Mnenje odbora (člen 64)

Mnenje št. 38/2023 o osnutku sklepa pristojnega nadzornega organa Slovenije glede odobritve zahtev za akreditacijo telesa za certificiranje v skladu s tretjim odstavkom 43. člena Splošne uredbe o varstvu podatkov

Sprejeto 21. decembra 2023

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju 63. člena, točke c prvega odstavka 64. člena, tretjega do osmega odstavka 64. člena in tretjega odstavka 43. člena 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 nadaljevanju: Splošna uredba o varstvu podatkov),

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

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

ob upoštevanju naslednjega:

(1) Glavna vloga Evropskega odbora za varstvo podatkov je zagotavljati dosledno uporabo Splošne uredbe o varstvu podatkov) v celotnem Evropskem gospodarskem prostoru. V skladu s prvim odstavkom 64. člena Splošne uredbe o varstvu podatkov odbor izda mnenje, kadar namerava nadzorni organ odobriti zahteve za akreditacijo telesa za certificiranje v skladu s 43. členom. 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. Evropski odbor za varstvo podatkov 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 43. členom Splošne uredbe o varstvu podatkov pristojni nadzorni organi sprejmejo akreditacijske zahteve. Pri tem uporabljajo 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 uživajo polje proste presoje glede nacionalnih ali regionalnih okoliščin, pri čemer morajo upoštevati svojo lokalno zakonodajo. Cilj mnenja Evropskega odbora za varstvo podatkov 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.

(4) „Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi člena 43 Splošne uredbe o varstvu podatkov (2016/679)“ (v nadaljevanju: 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 akreditacijske zahteve, ki med drugim vključujejo zahteve iz drugega odstavka 43. člena Splošne uredbe o varstvu podatkov. V primerjavi z obveznostmi za akreditacijo teles za

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

certificiranje pri nacionalnih akreditacijskih organih 43. člen daje manj navodil o zahtevah za akreditacijo, kadar nadzorni organ sam izvaja akreditacijo. Kot prispevek k usklajenemu pristopu k akreditaciji bi morale akreditacijske zahteve, ki jih uporablja nadzorni organ, temeljiti na standardu ISO/IEC 17065, dopolniti pa bi jih bilo treba z dodatnimi zahtevami, ki jih določi nadzorni organ v skladu s točko b prvega odstavka 43. člena. Odbor poudarja, da določbe v točkah a do e drugega odstavka 43. člena odražajo in določajo zahteve iz standarda ISO 17065, kar bo pripomoglo k dosledni uporabi.[2]

(6) V skladu s točko c prvega odstavka 64. člena in tretjim do osmim odstavkom istega člena Splošne uredbe o varstvu podatkov v povezavi z drugim odstavkom 10. člena poslovnika Evropski odbor za varstvo podatkov sprejme mnenje v osmih tednih od prvega delovnega dne po sprejetju sklepa predsednika in pristojnega nadzornega organa, da je dokumentacija popolna. Predsednica lahko odloči, da se to obdobje lahko glede na kompleksnost vsebine podaljša za šest tednov –

SPREJEL NASLEDNJE MNENJE:

1 POVZETEK DEJSTEV

1. Slovenski nadzorni organ je Evropskemu odboru za varstvo podatkov predložil osnutek zahtev za akreditacijo v skladu s točko b prvega odstavka 43. člena. Dokumentacija je bila 26. oktobra 2023 ocenjena kot popolna. Slovenski nacionalni akreditacijski organ bo telesa za certificiranje akreditiral na podlagi meril za certificiranje iz Splošne uredbe o varstvu podatkov. To pomeni, da bo nacionalni akreditacijski organ za akreditacijo teles za certificiranje uporabil standard ISO 17065 in dodatne zahteve, ki jih je določil slovenski nadzorni organ, in sicer potem, ko bo slovenski nadzorni organ te zahteve odobril na podlagi mnenja Evropskega odbora za varstvo podatkov o osnutku zahtev.

2 OCENA

2.1 Splošna obrazložitev Evropskega odbora za varstvo podatkov glede predloženega osnutka sklepa

2. Namen tega mnenja je oceniti akreditacijske zahteve, ki jih je določil nadzorni organ, bodisi v zvezi s standardom ISO 17065 bodisi celotnim sklopom zahtev, da se nacionalnemu akreditacijskemu organu ali nadzornemu organu, kot določa prvi odstavek 43. člena Splošne uredbe o varstvu podatkov, omogoči akreditacija telesa za certificiranje, odgovornega za izdajo in podaljšanje certifikata v skladu z 42. členom Splošne uredbe o varstvu podatkov. To ne posega v naloge in pooblastila pristojnega nadzornega organa. V tem primeru Evropski odbor za varstvo podatkov ugotavlja, da se je slovenski nadzorni organ odločil, da se za izdajo akreditacije obrne na nacionalni akreditacijski organ, saj je v skladu s smernicami pripravil dodatne zahteve, ki jih mora nacionalni akreditacijski organ uporabiti pri izdaji akreditacije.

[2] Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi člena 43 Splošne uredbe o varstvu podatkov, točka 39. Na voljo na spletnem naslovu: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

3. Namen te ocene dodatnih zahtev slovenskega nadzornega organa za akreditacijo je proučiti spremembe (dopolnitve ali črtanja) smernic in zlasti njihove Priloge 1. Poleg tega je mnenje Evropskega odbora za varstvo podatkov osredotočeno tudi na vse vidike, ki lahko vplivajo na dosleden pristop v zvezi z akreditacijo teles za certificiranje.

4. 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.

5. Evropski odbor za varstvo podatkov priznava dejstvo, da bi bilo treba nacionalnim akreditacijskim organom glede na njihovo strokovno znanje zagotoviti manevrski prostor pri opredelitvi nekaterih posebnih določb v okviru veljavnih akreditacijskih zahtev. Vendar pa je treba po mnenju odbora poudariti, da je treba v primeru določitve dodatnih zahtev te opredeliti na način, ki omogoča njihovo praktično in dosledno uporabo ter pregled, če je to potrebno.

6. Evropski odbor za varstvo podatkov ugotavlja, da standardi ISO, zlasti standard ISO 17065, ščitijo pravice intelektualne lastnine, zato se v tem mnenju ne bo skliceval na besedilo zadevnega dokumenta. Posledično se je odločil, da po potrebi vključi napotila na določene oddelke standarda ISO, ne da bi pri tem navajal njegovo dejansko besedilo.

7. Nazadnje je Evropski odbor za varstvo podatkov izvedel svojo oceno v skladu s strukturo, predvideno v Prilogi 1 k smernicam (v nadaljevanju: Priloga). Če posamezen oddelek osnutka zahtev slovenskega nadzornega organa za akreditacijo v tem mnenju ni omenjen, se šteje, da odbor nima nobenih pripomb in ne zahteva, da slovenski nadzorni organ sprejme nadaljnje ukrepe.

8. V tem mnenju niso zajeti elementi, ki jih je posredoval slovenski nadzorni organ in ne spadajo na področje uporabe drugega odstavka 43. člena Splošne uredbe o varstvu podatkov, kot so na primer sklici na nacionalno zakonodajo. Ne glede na to pa Evropski odbor za varstvo podatkov ugotavlja, da mora biti nacionalna zakonodaja skladna s Splošno uredbo o varstvu podatkov, kadar se to zahteva.

2.2 Glavne točke poudarka pri oceni (drugi odstavek 43. člena Splošne uredbe o varstvu podatkov in Priloga 1 k smernicam Evropskega odbora za varstvo podatkov), da zahteve za akreditacijo dosledno ocenjujejo naslednje:

a. obravnavo vseh ključnih področij, kot je poudarjeno v prilogi k smernicam, in upoštevanje vseh odstopanj od Priloge;

b. neodvisnost telesa za certificiranje;

c. nasprotja interesov telesa za certificiranje;

d. strokovno znanje telesa za certificiranje;

e. ustrezne zaščitne ukrepe za zagotovitev, da telesa za certificiranje ustrezno uporabijo merila za certificiranje iz Splošne uredbe o varstvu podatkov;

f. postopke za izdajo, redni pregled in preklic certificiranja v skladu s Splošno uredbo o varstvu podatkov in

g. pregledno obravnavo pritožb zaradi kršitev, povezanih s certificiranjem.

9. Ob upoštevanju, da:

   a. drugi odstavek 43. člena Splošne uredbe o varstvu podatkov določa seznam področij akreditacije, ki jih mora telo za certificiranje obravnavati, če želi pridobiti akreditacijo;

   b. tretji odstavek 43. člena Splošne uredbe o varstvu podatkov določa, da zahteve za akreditacijo teles za certificiranje odobri pristojni nadzorni organ;

   c. točki p in q prvega odstavka 57. člena Splošne uredbe o varstvu podatkov določa, da mora pristojni nadzorni organ pripraviti osnutek zahtev in objaviti zahteve za akreditacijo teles za certificiranje ter da se lahko odloči, da bo sam izvedel postopek akreditacije teles za certificiranje;

   d. točka c prvega odstavka 64. člena Splošne uredbe o varstvu podatkov določa, da Evropski odbor za varstvo podatkov izda mnenje, kadar namerava nadzorni organ odobriti zahteve za akreditacijo teles za certificiranje v skladu s tretjim odstavkom 43. člena;

   e. če postopek akreditacije izvaja nacionalni akreditacijski organ v skladu s standardom ISO/IEC 17065/2012, je treba uporabiti tudi dodatne zahteve, ki jih določi pristojni nadzorni organ;

   f. so v Prilogi 1 k smernicam o akreditaciji teles za certificiranje predlagane zahteve, katerih osnutek pripravi nadzorni organ za varstvo podatkov in ki se uporabljajo pri akreditaciji telesa za certificiranje pri nacionalnem akreditacijskem organu,

Evropski odbor za varstvo podatkov podaja naslednje mnenje:

2.2.1 UVOD

10. Evropski odbor za varstvo podatkov priznava dejstvo, da pogoji sodelovanja, ki urejajo razmerje med nacionalnim akreditacijskim organom in njegovim nadzornim organom za varstvo podatkov, sami po sebi niso zahteva za akreditacijo teles za certificiranje. Vendar zaradi popolnosti in preglednosti meni, da je treba tovrstne pogoje sodelovanja, če obstajajo, javno objaviti v obliki, ki je po mnenju nadzornega organa primerna.

2.2.2 SPLOŠNE OPOMBE

11. Evropski odbor za varstvo podatkov ugotavlja, da slovenski nadzorni organ v osnutku zahtev za akreditacijo v oddelku „izrazi in opredelitve pojmov“, navaja, da so ti izrazi in opredelitve pojmov iz Splošne uredbe o varstvu podatkov in smernic Evropskega odbora za varstvo podatkov št. 1/2018. Vendar nekatere opredelitve pojmov, na primer tista o akreditaciji, ne ustrezajo opredelitvam iz smernic odbora. Zato Evropski odbor za varstvo podatkov poziva slovenski nadzorni organ, naj zagotovi, da se izrazi, opredeljeni v smernicah, dosledno upoštevajo v zahtevah za akreditacijo.

2.2.3 SPLOŠNE ZAHTEVE ZA AKREDITACIJO

12. V zvezi z zahtevo glede pravne odgovornosti (pododdelek 4.1.1) je Evropski odbor za varstvo podatkov seznanjen z dejstvom, da slovenski nadzorni organ zahteva, da mora biti telo za certificiranje „sposobno dokazati skladnost s Splošno uredbo o varstvu podatkov in Zakonom o varstvu osebnih podatkov“. Za zagotovitev ustrezne ocene in izvajanja te zahteve Evropski odbor za varstvo podatkov

slovenskemu nadzornemu organu priporoča, naj besedilo „mora biti sposoben dokazati“ nadomesti z „dokaže“.

13. V zvezi z oddelkom 4.2 osnutka akreditacijskih zahtev, ki jih je pripravil slovenski nadzorni organ, o „upravljanju nepristranskosti“ Evropski odbor za varstvo podatkov potrjuje, da je slovenski nadzorni organ vključil zahtevo za preprečevanje nasprotja interesov. Kljub temu odbor slovenski nadzorni organ poziva, naj v zahteve za akreditacijo vključi tudi pravila za obvladovanje nasprotij interesov, kadar so taka nasprotja ugotovljena.

2.2.4 ZAHTEVE GLEDE VIROV

14. Evropski odbor za varstvo podatkov na splošno meni, da bi bilo treba zahteve po strokovnem znanju za ocenjevalce in odločevalce prilagoditi ob upoštevanju različnih nalog, ki jih opravljajo. V zvezi s tem meni, da bi morali imeti ocenjevalci specialistično strokovno znanje in strokovne izkušnje na področju tehničnih postopkov (na primer revizije in certificiranja), odločevalci pa bi morali imeti splošnejše in celovitejše strokovno znanje ter delovne izkušnje s področja varstva podatkov. Ob upoštevanju zgoraj navedenega Evropski odbor za varstvo podatkov slovenskemu nadzornemu organu svetuje, naj ta pododdelek preoblikuje ob upoštevanju različnih vsebinskih zahtev glede znanja in/ali izkušenj za ocenjevalce in odločevalce in ne let izkušenj.

15. V zvezi z oddelkom 6.1 osnutka akreditacijskih zahtev, ki jih je pripravil slovenski nadzorni organ, Evropski odbor za varstvo podatkov ugotavlja, da za osebje s tehničnim strokovnim znanjem manjka navedba, da mora biti kvalifikacija povezana z ustreznim reguliranim poklicem v skladu s smernicami. Zato odbor slovenski nadzorni organ poziva, naj to zahtevo ustrezno spremeni in jo uskladi s smernicami.

16. Podobno se Evropski odbor za varstvo podatkov v istem oddelku seznanja z obvestili odbora, da slovenski nadzorni organ za izkušnje osebja s tehničnim in pravnim strokovnim znanjem omenja „celovite“ strokovne izkušnje namesto „pomembne“ strokovne izkušnje, kot je to v skladu s smernicami. Odbor poziva slovenski nadzorni organ, naj te zahteve spremeni tako, da bodo skladne s smernicami.

17. Evropski odbor za varstvo podatkov je seznanjen z vsemi pogoji, ki jih mora izpolnjevati osebje s pravnim strokovnim znanjem. Vendar pa slovenski nadzorni organ ne navaja, da mora študij prava na slovenski ali tuji univerzi trajati „najmanj osem semestrov, vključno z akademskim nazivom magister (LLM)“. Odbor slovenskemu nadzornemu organu priporoča, da to zahtevo vključi v svoje akreditacijske zahteve v skladu s smernicami.

2.2.5 ZAHTEVE GLEDE POSTOPKOV

18. Slovenski nadzorni organ se v zvezi z oddelkom 7.3 o pregledu vloge sklicuje na oddelek 7.3.1(e) standarda ISO 17065. Vendar je v smernicah naveden oddelek 7.3(3). Evropski odbor za varstvo podatkov poziva slovenski nadzorni organ, naj te zahteve spremeni tako, da bodo skladne s smernicami.

19. V zvezi z oddelkom 7.11 osnutka akreditacijskih zahtev, ki jih je pripravil slovenski nadzorni organ, Evropski odbor za varstvo podatkov ugotavlja, da se slovenski nadzorni organ sklicuje na neskladnost s certificiranjem v primeru „pomembnih kršitev varstva podatkov“, ki se nanašajo na področje uporabe

certificiranja in cilj vrednotenja. Odbor s to zahtevo razume, da je treba v primeru pomembne kršitve varstva podatkov, povezane s področjem uporabe certificiranja in ciljem vrednotenja, ki po svoji naravi kaže na to, da stranka ni sprejela ustreznih ukrepov, kot je bilo pričakovano v skladu z njenim certificiranjem, v smislu, da če bi bile ustrezne zahteve za certificiranje dejansko pravilno izvedene, do take kršitve varstva podatkov ne bi prišlo, to obravnavati kot neskladnost s certificiranjem, certifikacijski organ pa mora sprejeti ustrezne ukrepe. Odbor poziva slovenski nadzorni organ, naj pojasni svojo zahtevo za akreditacijo.

2.2.6 ZAHTEVE ZA SISTEM UPRAVLJANJA

20. V oddelku 8 osnutka akreditacijskih zahtev, ki jih je pripravil slovenski nadzorni organ, v zvezi z „zahtevami za sistem upravljanja“ manjka navedba, da mora razkritje izvesti „akreditirani certifikacijski organ v skladu z 58. členom Splošne uredbe o varstvu podatkov“. Evropski odbor za varstvo podatkov poziva slovenski nadzorni organ, naj to zahtevo ustrezno spremeni in jo uskladi s smernicami.

3 SKLEPNE UGOTOVITVE/PRIPOROČILA

21. Osnutek akreditacijskih zahtev, ki jih je pripravil slovenski nadzorni organ, lahko vodi v nedosledno uporabo akreditacije teles za certificiranje, zato je treba uvesti naslednje spremembe:

22. Glede „splošnih zahtev za akreditacijo“ Evropski odbor za varstvo podatkov slovenskemu nadzornemu organu priporoča, naj:

    1) v oddelku 4.1.1 nadomesti sklicevanje na to, da mora biti telo za certificiranje sposobno dokazati skladnost s Splošno uredbo o varstvu podatkov in Zakonom o varstvu osebnih podatkih, s sklicevanjem na to, da mora telo za certificiranje skladnost dokazati in ne le biti sposobno to storiti.

23. V zvezi z „zahtevami glede virov“ Evropski odbor za varstvo podatkov slovenskemu nadzornemu organu priporoča, naj:

    1) doda zahtevo, da mora študij prava na slovenski ali tuji univerzi trajati „najmanj osem semestrov, vključno z akademskim nazivom magister (LLM)“, da se ta zahteva uskladi s smernicami.

4 KONČNE PRIPOMBE

24. To mnenje je namenjeno slovenskemu nadzornemu organu in bo v skladu s točko b petega odstavka 64. člena Splošne uredbe o varstvu podatkov na voljo javnosti.

25. V skladu s sedmim in z osmim odstavkom 64. člena Splošne uredbe o varstvu podatkov slovenski nadzorni organ svojo odločitev o spremembi oziroma ohranitvi svojega osnutka seznama sporoči predsednici po elektronski poti v dveh tednih po prejemu mnenja. V istem obdobju pošlje spremenjeni osnutek seznama, če ne namerava v celoti ali deloma upoštevati mnenja Evropskega odbora za varstvo podatkov, pa ustrezno utemelji, zakaj ga ne namerava upoštevati.

26. Slovenski nadzorni organ bo v skladu s točko y prvega odstavka 70. člena Splošne uredbe o varstvu podatkov svojo končno odločitev sporočil Evropskemu odboru za varstvo podatkov za vključitev v register odločitev glede vprašanj, obravnavanih v okviru mehanizma za skladnost.

Za Evropski odbor za varstvo podatkov

Predsednica

(Anu Talus)

Sprejeto