Komisija v sporočilu z dne 18. aprila 2023 o akademiji za kibernetske veščine. Izobraževalni viri in oblike formalnega usposabljanja so različni, znanje pa je mogoče pridobiti na različne načine, tako formalno, na primer z univerzitetnimi ali študijskimi programi, kot neformalno, na primer z usposabljanjem na delovnem mestu ali delovnimi izkušnjami na ustreznem področju. Da bi se visokokakovostne in bistvene 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 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 znanj in spretnosti na področju kibernetske varnosti, tudi prek evropskega okvira znanj in spretnosti za kibernetsko varnost. Sodelovanje med njimi 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 prakso mladim, tudi osebam, ki prebivajo v prikrajšanih regijah, kot so otoki ter redko poseljena, podeželska in oddaljena območja. S temi ukrepi si je treba tudi prizadevati, da bi k temu področju pritegnili več žensk in deklet ter prispevali k odpravljanju razkoraka med spoloma v naravoslovju, tehnologiji, inženirstvu in matematiki, zasebni sektor pa si mora prizadevati za usposabljanje na delovnem mestu, ki bo usmerjeno v najbolj iskana znanja in spretnosti, in sicer v javni upravi in zagonskih podjetjih, pa tudi v mikro podjetjih in MSP. Pomembno je tudi, da ponudniki teh storitev in države članice sodelujejo in prispevajo k zbiranju podatkov o razmerah na trgu dela na področju kibernetske varnosti in spremembah na njem.

(13) Agencija ENISA ima pomembno vlogo pri pripravi predlog za evropske certifikacijske sheme. 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, na podlagi katerih je mogoče vzpostaviti certifikacijske sheme za kibernetsko varnost za ponudnike upravljanih varnostnih storitev. V njej so določene in pojasnjene tudi nekatere določbe 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 členov 49 in 49a, nikakor ne bi smele vplivati na širšo oceno in pregled navedene uredbe, ki se zahtevata v njenem členu 67, vključno zlasti z oceno vpliva, učinkovitosti in uspešnosti določb naslova omenjene uredbe v zvezi s certifikacijskimi shemami za kibernetsko varnost. Ta ocena in pregled določb naslova v zvezi s certifikacijskimi shemami za kibernetsko varnost bi morala temeljiti na obsežnem posvetovanju z deležniki ter na celoviti in temeljiti analizi zadevnih postopkov.

(15) ***Ker cilja te uredbe, tj. omogočiti sprejetje 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 dosego omenjenega cilja.***

(16) ***V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta[6] je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 10. januarja 2024[7]–***

SPREJELA NASLEDNJO UREDBO:

---

6 ***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).***

7 ***UL C .../....***

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 in 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***, ***tudi strokovno svetovanje, povezano s tehnično podporo***;“;

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

„(20) ‚tehnične specifikacije‘ 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;

(21) ‚stopnja zagotovila‘ 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 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:

(a) stalnim spremljanjem razvoja na področjih, povezanih s standardizacijo, in dajanjem priporočil glede ustreznih tehničnih specifikacij, namenjenih razvoju evropske certifikacijske sheme za kibernetsko varnost na podlagi člena 54(1), točka (c), kadar standardi niso na voljo;

(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;

(c) ocenjevanjem sprejetih evropskih certifikacijskih shem za kibernetsko varnost v skladu s členom 49(8);

(d) sodelovanjem pri medsebojnih strokovnih pregledih na podlagi člena 59(4);

(e) podporo Komisiji pri zagotavljanju sekretariata evropski certifikacijski skupini za kibernetsko varnost na podlagi člena 62(5).“;

(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) v členu 46 se odstavka 1 in 2 nadomestita z naslednjim:

„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. Z njim se potrjuje, 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 navedenih storitev, ter da navedene storitve vedno izvaja osebje z ustreznimi kompetencami, strokovnim znanjem in izkušnjami ter ***zadostno in primerno*** ravnjo ustreznega tehničnega znanja in poklicne integritete.“;

(6) v členu 47 se odstavka 2 in 3 nadomestita z naslednjim:

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

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

(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;

(b) ustrezna politika ali pravo Unije ali politika ali pravo države članice;

(c) povpraševanje na trgu;

(ca) tehnološki razvoj ter razpoložljivost in razvoj mednarodnih certifikacijskih shem za kibernetsko varnost ter mednarodnih in industrijskih standardov;

(d) razvoj kibernetskih groženj;

(e) zahteva za pripravo posebne predloge sheme, ki jo predlaga evropska certifikacijska skupina za kibernetsko varnost.“;

(7) ***člen*** 49 ***se spremeni***:

(a) odstavki 1, 2, 3 in 4 se nadomestijo z naslednjim:

„1. Agencija ENISA na zahtevo Komisije na podlagi člena 48 pripravi predlogo za shemo, ki izpolnjuje ustrezne 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 ustrezne zahteve iz členov 51, 51a, 52 in 54. Če agencija ENISA zahtevo zavrne, mora to obrazložiti. Vsako odločitev o zavrnitvi zahteve sprejme upravni odbor.

3. Pri pripravi predloge za shemo se agencija ENISA pravočasno posvetuje z vsemi ustreznimi deležniki, in sicer v formalnem, odprtem, preglednem in vključujočem posvetovalnem postopku. Agencija ENISA pri oddaji predloge za shemo Komisiji v skladu s členom 49(6) Komisijo seznani, kako je izpolnila to obveznost.

4. Agencija ENISA za vsako predlogo za shemo ustanovi ad hoc delovno skupino v skladu s členom 20(4), da bi agenciji pomagala s specifičnimi nasveti ter strokovnim znanjem in izkušnjami. Ad hoc delovne skupine, ustanovljene v ta namen, po potrebi vključujejo strokovnjake iz javnih uprav držav članic, institucij, organov, uradov in agencij Unije ter iz zasebnega sektorja, pri čemer se ne posega v postopke in diskrecijsko pravico iz člena 20(4) .“;

(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 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 svojo zahtevo agenciji ENISA, naj pripravi predlogo za shemo ali pregleda obstoječo evropsko certifikacijsko shemo za kibernetsko varnost iz člena 48, objavi.

2 V času, ko agencija ENISA v skladu s členom 49 pripravlja predlogo za shemo, lahko Evropski parlament ali Svet od Komisije kot predsedujoče evropski certifikacijski skupini za kibernetsko varnost (ECCG) in agencije ENISA zahteva, 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 po potrebi 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 ali Svet Komisijo in agencijo ENISA pozove 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. Če je ustrezno, Komisija pri ocenjevanju te uredbe v skladu s členom 67 upošteva elemente, ki izhajajo iz stališč Evropskega parlamenta in 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***, kjer je to ustrezno,*** vključujejo najnovejše varnostne posodobitve ***in ne vsebujejo znanih ranljivosti***.“;

(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 stopenj zagotovila za proizvode IKT, storitve IKT, postopke IKT in upravljane varnostne storitve: ‚osnovno‘, ‚znatno‘ ali ‚visoko‘. Stopnja zagotovila 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 stopnji zagotovila, 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‘ stopnjo zagotovila, zagotavlja, da proizvodi IKT, storitve IKT, postopki IKT in upravljane varnostne storitve, za katere se izda navedeni certifikat ali navedena 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‘ stopnjo zagotovila, zagotavlja, da proizvodi IKT, storitve IKT, postopki IKT in 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 omejenimi veščinami in viri. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo najmanj naslednje: pregled za dokazovanje, da se javno znane ranljivosti 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‘ stopnjo zagotovila, zagotavlja, da proizvodi IKT, storitve IKT, postopki IKT in 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 obsežnimi veščinami in viri. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo najmanj naslednje: pregled za dokazovanje, da se javno znane ranljivosti ne pojavljajo; testiranje za dokazovanje, da se pri proizvodih IKT, storitvah IKT, postopkih IKT ali upravljanih varnostnih storitvah pravilno izvajajo potrebne najsodobnejše varnostne funkcionalnosti, in ocenjevanje njihove odpornosti proti veščim 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 in 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 iz 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 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 in upravljanih varnostnih storitev;“;

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

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

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

„(j) pravila za spremljanje skladnosti proizvodov IKT, storitev IKT, postopkov IKT in 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;“;

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

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

(d) 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 in upravljanih varnostnih storitev, varnostnih zahtev, meril in metod za ocenjevanje ter stopenj zagotovila;“;

(e) 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 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:

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

„(a) upošteva učinek ukrepov na proizvajalce ali ponudnike takšnih 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;“;

(bb) 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, vključno ***s posebnimi interesi in potrebami mikro podjetij ter*** MSP;“***;***

(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 iz člena 58, če 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 ranljivostih ali nepravilnostih v zvezi z varnostjo certificiranega proizvoda IKT, storitve IKT, postopka IKT ali upravljanih varnostnih storitev, ki bi lahko vplivale na njihovo 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 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 in 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 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 trg Unije.“***;***

(19) Priloga se nadomesti z besedilom iz Priloge 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 ...,

Za Evropski parlament	*Za Svet*
predsednica	*predsednik/predsednica*

PRILOGA

ZAHTEVE, KI JIH MORAJO IZPOLNJEVATI ORGANI ZA UGOTAVLJANJE SKLADNOSTI

Organi za ugotavljanje skladnosti, ki želijo biti akreditirani, izpolnjujejo naslednje zahteve:

1. ***Organ za ugotavljanje skladnosti se ustanovi v skladu z nacionalnim pravom in je pravna oseba.***

2. ***Organ za ugotavljanje skladnosti je organ tretje strani, neodvisen od organizacije ali proizvoda IKT, storitve IKT, postopka IKT ali upravljane varnostne storitve, 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, pri katerih se ugotavlja skladnost in ki so potrebni za delovanje organa za ugotavljanje skladnosti, ali uporabe teh 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.

6. Če je organ za ugotavljanje skladnosti v lasti ali upravljanju javne osebe ali ustanove, sta zagotovljeni in dokumentirani neodvisnost in odsotnost morebitnega nasprotja interesov med nacionalnim certifikacijskim organom za kibernetsko varnost in organom za ugotavljanje skladnosti.

7. Organi za ugotavljanje skladnosti zagotovijo, da dejavnosti njihovih odvisnih družb ali podizvajalcev ne vplivajo na zaupnost, objektivnost in nepristranskost njihovih dejavnosti za ugotavljanje skladnosti.

8. Organi za ugotavljanje skladnosti in njihovo osebje izvajajo dejavnosti za ugotavljanje skladnosti z največjo poklicno integriteto in potrebno tehnično usposobljenostjo na določenem področju brez kakršnih koli pritiskov in spodbud, ki bi lahko vplivali na njihovo presojo ali rezultate njihovih dejavnosti za ugotavljanje skladnosti, vključno s pritiski in spodbudami finančne narave, zlasti od oseb ali skupin oseb, za katere so rezultati navedenih dejavnosti pomembni.

9. Organ za ugotavljanje skladnosti je zmožen izvajati vse naloge ugotavljanja skladnosti, ki so mu dodeljene s to uredbo, ne glede na to, ali te naloge izvaja organ za ugotavljanje skladnosti sam ali se izvajajo v njegovem imenu in pod njegovo odgovornostjo. Vsako podizvajanje s strani zunanjega osebja ali posvetovanje z zunanjim osebjem se ustrezno dokumentira, ne vključuje posrednikov in je predmet pisnega sporazuma, ki med drugim zajema zaupnost in nasprotja interesov. Zadevni organ za ugotavljanje skladnosti prevzame polno odgovornost za opravljene naloge.

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:

(a) osebje s tehničnim znanjem ter zadostnimi in ustreznimi izkušnjami za izvajanje nalog ugotavljanja skladnosti;

(b) opise postopkov, v skladu s katerimi se mora izvajati ugotavljanje skladnosti,

za zagotovitev preglednost in zmožnost reprodukcije navedenih postopkov. Izvaja ustrezne politike in postopke, na podlagi katerih se ločijo naloge, ki jih izvaja kot organ, priglašen na podlagi člena 61, in njegove druge dejavnosti;

(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.

11. Organ za ugotavljanje skladnosti ima potrebna sredstva za ustrezno izvajanje tehničnih in upravnih nalog, povezanih z dejavnostmi za ugotavljanje skladnosti, ter dostop do vse potrebne opreme in prostorov.

12. Osebe, odgovorne za izvajanje dejavnosti za ugotavljanje skladnosti, imajo:

(a) dobro tehnično in poklicno usposobljenost, ki zajema vse dejavnosti za ugotavljanje skladnosti;

(b) zadovoljivo znanje o zahtevah glede ugotavljanja skladnosti, ki ga izvajajo, in ustrezna pooblastila za izvedbo tega;

(c) primerno znanje in razumevanje veljavnih zahtev in standardov preskušanja;

(d) zmožnost, ki je potrebna za pripravo certifikatov, zapisov in poročil, ki dokazujejo, da so bila ugotavljanja skladnosti izvedena.

13. Zagotovi se nepristranskost organa za ugotavljanje skladnosti, njegovega najvišjega vodstva in oseb, odgovornih za izvajanje dejavnosti ugotavljanja skladnosti ter morebitnih podizvajalcev.

14. Plačilo najvišjega vodstva in oseb, odgovornih za dejavnosti ugotavljanja skladnosti, ni odvisno od števila opravljenih ugotavljanj skladnosti ali rezultatov navedenih ugotavljanj skladnosti.

15. Organi za ugotavljanje skladnosti sklenejo zavarovanje odgovornosti, razen če odgovornost prevzame država članica v skladu z nacionalnim pravom ali če je država članica sama neposredno odgovorna za ugotavljanje skladnosti.

16. Organ za ugotavljanje skladnosti in njegovo osebje, odbori, odvisne družbe, podizvajalci ter povezani organi ali osebje zunanjih organov organa za

ugotavljanje skladnosti spoštujejo zaupnost informacij in so zavezani k poklicni molčečnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog ugotavljanja skladnosti iz te uredbe ali na podlagi katere koli določbe nacionalnega prava za izvajanje te uredbe, razen kadar njihovo razkritje zahteva pravo Unije ali države članice, ki velja za te osebe, in razen pred pristojnimi organi držav članic, v katerih se izvajajo njegove dejavnosti. Pravice intelektualne lastnine so zaščitene. Organ za ugotavljanje skladnosti vzpostavi dokumentirane postopke v zvezi z zahtevami iz te točke.

17. Z izjemo točke 16 zahteve iz te priloge ne izključujejo izmenjave tehničnih informacij in regulativnih navodil med organom za ugotavljanje skladnosti in osebo, ki zaprosi za certifikacijo ali preučuje možnost, da bi to storila.

18. Organi za ugotavljanje skladnosti delujejo v skladu z vrsto doslednih, poštenih in razumnih pogojev, ob upoštevanju interesov MSP v zvezi s pristojbinami.

19. Organi za ugotavljanje skladnosti izpolnjujejo zahteve ustreznega standarda, harmoniziranega na podlagi 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 standarda, harmoniziranega na podlagi Uredbe (ES) št. 765/2008, za akreditacijo laboratorijev, ki izvajajo preskuse.

Or. en