Uradni list
Evropske unije

SL
Serija L

2025/2540

12.12.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/2540

z dne 9. decembra 2025

o določitvi pravil za uporabo Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta glede določitve načrta za medsebojne strokovne preglede

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (Agencija ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) ([1]) in zlasti člena 59(5) Uredbe,

ob upoštevanju naslednjega:

(1) V skladu s členom 59(4) Uredbe (EU) 2019/881 medsebojne strokovne preglede nacionalnih certifikacijskih organov za kibernetsko varnost (v nadaljnjem besedilu: organi NCCA (*national cybersecurity certification authorities*)) izvajata dva organa NCCA iz drugih držav članic in Komisije. Da bi dosegli enakovredne standarde v zvezi z evropskimi certifikati kibernetske varnosti in izjavami EU o skladnosti, bi morala Komisija spremljati vidike, povezane s skladnostjo s to uredbo, in zagotoviti, da se medsebojni strokovni pregledi izvajajo dosledno po vsej Uniji. Da se pripomore k opredelitvi dobrih praks, izzivov in izkušenj, pridobljenih pri izvajanju evropskih certifikacijskih shem za kibernetsko varnost, bi morala imeti Agencija Evropske unije za kibernetsko varnost (ENISA) možnost, da v medsebojnih strokovnih pregledih sodeluje kot opazovalka. V podporo usklajenemu izvajanju določb te uredbe bi bilo treba agenciji ENISA v sodelovanju s Komisijo in evropsko certifikacijsko skupino za kibernetsko varnost omogočiti tudi pripravo predlog.

(2) Za zagotovitev predvidljivega načrtovanja in učinkovite dodelitve virov bi bilo treba medsebojne strokovne preglede vsakega organa NCCA izvesti v skladu z določenim časovnim razporedom. Organ NCCA bi moral imeti možnost, da zahteva odložitev medsebojnega strokovnega pregleda v izjemnih okoliščinah, kot je nepričakovano pomanjkanje osebja ali višja sila. V ta namen je treba določiti ureditve za presojo te zahteve, pri čemer je treba zagotoviti, da se ohrani splošni časovni razpored in da se ne ogrozijo cilji mehanizma medsebojnega strokovnega pregleda.

(3) Da bi zagotovili, da vse države članice prispevajo k izvajanju mehanizma medsebojnega strokovnega pregleda, in jim omogočili, da izkoristijo prednosti vzajemnega učenja, bi morali organi NCCA vsake države članice v petletnem obdobju izvesti dva medsebojna strokovna pregleda. Zato bi bilo treba vzpostaviti sistem rotacije, ki bi organom NCCA vseh držav članic omogočil organizacijo njihovega sodelovanja. Določiti je treba tudi merila, ki bi jih morali organi NCCA upoštevati pri izbiri predstavnikov za izvajanje medsebojnih strokovnih pregledov, da bi zagotovili ustrezno strokovno znanje in kompetence. Organom NCCA bi bilo treba tudi omogočiti, da sodelujejo pri medsebojnih strokovnih pregledih kot opazovalci za namene spremljanja in učenja iz procesa. V takih primerih se od njihovega predstavnika ne bi smelo zahtevati, da ima enako strokovno znanje in kompetence, kot se pričakuje od predstavnikov organov NCCA, ki izvajajo medsebojne strokovne preglede.

(4) Za zagotovitev, da vsaj en NCCA, ki uporablja enak pristop k izdajanju certifikatov na „visoki“ ravni, opravi medsebojni strokovni pregled drugega NCCA, bi morala agencija ENISA, ko organe NCCA pozove, naj izrazijo interes za izvajanje medsebojnih strokovnih pregledov, navesti, ali NCCA, pri katerem se izvaja medsebojni strokovni pregled, neposredno izdaja certifikate na „visoki“ ravni, uporablja model predhodne odobritve iz člena 56(6), točka (a), Uredbe (EU) 2019/881, odobri splošni prenos pooblastil v skladu s točko (b) navedenega odstavka ali ima kombinacijo teh značilnosti.

([1]) UL L 151, 7.6.2019, str. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(5) Za zagotovitev skupnih ocenjevalnih meril in postopkov za izvajanje medsebojnih strokovnih pregledov po vsej Uniji bi moral vsak medsebojni strokovni pregled vedno vključevati vprašalnik za samoocenjevanje, pregled dokumentacije in obisk na kraju samem z razgovori. Po obisku na kraju samem bi morala skupina za medsebojne strokovne preglede o ugotovitvah razpravljati z NCCA, pri katerem se izvaja medsebojni strokovni pregled, pripraviti osnutek poročila in ga predložiti zadevnemu NCCA, da poda pripombe in se tako po možnosti zagotovi soglasje. Skupina za medsebojne strokovne preglede bi morala evropski certifikacijski skupini za kibernetsko varnost predložiti končno poročilo, ki lahko vključuje smernice ali priporočila, da se omogoči izboljšanje stanja za NCCA, pri katerem je bil izveden medsebojni strokovni pregled. Evropska certifikacijska skupina za kibernetsko varnost bi morala na predlog skupine za medsebojne strokovne preglede potrditi tudi zbirno poročilo, ki bo javno dostopno.

(6) Za zagotovitev varne obravnave informacij, pridobljenih s postopkom medsebojnega strokovnega pregleda, bi morala skupina za medsebojne strokovne preglede zagotoviti uporabo varnih komunikacijskih kanalov, kot je varna platforma za shranjevanje in izmenjavo dokumentov, ter uporabo ustreznih zaščitnih ukrepov za zaupne podatke, ki si jih izmenjujejo člani skupine za medsebojne strokovne preglede. Agencija ENISA bi morala imeti tudi možnost, da ob upoštevanju obstoječih najboljših praks organov NCCA pripravi smernice o tem, kako zagotoviti varno komunikacijo, zlasti za zagotovitev, da je raven varnosti, ki jo uporablja skupina za medsebojne strokovne preglede pri zbiranju, izmenjavi in obdelavi informacij, usklajena z varnostnimi potrebami NCCA, pri katerem se izvaja medsebojni strokovni pregled.

(7) Da bi olajšali sodelovanje in učinkovito izmenjavo informacij med organi NCCA, bi morala evropska certifikacijska skupina za kibernetsko varnost, zlasti njena podskupina za medsebojne strokovne preglede, prispevati k razvoju predlog in pomagati Komisiji pri izvajanju te uredbe.

(8) Mehanizem medsebojnih strokovnih pregledov pomeni vseevropsko digitalno javno storitev v smislu Uredbe (EU) 2024/903 Evropskega parlamenta in Sveta ([2]). Ta uredba uvaja nove zavezujoče zahteve, ki vplivajo na navedeno storitev, zato zanjo velja obveznost ocene interoperabilnosti iz člena 3 Uredbe (EU) 2024/903. V skladu s tem je bila izvedena ocena interoperabilnosti, poročilo o njej pa bo objavljeno na portalu interoperabilne Evrope.

(9) Komisija je pri pripravi te uredbe upoštevala stališča evropske certifikacijske skupine za kibernetsko varnost, vključno z njeno podskupino za medsebojne strokovne preglede.

(10) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega s členom 66 Uredbe (EU) 2019/881 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Časovni razpored, pogostost in stroški medsebojnih strokovnih pregledov

1. Medsebojni strokovni pregledi nacionalnih certifikacijskih organov za kibernetsko varnost (v nadaljnjem besedilu: organi NCCA (*national cybersecurity certification authorities*)) se izvedejo v skladu s časovnim razporedom iz Priloge I. Vsak medsebojni strokovni pregled mora biti izveden do datuma, navedenega v tem razporedu, in se nato izvaja vsakih pet let.

2. V izjemnih okoliščinah lahko NCCA, pri katerem se izvaja medsebojni strokovni pregled, Komisiji predloži ustrezno utemeljeno zahtevo za odložitev tega postopka medsebojnega strokovnega pregleda na poznejši datum, kot je naveden v razporedu iz Priloge I. Komisija v sodelovanju z evropsko certifikacijsko skupino za kibernetsko varnost, ustanovljeno s členom 62 Uredbe (EU) 2019/881, oceni zahtevo in o rezultatu pravočasno obvesti vse zadevne strani.

([2]) Uredba (EU) 2024/903 Evropskega parlamenta in Sveta z dne 13. marca 2024 o določitvi ukrepov za visoko raven interoperabilnosti javnega sektorja v Uniji (Akt o interoperabilni Evropi) (UL L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. Kadar država članica v skladu s členom 58(1) Uredbe (EU) 2019/881 imenuje:

(a) več organov NCCA na svojem ozemlju, se za vse organe NCCA v navedeni državi članici hkrati izvedejo medsebojni strokovni pregledi;

(b) organ ali organe NCCA druge države članice, se lahko medsebojni strokovni pregledi za navedeni organ oz. organe NCCA izvedejo v skladu s časovnim razporedom, določenim bodisi za državo članico, ki organe imenuje, bodisi za državo članico, v kateri so bili ti organi imenovani, in sicer v zvezi z nadzornimi nalogami, ki se izvajajo v državi članici, ki organe imenuje.

4. Agencija Evropske unije za kibernetsko varnost (ENISA) na spletišču o evropskih certifikacijskih shemah za kibernetsko varnost, vzpostavljenem v skladu s členom 50 Uredbe (EU) 2019/881, objavi naslednje informacije:

(a) informacije o časovnem razporedu iz Priloge I;

(b) seznam organov NCCA, ki izvajajo medsebojne strokovne preglede, ki se vodi v skladu s členom 2(5).

5. Vsak organ NCCA, vključen v postopek medsebojnega strokovnega pregleda, krije svoje stroške sodelovanja.

Člen 2

Rotacijski sistem za organe NCCA, ki izvajajo medsebojne strokovne preglede

1. V skladu s členom 59(4) Uredbe (EU) 2019/881 vsak medsebojni strokovni pregled izvedeta dva organa NCCA iz drugih držav članic in Komisije. Organi NCCA vsake države članice sodelujejo pri medsebojnem strokovnem pregledu vsaj dveh organov NCCA v vsakem obdobju iz Priloge I.

2. Organi NCCA drugih držav članic lahko pri medsebojnem strokovnem pregledu sodelujejo kot opazovalci z enim ali več predstavniki, če se s tem strinjajo organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, organa NCCA, ki izvajata medsebojni strokovni pregled, in Komisija.

3. En predstavnik agencije ENISA lahko sodeluje pri medsebojnem strokovnem pregledu kot opazovalec. Sodelujejo lahko tudi dodatni predstavniki, če se s tem strinjajo organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, organa NCCA, ki izvajata medsebojni strokovni pregled, in Komisija.

4. Opazovalci imajo dostop do istih informacij kot drugi člani skupine za medsebojne strokovne preglede, vendar ne izvajajo nalog, povezanih z izvajanjem medsebojnega strokovnega pregleda.

5. ENISA v sodelovanju s Komisijo in evropsko certifikacijsko skupino za kibernetsko varnost predlaga in vodi seznam organov NCCA, ki izvajajo medsebojne strokovne preglede v skladu s časovnim razporedom iz Priloge I. V danem letu agencija ENISA v sodelovanju s Komisijo pozove organe NCCA, da izrazijo interes za izvajanje medsebojnih strokovnih pregledov organov NCCA v skladu s časovnim razporedom iz Priloge I za naslednje leto ali za sodelovanje pri njih kot opazovalci.

6. Kadar več kot dva NCCA izrazita interes za izvedbo medsebojnega strokovnega pregleda istega organa NCCA, se Komisija in agencija ENISA posvetujeta z zainteresiranimi organi NCCA in se odločita o udeležencih medsebojnega strokovnega pregleda.

7. Kadar v danem letu ni dovolj organov NCCA, ki bi izrazili interes za izvajanje medsebojnih strokovnih pregledov, Komisija po posvetovanju z evropsko certifikacijsko skupino za kibernetsko varnost izbere organe NCCA za izvajanje medsebojnih strokovnih pregledov. Komisija pri izbiri upošteva obveznost organov NCCA vsake države članice iz odstavka 1, da sodelujejo pri medsebojnem strokovnem pregledu vsaj dveh organov NCCA.

Člen 3

Merila za sestavo skupine za medsebojne strokovne preglede

1. Vsak organ NCCA, ki izvaja medsebojni strokovni pregled, pravočasno pred začetkom medsebojnega strokovnega pregleda imenuje enega predstavnika za izvajanje medsebojnega strokovnega pregleda. Organi NCCA, ki izvajajo medsebojne strokovne preglede, lahko imenujejo več predstavnikov, kadar je to potrebno za zagotovitev, da ima skupina za medsebojne strokovne preglede potrebne kompetence za izvajanje teh pregledov.

2. Predstavnik organov NCCA, ki izvajajo medsebojne strokovne preglede, razen predstavnikov organov NCCA, ki sodelujejo kot opazovalci, izpolnjuje naslednja merila:

(a) vsaj dve leti je delal za NCCA, ki izvaja medsebojni strokovni pregled, ali je sodeloval pri vsaj dveh medsebojnih strokovnih pregledih kot opazovalec;

(b) ima zadostno znanje o certifikacijskem okviru za kibernetsko varnost iz Uredbe (EU) 2019/881;

(c) dobro obvlada angleščino in, če je mogoče, enega ali več jezikov, ki se govorijo v državi članici organov NCCA, pri katerih se izvajajo medsebojni strokovni pregledi;

(d) deluje neodvisno od organa NCCA, pri katerem se izvaja medsebojni strokovni pregled.

3. Organi NCCA, ki izvajajo medsebojne strokovne preglede, zagotovijo, da se vsako tveganje nasprotja interesov v zvezi z imenovanimi predstavniki razkrije drugim organom NCCA, Komisiji in agenciji ENISA pred začetkom postopka medsebojnega strokovnega pregleda. Organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, lahko v skladu z odstavkom 5 nasprotuje imenovanju posameznih predstavnikov.

4. Organa NCCA, ki izvajata medsebojni strokovni pregled, izbereta iz svojih vrst predstavnika (v nadaljnjem besedilu: vodja skupine), ki usklajuje medsebojni strokovni pregled.

5. Komisija organu NCCA, pri katerem se izvaja medsebojni strokovni pregled, pred začetkom postopka medsebojnega strokovnega pregleda predloži imena in kontaktne podatke predstavnikov organov NCCA, ki izvajata medsebojni strokovni pregled. Kadar želi organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, nasprotovati imenovanju enega ali več predstavnikov, v dveh tednih Komisiji predloži jasno utemeljitev, o tem obvesti agencijo ENISA in evropsko certifikacijsko skupino za kibernetsko varnost ter zahteva, da organ NCCA, ki izvaja medsebojni strokovni pregled, imenuje drugega predstavnika.

6. Kadar postopek iz odstavka 5 povzroči neupravičene zamude pri začetku medsebojnega strokovnega pregleda zaradi izjemnih okoliščin, Komisija v posvetovanju z agencijo ENISA in evropsko certifikacijsko skupino za kibernetsko varnost odloči o sestavi skupine za medsebojne strokovne preglede.

Člen 4

Metodologija za medsebojni strokovni pregled

1. Pri medsebojnem strokovnem pregledu se ocenijo vidiki iz Priloge II v skladu s členom 59(3) Uredbe (EU) 2019/881.

2. Agencija ENISA lahko v sodelovanju z evropsko certifikacijsko skupino za kibernetsko varnost in Komisijo pripravi predloge za oceno postopkov, ki jih vzpostavi organ NCCA, pri katerem se izvaja medsebojni strokovni pregled.

3. Medsebojni strokovni pregled vključuje naslednje:

(a) vprašalnik za samooceno,

(b) oceno ustrezne dokumentacije,

(c) razgovore v živo ali prek spleta ali oboje;

(d) obisk na kraju samem.

4. O dolžini medsebojnega strokovnega pregleda se lahko vnaprej dogovorita skupina za medsebojne strokovne preglede in organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, odvisno od obsega in zapletenosti dejavnosti organa NCCA, pri katerem se izvaja medsebojni strokovni pregled. Obisk na kraju samem ne sme trajati dlje kot tri delovne dni.

5. Če se skupina za medsebojne strokovne preglede, organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, in Komisija ne dogovorijo drugače, je jezik sodelovanja angleščina. Poročilo o medsebojnem strokovnem pregledu iz člena 5 se pripravi vsaj v angleščini.

6. Organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, sodeluje s skupino za medsebojne strokovne preglede in ji zagotovi dostop do informacij in dokumentov, ki so potrebni za izvedbo medsebojnega strokovnega pregleda. Organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, predloži vprašalnik za samooceno in zadnje letno zbirno poročilo, sprejeto v skladu s členom 58(7), točka (g), Uredbe (EU) 2019/881, vsaj 21 dni pred datumom obiska na kraju samem. Dodatni dokumenti se na zahtevo skupine za medsebojne strokovne preglede predložijo v sedmih dneh od prejema takih zahtev.

7. Dokumenti se predložijo v angleščini, razen če je v skladu z odstavkom 5 dogovorjeno drugače. Kadar dokumenti niso na voljo v angleščini, lahko skupina za medsebojne strokovne preglede zahteva, da se dokumenti, potrebni za izvedbo medsebojnega strokovnega pregleda, prevedejo v angleščino.

8. Pred pripravo poročila o medsebojnem strokovnem pregledu v skladu s členom 5 se skupina za medsebojne strokovne preglede o predhodnih ugotovitvah pogovori z organom NCCA, pri katerem se izvaja medsebojni strokovni pregled.

Člen 5

Poročilo o medsebojnem strokovnem pregledu

1. Skupina za medsebojne strokovne preglede v 21 dneh po izvedbi medsebojnega strokovnega pregleda pripravi osnutek poročila o navedenem pregledu, ki vključuje podrobnosti o državi članici organa NCCA, pri katerem je bil izveden medsebojni strokovni pregled, organih NCCA, ki sta izvedla medsebojni strokovni pregled, Komisiji in morebitnih opazovalcih ter ugotovitve in zaključke medsebojnega strokovnega pregleda. Poročila vsebujejo priporočila za izboljšanje vidikov, zajetih v medsebojnem strokovnem pregledu.

2. Agencija ENISA lahko v sodelovanju s Komisijo in evropsko certifikacijsko skupino za kibernetsko varnost pripravi predlogo za poročilo o medsebojnem strokovnem pregledu.

3. Skupina za medsebojne strokovne preglede po pripravi osnutka poročila o medsebojnem strokovnem pregledu v skladu z odstavkom 1 ta osnutek predloži organu NCCA, pri katerem je bil izveden medsebojni strokovni pregled, da ta v 14 dneh poda pripombe. Skupina za medsebojne strokovne preglede oceni pripombe in jih po možnosti vključi v končno poročilo, da se zagotovi soglasje. V primeru nesoglasja se odgovor NCCA, pri katerem je bil izveden medsebojni strokovni pregled, priloži končnemu poročilu.

4. Končno poročilo se v dveh mesecih od izvedbe medsebojnega strokovnega pregleda pošlje evropski certifikacijski skupini za kibernetsko varnost, vključno s povzetkom za objavo. V skladu s členom 59(6) Uredbe (EU) 2019/881 evropska certifikacijska skupina za kibernetsko varnost pregleda poročilo in potrdi njegov povzetek, ki se objavi na spletišču o evropskih certifikacijskih shemah za kibernetsko varnost, vzpostavljenem v skladu s členom 50 Uredbe (EU) 2019/881. Povzetek vključuje tudi odgovor organa NCCA, pri katerem je bil izveden medsebojni strokovni pregled, ali dele tega odgovora v dogovoru z navedenim organom NCCA.

5. Skupina za medsebojne strokovne preglede anonimizira osebne podatke, ki jih je morda zbrala med medsebojnim strokovnim pregledom, preden poročilo o medsebojnem strokovnem pregledu razpošlje prejemnikom, ki niso del skupine za medsebojne strokovne preglede.

Člen 6

Zaupnost

1. Vse strani, ki so vključene v medsebojne strokovne preglede, spoštujejo zaupnost informacij in podatkov, pridobljenih pri opravljanju svojih nalog in dejavnosti, tako da varujejo zlasti:

(a) pravice intelektualne lastnine in zaupne poslovne informacije ali poslovne skrivnosti fizične ali pravne osebe, vključno z izvorno kodo, razen v primerih iz člena 5 Direktive (EU) 2016/943 Evropskega parlamenta in Sveta ([3]);

(b) učinkovito izvajanje te uredbe.

(c) javne interese in interese nacionalne varnosti;

(d) celovitost kazenskih ali upravnih postopkov.

2. Skupina za medsebojne strokovne preglede zagotovi, da se z vsemi informacijami, pridobljenimi s postopkom medsebojnega strokovnega pregleda, ravna varno. Skupina za medsebojne strokovne preglede, vključno z vsemi opazovalci, po pripravi končnega poročila in povzetka iz člena 5(4) izbriše ali uniči vse dokumente, razen končnega poročila in povzetka, ki so bili zbrani ali ustvarjeni v postopku medsebojnega strokovnega pregleda.

3. Agencija ENISA lahko ob upoštevanju obstoječih najboljših praks organov NCCA v sodelovanju z evropsko certifikacijsko skupino za kibernetsko varnost pripravi smernice za varno in zaupno komunikacijo.

([3]) Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem (UL L 157, 15.6.2016, str. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Člen 7

Krepitev zmogljivosti

Agencija ENISA analizira zbirne rezultate medsebojnih strokovnih pregledov ter izpostavi pridobljene izkušnje in dobre najboljše prakse, da bi prispevala h krepitvi zmogljivosti organov NCCA in vzdrževanju evropskih certifikacijskih shem za kibernetsko varnost. Ta analiza lahko po potrebi vključuje usposabljanje in dodatne smernice za organe NCCA, pripravljene v sodelovanju z evropsko certifikacijsko skupino za kibernetsko varnost.

Člen 8

Začetek veljavnosti

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, 9. decembra 2025

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

Razpored nacionalnih certifikacijskih organov za kibernetsko varnost (NCCA), pri katerih se izvede medsebojni strokovni pregled

Pri organih NCCA naslednjih držav članic se medsebojni strokovni pregled izvede do 31. decembra 2026 in nato vsakih pet let:

Belgija, Češka, Malta, Nemčija, Slovaška, Švedska

Pri organih NCCA naslednjih držav članic se medsebojni strokovni pregled izvede do 31. decembra 2027 in nato vsakih pet let:

Estonija, Grčija, Italija, Madžarska, Nizozemska, Slovenija

Pri organih NCCA naslednjih držav članic se medsebojni strokovni pregled izvede do 31. decembra 2028 in nato vsakih pet let:

Bolgarija, Danska, Hrvaška, Irska, Litva, Španija

Pri organih NCCA naslednjih držav članic se medsebojni strokovni pregled izvede do 31. decembra 2029 in nato vsakih pet let:

Avstrija, Finska, Latvija, Luksemburg, Poljska, Romunija

Pri organih NCCA naslednjih držav članic in držav EGP/Efte se medsebojni strokovni pregled izvede do 31. decembra 2030 in nato vsakih pet let:

Ciper, Francija, Islandija, Lihtenštajn, Norveška, Portugalska

PRILOGA II

Metodologija medsebojnega strokovnega pregleda

II.1 **Ločevanje med certifikacijskimi in nadzornimi dejavnostmi**

Kar zadeva oceno ločitve certifikacijskih in nadzornih dejavnosti organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, kot je navedeno v členu 59(3), točka (a), Uredbe (EU) 2019/881, se v medsebojnem strokovnem pregledu ocenijo vsaj naslednji vidiki:

(a) podroben opis delovanja organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, v katerem so jasno opredeljeni različni subjekti in/ali oddelki, vključeni v izvajanje Uredbe (EU) 2019/881;

(b) beleženje dejavnosti organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, glede na dejavnosti iz člena 58(7) Uredbe (EU) 2019/881;

(c) kadar organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, izdaja certifikate, obrazložitev, ki dokazuje, da se njegove dejavnosti certificiranja ne prepletajo z njegovimi nadzornimi dejavnostmi, kot je opredeljeno v točki (b).

II.2 **Nadziranje in izvrševanje pravil za spremljanje skladnosti s certifikati**

Kar zadeva ocenjevanje postopkov organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, za nadziranje in izvrševanje pravil za spremljanje skladnosti proizvodov IKT, storitev IKT in postopkov IKT ter upravljanih varnostnih storitev z evropskimi certifikati kibernetske varnosti iz člena 59(3), točka (b), Uredbe (EU) 2019/881, se v medsebojnem strokovnem pregledu ocenijo vsaj naslednji vidiki:

(a) kakovost in raven podrobnega opisa takih procesov in postopkov ter obseg, v katerem so dokumentirani;

(b) ali in v kolikšni meri taki procesi in postopki zajemajo ustrezne evropske certifikacijske sheme za kibernetsko varnost;

(c) ali je organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, dejansko pooblaščen za pregledovanje organov za ugotavljanje skladnosti, ki izdajajo certifikate, in po potrebi za izvrševanje odvzema certifikatov;

(d) obseg sodelovanja organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, z ustreznimi organi za nadzor trga;

(e) ali ima organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, mehanizem za obravnavo pritožb fizičnih ali pravnih oseb, ki se zahteva v skladu s členom 58(7), točka (f), Uredbe (EU) 2019/881, vključno z dokazi, ali imajo fizične in pravne osebe pravico do vložitve pritožbe in pridobitve učinkovitega sodnega pravnega sredstva v skladu s členom 63 oziroma členom 64 navedene uredbe.

II.3 **Spremljanje in izvrševanje obveznosti proizvajalcev ali ponudnikov**

Kar zadeva ocenjevanje postopkov organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, za spremljanje in izvrševanje obveznosti proizvajalcev ali ponudnikov, ki izvajajo samoocenjevanje skladnosti, kot je navedeno v členu 59(3), točka (c), Uredbe (EU) 2019/881, se v medsebojnem strokovnem pregledu ocenijo vsaj naslednji vidiki:

(a) ali je organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, vzpostavil take postopke in v kolikšni meri so dokumentirani, zlasti ali je vzpostavil mehanizem za prejemanje in obdelavo informacij iz zunanjih virov;

(b) ali in v kolikšni meri taki postopki zajemajo ustrezne evropske certifikacijske sheme za kibernetsko varnost;

(c) ali in v kolikšni meri organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, izvaja lastne preiskave in ali obseg preiskav zajema obveznosti proizvajalcev iz člena 53(2) in (3) Uredbe (EU) 2019/881 ter ustreznih evropskih certifikacijskih shem za kibernetsko varnost;

(d) ali obstaja postopek za izmenjavo informacij med certifikacijskimi in nadzornimi dejavnostmi organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, ki so pomembne za spremljanje in izvrševanje obveznosti proizvajalcev ali ponudnikov.

II.4 **Spremljanje, odobritev in nadziranje organov za ugotavljanje skladnosti**

Kar zadeva ocenjevanje postopkov organa NCCA, pri katerem se izvaja medsebojni strokovni pregled, za spremljanje, odobritev in nadziranje dejavnosti organov za ugotavljanje skladnosti, kot je navedeno v členu 59(3), točka (d), Uredbe (EU) 2019/881, se v medsebojnem strokovnem pregledu ocenijo vsaj naslednji vidiki:

(a) kakovost in raven podrobnega opisa takih postopkov ter obseg, v katerem so dokumentirani, tudi za sodelovanje z nacionalnim akreditacijskim organom;

(b) ključni statistični podatki o številu izdanih, začasno preklicanih ali odvzetih pooblastil, skupnem številu organov za ugotavljanje skladnosti, ki opravljajo dejavnost, številu izdanih certifikatov in številu popravnih ukrepov, ki jih je sprejel organ NCCA, pri katerem se izvaja medsebojni strokovni pregled;

(c) kadar organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, omogoča izdajo evropskih certifikatov kibernetske varnosti na „visoki“ ravni po predhodni odobritvi ali na podlagi splošnega prenosa naloge, kot je določeno v členu 56(6) Uredbe (EU) 2019/881, strokovno znanje osebja in postopki, s katerimi organ NCCA, pri katerem se izvaja medsebojni strokovni pregled, spremlja in nadzoruje dejavnosti organov za ugotavljanje skladnosti.