
# Mnenje št. 5/2020 o osnutku sklepa pristojnega nadzornega organa Luksemburga glede odobritve zahtev za akreditacijo telesa za certificiranje v skladu s členom 43.3 (Splošna uredba o varstvu podatkov)

**Sprejeto 29. januarja 2020.**

Sprejeto

# Kazalo

## Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 63, člena 64(1c) in (3)–(8) ter člena 43(3) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov),

ob upoštevanju člena 51(1b) Direktive (EU) 2016/680 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (v nadaljnjem besedilu: Direktiva o kazenskem pregonu).

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 10 in 22 svojega poslovnika z dne 25. maja 2018,

ob upoštevanju naslednjega:

(1) Glavna vloga Evropskega odbora o varstvu podatkov (v nadaljnjem besedilu: Odbor) je zagotavljati dosledno uporabo Uredbe (EU) 2016/679 (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov) v celotnem Evropskem gospodarskem prostoru. V skladu s členom 64(1) Splošne uredbe o varstvu podatkov Odbor izda mnenje, kadar namerava nadzorni organ odobriti zahteve za akreditacijo teles za certificiranje v skladu s členom 43. Cilj tega mnenja je zato zagotoviti usklajen pristop glede zahtev, ki jih bo nadzorni organ za varstvo podatkov ali nacionalni akreditacijski organ uporabljal pri akreditaciji telesa za certificiranje. Splošna uredba o varstvu podatkov sicer neposredno ne uvaja enotnega sklopa zahtev za akreditacijo, spodbuja pa doslednost. Odbor si v svojih mnenjih prizadeva doseči ta cilj, prvič, s spodbujanjem nadzornih organov, naj pripravijo osnutek svojih zahtev za akreditacijo ob upoštevanju strukture iz Priloge k smernicam Odbora o akreditaciji teles za certificiranje, in, drugič, z analiziranjem takih zahtev na podlagi predloge Odbora, ki omogoča primerjalno analizo zahtev (v skladu z ISO 17065 in smernicami Odbora o akreditaciji teles za certificiranje).

(2) V skladu s členom 43 Splošne uredbe o varstvu podatkov pristojni nadzorni organi sprejmejo zahteve za akreditacijo. Vendar uporabijo mehanizem za skladnost, da omogočijo vzpostavitev zaupanja v mehanizem certificiranja, zlasti z določitvijo visoke ravni zahtev.

(3) Čeprav se za zahteve za akreditacijo uporablja mehanizem za skladnost, to ne pomeni, da bi morale biti zahteve enake. Pristojni nadzorni organi imajo polje proste presoje glede nacionalnih ali regionalnih okoliščin, pri čemer bi morali upoštevati svojo lokalno zakonodajo. Cilj mnenja Odbora ni doseči enoten sklop zahtev EU, temveč preprečiti pomembna neskladja, ki bi lahko vplivala na primer na zaupanje v neodvisnost ali strokovno znanje akreditiranih teles za certificiranje.

[1] Sklicevanje na „Unijo“ v tem mnenju je treba razumeti kot sklicevanje na „EGP“.

(4) „Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi člena 43 Splošne uredbe o varstvu podatkov (2016/679)“ (v nadaljnjem besedilu: smernice) in „Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe 2016/679“ se bodo uporabljale kot rdeča nit v okviru mehanizma za skladnost.

(5) Če država članica določi, da mora telesa za certificiranje akreditirati nadzorni organ, mora ta opredeliti zahteve za akreditacijo, ki med drugim vključujejo zahteve iz člena 43(2). V primerjavi z obveznostmi za akreditacijo teles za certificiranje s strani nacionalnih akreditacijskih organov člen 43 daje manj navodil o zahtevah za akreditacijo, kadar nadzorni organ sam izvaja akreditacijo. Kot prispevek k harmoniziranemu pristopu k akreditaciji bi morala biti merila zanjo, ki jih uporablja nadzorni organ, urejena v ISO/IEC 17065 in bi jih bilo treba dopolniti z dodatnimi zahtevami, ki jih določi nadzorni organ v skladu s členom 43(1)(b). Odbor poudarja, da določbe v členu 43(2)(a) do (e) odražajo in natančneje določajo zahteve iz ISO 17065, kar bo prispevalo k dosledni uporabi.[2]

(6) Mnenje Odbora se sprejme v skladu s členom 64(1)(c), (3) in (8) Splošne uredbe o varstvu podatkov v povezavi s členom 10(2) poslovnika Odbora v osmih tednih od prvega delovnega dne po sprejetju odločitve predsednika in pristojnega nadzornega organa, da je dokumentacija popolna. Predsednik lahko odloči, da se to obdobje glede na kompleksnost vsebine podaljša za šest tednov –

**SPREJEL NASLEDNJE MNENJE:**

# 1 POVZETEK DEJSTEV

1. Luksemburški nadzorni organ je Odbor predložil osnutek zahtev za akreditacijo v skladu s členom 43(1)(a). Po sprejetju odločitve o popolnosti dokumentacije je bil predložen 25. oktobra 2019. Luksemburški nadzorni organ bo izvajal akreditacijo teles za certificiranje na podlagi meril za certificiranje iz Splošne uredbe o varstvu podatkov.
2. V skladu s členom 10(2) poslovnika Odbora je predsednica zaradi kompleksnosti obravnavane zadeve sprejela odločitev o podaljšanju prvotnega osemtedenskega obdobja za sprejetje za dodatnih šest tednov.

# 2 OCENA

## 2.1 Splošna obrazložitev Odbora glede predloženega osnutka zahtev za akreditacijo

Cilj tega mnenja je oceniti zahteve za akreditacijo, ki jih je pripravil nadzorni organ kot dodatek k ISO 17065 ali kot popoln sklop zahtev, da bo lahko nacionalni organ za akreditacijo ali nadzorni organ v skladu s členom 43(1) Splošne uredbe o varstvu podatkov akreditiral telo za certificiranje, pristojno za izdajanje in obnavljanje certifikatov v skladu s členom 42 Splošne uredbe o varstvu podatkov. To ne posega v naloge in pooblastila pristojnega nadzornega organa. V tem posebnem primeru Odbor

[2] Odstavek 39 smernic: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_sl.pdf.

ugotavlja, da nacionalna zakonodaja luksemburškemu nadzornemu organu nalaga nalogo izvajanja akreditacije teles za certificiranje. Luksemburški nadzorni organ je v ta namen pripravil sklop zahtev posebej za akreditacijo teles za certificiranje v povezavi s sklopom meril za certificiranje, ki jih je treba še formalno odobriti.

Cilj ocene zahtev za akreditacijo je proučiti spremembe (dodatke ali izbrise) iz smernic in predvsem iz Priloge. Poleg tega je mnenje Odbora osredotočeno tudi na vse vidike, ki bi lahko vplivali na skladen pristop glede akreditacije teles za certificiranje.

Opozoriti je treba, da je cilj smernic o akreditaciji teles za certificiranje pomagati nadzornim organom pri opredelitvi njihovih zahtev za akreditacijo. Priloga k smernicam ne pomeni zahtev za akreditacijo kot takih. Nadzorni organ mora zato zahteve za akreditacijo teles za certificiranje opredeliti tako, da omogoči njihovo praktično in dosledno uporabo, kot se zahteva v skladu z njegovimi okoliščinami.

Odbor je opravil oceno v skladu s strukturo iz Priloge 1 k smernicam. Če v mnenju določeni oddelek osnutka zahtev za akreditacijo, ki ga je predložil luksemburški nadzorni organ, ni obravnavan, je to treba razumeti, kot da Odbor nima pripomb in od luksemburškega nadzornega organa ne zahteva sprejetja dodatnih ukrepov. Odbor ugotavlja, da je luksemburški nadzorni organ predložil informacije za pomoč pri oceni osnutka zahtev za akreditacijo. V mnenju Odbora je obravnavan samo osnutek zahtev za akreditacijo.

V tem mnenju niso obravnavani elementi, ki jih je predložil luksemburški nadzorni organ in ki ne spadajo na področje uporabe člena 43(2) Splošne uredbe o varstvu podatkov, kot so sklicevanja na nacionalno zakonodajo. Ne glede na to pa Odbor poudarja, da mora biti nacionalna zakonodaja v skladu s Splošno uredbo o varstvu podatkov, kjer se to zahteva.

## 2.2 Glavne točke poudarka pri oceni (člen 43.2 Splošne uredbe o varstvu podatkov in Priloga 1 k smernicam Odbora) za zagotovitev dosledne ocene zahtev za akreditacijo:

a. obravnavanje vseh ključnih področij, kot so poudarjena v Prilogi k smernicam, in proučitev morebitnih odstopanj od Priloge;

b. neodvisnost telesa za certificiranje;

c. navzkrižje interesov telesa za certificiranje;

d. strokovno znanje telesa za certificiranje;

e. ustrezni zaščitni ukrepi za zagotovitev, da telo za certificiranje ustrezno uporablja merila za certificiranje iz Splošne uredbe o varstvu podatkov;

f. postopki za izdajo, redno pregledovanje in preklic certifikata iz Splošne uredbe o varstvu podatkov ter

g. pregledno obravnavanje pritožb zaradi kršitev certifikata.

3. Ob upoštevanju, da:

a. člen 43(2) Splošne uredbe o varstvu podatkov določa seznam področij akreditacije, ki jih mora telo za certificiranje obravnavati za pridobitev akreditacije;

b. člen 43(3) Splošne uredbe o varstvu podatkov določa, da zahteve za akreditacijo teles za certificiranje odobri pristojni nadzorni organ;

c. člen 57(1)(p) in (q) Splošne uredbe o varstvu podatkov določa, da mora pristojni nadzorni organ pripraviti osnutek zahtev za akreditacijo teles za certificiranje in take zahteve objaviti, pri čemer se lahko odloči, da sam izvaja akreditacijo teles za certificiranje;

d. člen 64(1)(c) Splošne uredbe o varstvu podatkov določa, da Odbor izda mnenje, kadar namerava nadzorni organ odobriti zahteve za akreditacijo telesa za certificiranje v skladu s členom 43(3);

Odbor izdaja naslednje mnenje:

### 2.2.1 SPLOŠNE OPOMBE

4. Odbor ugotavlja, da osnutek zahtev za akreditacijo ni popolnoma v skladu s strukturo iz Priloge 1 k smernicam. Manjkata na primer oddelka „področje uporabe“ ter „izrazi in opredelitve pojmov“. Odbor v zvezi s tem ugotavlja, da se v celotnem dokumentu nekateri izrazi, kot sta „stranka“ in „vložnik“, ne uporabljajo dosledno. Da bi preprečili zmedo, bi bilo treba uporabljene izraze uskladiti z opredelitvami pojmov iz smernic in Priloge, kjer je to mogoče, ter jih dosledno uporabljati. Da bi Odbor olajšal oceno, luksemburški nadzorni organ spodbuja, naj v osnutku zahtev za akreditacijo upošteva strukturo iz Priloge 1 (k smernicam) in doda manjkajoča oddelka.

5. Odbor ugotavlja, da je v celotnem dokumentu več sklicevanj na zahteve „tega mehanizma certificiranja“ (npr. zahteva 4.6.4) ali na telesa za certificiranje, ki se akreditirajo „v skladu z [...] mehanizmom certificiranja“ (npr. zahteva 2.2.2). Zdi se, da je sklicevanje na mehanizem certificiranja vprašanje oblikovanja. Odbor zato luksemburški nadzorni organ poziva, naj preoblikuje sklicevanja, da bi ta izražala, da se telesa za certificiranje akreditirajo v skladu z zahtevami, ki jih odobri nadzorni organ.

6. Podobno povzroča zmedo tudi sklicevanje na „zahteve iz tega mehanizma certificiranja“, ki se uporablja v celotnem dokumentu (npr. na zahtevo 1.1.1.2). Ustreznejše sklicevanje bi bila „merila iz mehanizma certificiranja“. Odbor zato luksemburški nadzorni organ spodbuja, naj v celotnem dokumentu pojasni vsa sklicevanja na „mehanizem certificiranja“.

7. Odbor ugotavlja, da se več zahtev (npr. 3.2.1.1 in 4.1.2) nanaša na „zadevne mednarodne standarde“, „zadevni standard“ ali „določeni standard“. Vendar taki standardi niso opredeljeni, zato ni jasno, na katere standarde se sklicevanja nanašajo. Odbor zato luksemburškemu nadzornemu organu priporoča, naj pojasni pomen takih standardov. To bi se lahko na primer pojasnilo v oddelku „področje uporabe“ ali „izrazi in opredelitve pojmov“.

### 2.2.2 SPLOŠNE ZAHTEVE ZA AKREDITACIJO

8. Odbor ugotavlja, da se zahteva 1.1.1.1 luksemburškega nadzornega organa nanaša na drug standard („ISAE 3000“), ki ga Odbor ni ocenil. Odbor zato luksemburškemu nadzornemu organu priporoča, naj pojasni, da zunanji standard, kot je ISAE 3000, ne more prevladati nad zahtevami.

9. Odbor ugotavlja, da zahteve iz točke 1.6 ne vključujejo obveznosti, da mora telo za certificiranje objaviti vse različice odobrenih meril in vse postopke za certificiranje ter javnosti omogočiti preprost dostop do njih v skladu s Prilogo k smernicam (oddelek 4.6). Odbor ugotavlja, da je luksemburški nadzorni organ lahko lastnik sistema certificiranja, vendar meni, da bi bilo koristno dodati ustrezno sklicevanje za zagotovitev posodobljenosti meril in njihove preproste dostopnosti prek samega telesa za certificiranje. Odbor v zvezi s tem meni, da luksemburški nadzorni organ z dajanjem informacij na voljo samo na zahtevo v skladu z zahtevo 1.6.1 določa strožjo zahtevo kot Priloga, ki

določa, da se informacije dajo na voljo javnosti v preprosto dostopni obliki. Odbor zato luksemburškemu nadzornemu organu priporoča, naj spremeni zahtevo, da bi ta vključevala obveznost, da mora telo za certificiranje javnosti omogočiti preprost dostop do vseh različic odobrenih meril in vseh postopkov za certificiranje v skladu s Prilogo k smernicam.

10. Odbor ugotavlja, da se zahteva 1.2.4 nanaša na „certificirani postopek“. Odbor meni, da bi bilo mogoče v skladu s smernicami uporabiti natančnejše besedilo, kot je „certificirana dejanja/dejavnosti obdelave“. To določa širše področje uporabe certificiranja v skladu s Splošno uredbo o varstvu podatkov. Odbor zato luksemburški nadzorni organ spodbuja, naj ustrezno spremeni osnutek zahtev.

### 2.2.3 ZAHTEVE GLEDE VIROV

11. Odbor ugotavlja, da se zdi zahteva 3.1.1.2 ponavljajoča in nejasna, pri čemer je ne podpira različna terminologija. Na primer, tretji odstavek se razume, da sodelujoči partner odločitev o ustreznosti sprejme samo na podlagi svoje presoje. Odbor luksemburškemu nadzornemu organu priporoča, naj z dosledno terminologijo jasneje in razumljiveje oblikuje zahtevo.

### 2.2.4 ZAHTEVE GLEDE POSTOPKA

12. Odbor ugotavlja, da je v zahtevi 4.2.1 navedenih več primerov potrebnih informacij. V skladu z oddelkom 7.2 Priloge 1 k smernicam pa bi morala biti že prva dva navedena primera sama po sebi zahteva. Odbor zato luksemburški nadzorni organ spodbuja, naj spremeni besedilo in zgoraj navedena primera vključi kot zahtevi.

13. Odbor glede oddelka 4.4 (Vrednotenje) v zvezi z zahtevami luksemburškega nadzornega organa za akreditacijo meni, da bi zahteve za akreditacijo morale vključevati obveznost, da mora telo za certificiranje zagotoviti, da se sprejmejo metode vrednotenja ter da so te metode vrednotenja, opisane v mehanizmu certificiranja, standardizirane in na splošno uporabne. S tem bi se zagotovilo, da se za primerljive cilje vrednotenja uporabljajo primerljive metode vrednotenja. Telo za certificiranje bi moralo vsako odstopanje od teh metod vrednotenja utemeljiti. Odbor zato luksemburškemu nadzornemu organu priporoča, naj spremeni osnutek, da bi ta vključeval zgoraj navedene obveznosti za telo za certificiranje.

14. Odbor nadalje ugotavlja, da zahteva 4.4.2 določa, da čeprav zunanje izvajanje ni dovoljeno, lahko organ za certificiranje za določena področja uporabi zunanje strokovnjake. V zvezi s tem je treba pojasniti, da bo telo za certificiranje še naprej odgovorno za odločanje, tudi kadar uporabi zunanje strokovnjake. Odbor zato luksemburškemu nadzornemu organu priporoča, naj besedilo zahteve 4.4.2 ustrezno spremeni.

15. Odbor ugotavlja, da oddelek 4.7 glede zahtev luksemburškega organa za akreditacijo („dokumentacija o certificiranju“) ne obravnava zahteve iz Priloge glede dokumentiranja obdobja nadzora (oddelek 7.9). Odbor zato luksemburški nadzorni organ spodbuja, naj vključi obdobje spremljanja v smislu oddelka 7.9 o nadzoru.

16. Zahteva 4.8.1 glede oddelka 4.8 („register certifciranih dejavnosti obdelave“) v zvezi z zahtevami luksemburškega nadzornega organa za akreditacijo določa, da se bodo informacije javnosti zagotovile „na zahtevo“. Odbor meni, da bi bila obveznost glede preglednosti iz oddelka 7.8 Priloge 1 bolje izpolnjena, če bi telo za certificiranje dajalo informacije na voljo proaktivno. Odbor zato luksemburškemu nadzornemu organu priporoča, naj spremeni osnutek in tako zagotovi, da bo telo za certificiranje javnosti dajalo na voljo informacije iz oddelka 7.8 Priloge 1 k smernicam.

17. Odbor ugotavlja, da oddelek 4.8 vključuje poglavje o nadzoru brez zahtev. Odbor luksemburškemu nadzornemu organu priporoča, naj pojasni, kako se bo izvajalo spremljanje.

18. Glede prekinitve, omejitve, začasnega odvzema ali preklica certifikata (oddelek 4.10) Odbor ugotavlja, da ni navedena obveznost telesa za certificiranje glede sprejetja odločitev in odredb pristojnega nadzornega organa o preklicu ali neizdaji certifikata stranki (vložniku), če zahteve glede certificiranja niso ali niso več izpolnjene. Ta obveznost je določena v členu 58(2)(h) Splošne uredbe o varstvu podatkov in oddelku 7.11 Priloge 1. Odbor zato luksemburškemu nadzornemu organu priporoča, naj zahteve za akreditacijo spremeni, pri čemer naj navede pravila, ki zajemajo preklic, prekinitev, omejitev ali začasni odvzem certifikata.

19. Odbor ugotavlja, da oddelek 9 Priloge, ki vsebuje splošna poglavja, ne vsebuje zahtev. Tukaj ni zajet na primer oddelek 9.3.4 o začasnem odvzemu ali preklicu akreditacije. To so pomembna poglavja, ki zagotavljajo sklicevanje na zadevne oddelke ali zahteve, ki se dodajo. Odbor luksemburški nadzorni organ spodbuja, naj pojasni, kje so zajete zahteve.

# 3 ZAKLJUČKI/PRIPOROČILA

20. Osnutek zahtev luksemburškega nadzornega organa za akreditacijo lahko vodi v nedosledno uporabo akreditacije teles za certificiranje, zato je treba uvesti naslednje spremembe:

21. Med splošnimi pripombami Odbor luksemburškemu nadzornemu organu priporoča, naj:

    1. pojasni pomen izraza „standard“ iz več zahtev (npr. 3.2.1.1 in 4.1.2). To bi se lahko na primer pojasnilo v oddelku „področje uporabe“ ali „izrazi in opredelitve pojmov“.

22. Glede „splošnih zahtev za akreditacijo“ Odbor luksemburškemu nadzornemu organu priporoča, naj:

    1. pojasni, da zunanji standard, kot je ISAE 3000, ne more prevladati nad zahtevami;

    2. spremeni zahteve iz točke 1.6 za vključitev obveznosti, da mora telo za certificiranje objaviti vse različice odobrenih meril in vse postopke za certificiranje ter javnosti omogočiti preprost dostop do njih v skladu s Prilogo k smernicam.

23. V zvezi z „zahtevami glede virov“ Odbor luksemburškemu nadzornemu organu priporoča, naj:

    1. z dosledno terminologijo preoblikuje zahtevo 3.1.1.2, da bo jasnejša in razumljivejša.

24. V zvezi z „zahtevami glede postopka“ Odbor luksemburškemu nadzornemu organu priporoča, naj:

    1. spremeni oddelek 4.4 osnutka glede zahtev z vključitvijo obveznosti telesa za certificiranje, da zagotavlja, da se sprejmejo metode vrednotenja ter da so te metode vrednotenja, opisane v mehanizmu certificiranja, standardizirane in splošno uporabne. Telo za certificiranje bi moralo utemeljiti vsako odstopanje od teh metod vrednotenja;

    2. spremeni besedilo zahteve 4.4.2, da se izrecno določi, da bo telo za certificiranje še naprej odgovorno za odločanje, tudi kadar uporabi zunanje strokovnjake;

    3. spremeni oddelek 4.8 osnutka svojih zahtev za akreditacijo in tako zagotovi, da bo telo za certificiranje javnosti dajalo na voljo informacije iz oddelka 7.8 Priloge 1 k smernicam;

4. v oddelku 4.8 pojasni, kako se bo izvajalo spremljanje;

5. spremeni pododdelek 4.10 za določitev pravil, ki vključujejo preklic, prekinitev, omejitev ali začasni odvzem certifikata.

# 4 KONČNE PRIPOMBE

25. To mnenje je naslovljeno na luksemburški nadzorni organ in bo objavljeno v skladu s členom 64(5b) Splošne uredbe o varstvu podatkov.

26. Nadzorni organ v skladu s členom 64(7) in (8) Splošne uredbe o varstvu podatkov v dveh tednih po prejemu mnenja z elektronskimi sredstvi predsednico Odbora obvesti, ali bo svoj osnutek seznama spremenil ali ohranil. V istem obdobju pošlje spremenjeni osnutek seznama, če ne namerava v celoti ali deloma upoštevati mnenja Odbora, pa ustrezno utemelji, zakaj ne namerava upoštevati tega mnenja.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)