Mnenje odbora (člen 64)

Mnenje št. 14/2020 o osnutku sklepa pristojnega nadzornega organa Irske glede odobritve zahtev za akreditacijo telesa za certificiranje v skladu s členom 43.3 (Splošne uredbe o varstvu podatkov)

Sprejeto 25. maja 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 nadaljevanju: Splošna uredba o varstvu podatkov),

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 za varstvo podatkov (v nadaljevanju: odbor) je zagotavljati dosledno uporabo Uredbe (EU) 2016/679 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 ta cilj prizadeva doseči, prvič, s spodbujanjem nadzornih organov, naj pripravijo osnutek svojih zahtev za akreditacijo ob upoštevanju strukture iz Priloge 1 k smernicam odbora št. 4/2018 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 morajo 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.

4) „Smernice št. 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 zahteve za akreditacijo, ki med drugim vključujejo zahteve iz člena 43(2) Splošne uredbe o varstvu podatkov. V primerjavi z obveznostmi za akreditacijo teles za certificiranje pri nacionalnih akreditacijskih organih člen 43 Splošne uredbe o varstvu podatkov daje manj navodil o zahtevah za

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

akreditacijo, kadar nadzorni organ sam izvaja akreditacijo. Kot prispevek k usklajenemu pristopu k akreditaciji bi morala biti merila zanjo, ki jih uporablja nadzorni organ, urejena s standardom ISO/IEC 17065 in bi jih bilo treba dopolniti z dodatnimi zahtevami, ki jih določi nadzorni organ v skladu s členom 43(1)(b) Splošne uredbe o varstvu podatkov. Odbor poudarja, da določbe v členu 43(2)(a)–(e) Splošne uredbe o varstvu podatkov odražajo in določajo zahteve iz standarda ISO 17065, kar bo pripomoglo k dosledni uporabi.[2]

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

SPREJEL MNENJE:

1 POVZETEK DEJSTEV

1. Irski nadzorni organ je odboru predložil osnutek zahtev za akreditacijo v skladu s členom 43(1)(b). Dokumentacija je bila 13. februarja 2020 ocenjena kot popolna. Irski 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 irski nadzorni organ, in sicer po tem, ko bo irski nadzorni organ te zahteve odobril na podlagi mnenja odbora o osnutku zahtev.

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 sklepa

3. Namen tega mnenja je oceniti zahteve za akreditacijo, 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 člen 43(1) Splošne uredbe o varstvu podatkov, omogoči akreditacija telesa za certificiranje, odgovornega za izdajo in podaljšanje certifikata v skladu s členom 42 Splošne uredbe o varstvu podatkov. To ne posega v naloge in pristojnosti pristojnega nadzornega organa. V tem primeru odbor ugotavlja, da se je irski 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/smjernice/guidelines-42018-accreditation-certification-bodies-under_sl

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

5. 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.

6. Odbor 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 zahtev za akreditacijo. 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.

7. Odbor ugotavlja, da standarde ISO, zlasti standard ISO 17065, ščitijo pravice intelektualne lastnine, zato se v tem mnenju ne bo skliceval na besedilo zadevnega dokumenta. Zato se je odbor odločil, da po potrebi vključi napotila na posamezne oddelke standarda ISO, ne da bi pri tem navajal dejansko besedilo standarda.

8. Nazadnje je odbor izvedel svojo oceno v skladu z zgradbo, predvideno v Prilogi 1 k smernicam (v nadaljevanju: Priloga). Če posamezen oddelek osnutka zahtev irskega nadzornega organa za akreditacijo v tem mnenju ni omenjen, se šteje, da odbor nima nobenih pripomb in ne zahteva, da irski nadzorni organ sprejme nadaljnje ukrepe.

9. V tem mnenju niso zajeti elementi, ki jih je posredoval irski nadzorni organ in ne spadajo na področje uporabe člena 43(2) Splošne uredbe o varstvu podatkov, kot so na primer sklici na nacionalno zakonodajo. Ne glede na to pa odbor poudarja, da mora biti nacionalna zakonodaja v skladu s Splošno uredbo o varstvu podatkov, kadar se to zahteva.

2.2 Glavne točke za oceno (člen 43(2) Splošne uredbe o varstvu podatkov in Priloga 1 k smernicam odbora), da zahteve za akreditacijo dosledno ocenjujejo naslednje:

1) obravnavo vseh ključnih področij, kot je poudarjeno v prilogi k smernicam, in upoštevanje vseh odstopanj od priloge;

2) neodvisnost telesa za certificiranje;

3) navzkrižja interesov telesa za certificiranje;

4) strokovno znanje telesa za certificiranje;

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

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

7) pregledno obravnavo pritožb zaradi kršitev, povezanih s certificiranjem.

10. Ob upoštevanju, da:

a. člen 43(2) Splošne uredbe o varstvu podatkov določa seznam področij akreditacij, ki jih mora telo za certificiranje obravnavati, če želi pridobiti akreditacijo;

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 in objaviti zahteve za akreditacijo za telesa za certificiranje ter da se lahko odloči, da sam izvede postopek akreditacije teles za certificiranje;

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

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,

odbor podaja naslednje mnenje:

2.2.1 OZNAKA (Oddelek 0 osnutka zahtev irskega nadzornega organa za akreditacijo)

11. Odbor 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 odbor zaradi popolnosti in preglednosti meni, da je treba take pogoje sodelovanja, če obstajajo, javno objaviti v obliki, ki je po mnenju nadzornega organa primerna.

2.2.2 IZRAZI IN OPREDELITVE POJMOV

12. Odbor ugotavlja, da sklicevanje na smernice o akreditaciji kot „WP 261“ ni posodobljeno. Odbor je sprejel Smernice št. 4/2018 o akreditaciji teles za certificiranje na podlagi člena 43 Splošne uredbe o varstvu podatkov (2016/679). Odbor irski nadzorni organ zato spodbuja, naj spremeni besedilo in se sklicuje na Smernice št. 4/2018.

2.2.3 SPLOŠNE OPOMBE

13. Odbor ugotavlja, da se osnutek smernic irskega nadzornega organa nenehno sklicuje na „pristojni nadzorni organ“. Ker je pristojni nadzorni organ v tem primeru irski nadzorni organ, odbor irskemu nadzornemu organu priporoča, naj ta sklic zamenja s „Komisijo za varstvo podatkov“ ali „irskim nadzornim organom“, da se prepreči zmeda.

14. Odbor priznava, da osnutek zahtev irskega nadzornega organa vključuje oddelek o izrazih in opredelitvi pojmov. Vendar se nekateri izrazi ne uporabljajo dosledno v celotnem dokumentu (na primer „predmet ocene“ in „cilj ocene“). Za preprečitev zmede odbor irski nadzorni organ poziva, naj v osnutku zahtev uporablja dosledno izrazje.

2.2.4 SPLOŠNE ZAHTEVE ZA AKREDITACIJO (oddelek 4 osnutka zahtev za akreditacijo)

15. V zvezi z določbo 7 pododdelka 4.1.2 osnutka zahtev za akreditacijo irskega nadzornega organa odbor meni, da je besedilo nekoliko nejasno glede tega, komu se navedejo razlogi za odobritev certifikacije. Tudi sklicevanje na „omogočanje“ registra je nejasno. Odbor zato irski nadzorni organ poziva, naj besedilo preoblikuje tako, da bo jasnejše.

2.2.5 STRUKTURNE ZAHTEVE (oddelek 5 osnutka zahtev za akreditacijo)

16. Odbor ugotavlja, da se osnutek zahtev irskega nadzornega organa za akreditacijo sklicuje na imenovanje „oseb z ustrezno delovno dobo, ki so odgovorne za nadzor nad skladnostjo z zahtevami varstva podatkov in upravljanjem informacij“. Sklicevanje na ustrezno delovno dobo bi bilo treba pojasniti v smislu izkušenj in obsega pooblastil. Hkrati se funkcije te osebe zdijo podobne funkcijam pooblaščene osebe za varstvo podatkov. Odbor irskemu nadzornemu organu svetuje, naj jasno določi funkcije te osebe in opredeli ustrezne izkušnje.

2.2.6 ZAHTEVE GLEDE VIROV (oddelek 6 osnutka zahtev za akreditacijo)

17. Glede osebja telesa za certificiranje (pododdelek 6.1) organ ugotavlja, da zahteve za osebje s tehničnim strokovnim znanjem, odgovorno za sprejemanje odločitev, vključujejo vsaj pet let delovnih izkušenj v zvezi s predmetom certifikacije, osebje, odgovorno za ocene, pa bi moralo imeti vsaj dve leti delovnih izkušenj. Podobno mora osebje s pravnim strokovnim znanjem, ki sprejema odločitve, imeti vsaj pet let delovnih izkušenj, osebje, odgovorno za ocene, pa mora imeti vsaj dve leti izkušenj. Odbor ugotavlja, da se zahtevano najmanjše število let delovnih izkušenj med osebjem, odgovornim za odločanje, in osebjem, odgovornim za ocene, močno razlikuje. Glede tega odbor meni, da bi poudarek moral biti na različnih vrstah strokovnega znanja in ne na številu let delovnih izkušenj. Po mnenju odbora bi morali ocenjevalci imeti specialistično strokovno znanje in delovne izkušnje s tehničnimi postopki (na primer revizije in certifikacije), nosilci odločanja pa bi morali imeti splošnejše in celovitejše strokovno znanje ter delovne izkušnje z varstvom podatkov. Ob upoštevanju zgoraj navedenega odbor irskemu nadzornemu organu svetuje, naj nameni večji poudarek različnemu vsebinskemu znanju in/ali izkušnjam za ocenjevalce in nosilce odločanja ter zmanjša razlike v zahtevanih letih izkušenj zanje.

2.2.7 ZAHTEVE GLEDE POSTOPKA (oddelek 7 osnutka zahtev za akreditacijo)

18. Glede pododdelka 7.10 osnutka zahtev irskega organa za akreditacijo („Spremembe, ki vplivajo na akreditacijo“), odbor ugotavlja, da niso navedeni postopki o spremembah, o katerih se je treba dogovoriti, v skladu z oddelkom 7.10 Priloge. Odbor irski nadzorni organ poziva, naj vključi tako navedbo in naj navede nekatere od postopkov, ki jih je mogoče uvesti (na primer prehodna obdobja, postopek odobritve s pristojnim nadzornim organom). Hkrati odbor meni, da so ustrezne tudi tehnične spremembe in bi lahko vplivale na certificiranje. Odbor zato irskemu nadzornemu organu svetuje, naj vključi to možnost na seznam sprememb, ki vplivajo na certificiranje. Nazadnje odbor pozdravlja vključitev kršitev varstva osebnih podatkov iz Splošne uredbe o varstvu podatkov na seznam

sprememb, ki lahko vplivajo na certificiranje. Vendar pa odbor zaradi zagotovitve jasnosti irskemu nadzornemu organu svetuje, naj navede, da bodo kršitve iz Splošne uredbe o varstvu podatkov upoštevane le toliko, kolikor se nanašajo na certificiranje.

19. Glede sprememb, ki vplivajo na certificiranje (pododdelek 7.10 osnutka zahtev irskega nadzornega organa), in zlasti pete alinee odbor ugotavlja, da se irski nadzorni organ sklicuje na „zavezujoče sklepe Evropskega odbora za varstvo podatkov, ki veljajo“, ter na člen 39 poslovnika odbora, ki vključuje „vse končne dokumente, ki jih je sprejel odbor“. Vendar pa za zagotovitev jasnega razumevanja, kaj pomenijo „sklepi Evropskega odbora za varstvo podatkov“, odbor irski nadzorni organ poziva, naj sklicevanje pojasni. Besedilo bi se lahko na primer glasilo: „dokumenti, ki jih sprejme Evropski odbor za varstvo podatkov“.

20. Odbor ugotavlja, da pododdelek 7.11 osnutka zahtev irskega nadzornega organa (prekinitev, omejitev, začasen odvzem ali preklic certifikata) ne določa obveznosti telesa za certificiranje glede sprejetja odločitev in odredb irskega nadzornega organa o preklicu ali neizdaji certifikata prijavitelju, če zahteve glede certificiranja niso ali niso več izpolnjene. Zato odbor irskemu nadzornemu organu priporoča, naj vključi tako obveznost.

3 SKLEPNE UGOTOVITVE/PRIPOROČILA

21. Osnutek zahtev irskega nadzornega organa za akreditacijo lahko vodi v nedosledno uporabo akreditacije teles za certificiranje, zato je treba spremeniti naslednje:

22. Glede „zahtev glede postopkov“ odbor irskemu nadzornemu organu priporoča, naj:

1) v pododdelek 7.11 vključi obveznost telesa za certificiranje glede sprejetja odločitev in odredb irskega nadzornega organa o preklicu ali neizdaji certifikata prijavitelju, če zahteve glede certificiranja niso ali niso več izpolnjene.

4 KONČNE PRIPOMBE

23. To mnenje je namenjeno irskemu nadzornemu organu in bo v skladu s členom 64(5)(b) Splošne uredbe o varstvu podatkov na voljo javnosti.

24. V skladu s členom 64(7) in (8) Splošne uredbe o varstvu podatkov irski nadzorni organ svojo odločitev o spremembi oziroma ohranitvi svojega osnutka seznama sporoči predsedniku 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 odbora, pa ustrezno utemelji, zakaj tega mnenja ne namerava upoštevati.

25. Irski nadzorni organ bo v skladu s členom 70(1)(y) Splošne uredbe o varstvu podatkov svojo končno odločitev sporočil odboru za vključitev v register odločitev glede vprašanj, obravnavanih v okviru mehanizma za skladnost.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

Sprejeto