Mišljenje 14/2020 o nacrtu odluke irskog nadležnog nadzornog tijela o odobravanju zahtjeva za akreditaciju certifikacijskog tijela u skladu s člankom 43. stavkom 3. Opće uredbe o zaštiti podataka

Usvojeno 25. svibnja 2020.

Sadržaj

uzimajući u obzir članak 63., članak 64. stavak 1. točku (c) te stavke od 3. do 8. i članak 43. stavak 3. Uredbe 2016/679/EU Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „Opća uredba”),

uzimajući u obzir Sporazum o EGP-u, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.,1

uzimajući u obzir članak 10. i članak 22. svojeg Poslovnika od 25. svibnja 2018.,

budući da:

1. Glavna je uloga Odbora osigurati dosljednu primjenu Uredbe 2016/679 (dalje u tekstu „Opća uredba”) u čitavom Europskom gospodarskom prostoru. U skladu s člankom 64. stavkom 1. Opće uredbe, Odbor daje mišljenje kada nadzorno tijelo namjerava odobriti zahtjeve za akreditaciju certifikacijskih tijela u skladu s člankom 43. Cilj je ovog mišljenja stvoriti usklađeni pristup u pogledu zahtjeva koje će nadzorno tijelo za zaštitu osobnih podataka ili nacionalno akreditacijsko tijelo primijeniti prilikom akreditacije certifikacijskog tijela. Iako ne propisuje jedinstven skup zahtjeva za akreditaciju, Opća uredba promiče dosljednost. Odbor u svojim mišljenjima nastoji postići ovaj cilj, kao prvo potičući nadzorna tijela da sastave svoje zahtjeve za akreditaciju slijedeći strukturu iz Priloga 1. Smjernicama 4/2018 Europskog odbora za zaštitu podataka o akreditaciji certifikacijskih tijela, a kao drugo analizirajući ih uz pomoć predloška Europskog odbora za zaštitu podataka koji omogućuje usporedbu zahtjeva (vođenih normom ISO 17065 i smjernicama Europskog odbora za zaštitu podataka o akreditaciji certifikacijskih tijela).

2. Pozivanjem na članak 43. Opće uredbe, nadležna nadzorna tijela donose zahtjeve za akreditaciju. No, ona moraju primijeniti mehanizam konzistentnosti kako bi se omogućilo stvaranje povjerenja u mehanizam certifikacije, posebice postavljanjem visoke razine zahtjeva.

3. Iako su zahtjevi za akreditaciju podložni mehanizmu konzistentnosti, to ne znači da bi zahtjevi trebali biti jednaki. Nadležna nadzorna tijela imaju određenu diskrecijsku slobodu s obzirom na nacionalni ili regionalni kontekst i trebaju uzeti u obzir lokalno zakonodavstvo. Cilj mišljenja Europskog odbora za zaštitu podataka nije postići jedinstveni skup zahtjeva na razini EU-a, već izbjeći značajne nekonzistentnosti koje mogu utjecati, primjerice, na povjerenje u neovisnost ili stručnost akreditiranih certifikacijskih tijela.

4. „Smjernice 4/2018 o akreditaciji certifikacijskih tijela temeljem članka 43. Opće uredbe o zaštiti podataka (2016/679)” (dalje u tekstu „Smjernice”) i „Smjernice 1/2018 o certifikaciji i utvrđivanju kriterija certifikacije u skladu s člancima 42. i 43. Uredbe 2016/679” služit će kao nit vodilja u kontekstu mehanizma konzistentnosti.

5. Ako država članica propisuje da certifikacijska tijela mora akreditirati nadzorno tijelo, nadzorno tijelo treba utvrditi zahtjeve za akreditaciju, uključujući, ali ne ograničavajući se na zahtjeve navedene u članku 43. stavku 2. Opće uredbe. U usporedbi s obvezama koje se odnose na akreditaciju certifikacijskih tijela koju provode nacionalna akreditacijska tijela, članak 43. Opće uredbe navodi manje pojedinosti o zahtjevima za akreditaciju kada nadzorno tijelo samostalno

1 Upućivanja na „Uniju” u ovom mišljenju trebaju se tumačiti kao upućivanja na „EGP”.

provodi akreditaciju. Radi doprinosa usklađenom pristupu akreditaciji, zahtjevi za akreditaciju koje primjenjuje nadzorno tijelo trebali bi se voditi normom ISO/IEC 17065 i trebali bi biti dopunjeni dodatnim zahtjevima koje određuje nadzorno tijelo u skladu s člankom 43. stavkom 1. točkom (b) Opće uredbe. Europski odbor za zaštitu podataka napominje da se u članku 43. stavku 2. točkama od (a) do (e) Opće uredbe odražavaju i navode zahtjevi iz norme ISO 17065, čime će se pridonijeti konzistentnosti.2

6. Mišljenje Europskog odbora za zaštitu podataka donosi se sukladno članku 64. stavku 1. točki (c) i stavcima 3. i 8. Opće uredbe u vezi s člankom 10. stavkom 2. Poslovnika Europskog odbora za zaštitu podataka u roku od osam tjedana od prvog radnog dana nakon što predsjednik i nadležno nadzorno tijelo odluče da je dokumentacija cjelovita. Odlukom predsjednika taj se rok može produžiti za dodatnih šest tjedana, uzimajući u obzir složenost predmeta.

USVOJIO JE SLJEDEĆE MIŠLJENJE:

Sažetak činjenica

Irsko nadzorno tijelo podnijelo je svoj nacrt zahtjeva za akreditaciju na temelju članka 43. stavka 1. točke (b) Europskom odboru za zaštitu podataka. Smatra se da je dokumentacija bila cjelovita 13. veljače 2020. Irsko nacionalno akreditacijsko tijelo (INAB) provodit će akreditaciju certifikacijskih tijela za certificiranje na temelju kriterija za certifikaciju iz Opće uredbe. To znači da će irsko nacionalno akreditacijsko tijelo upotrebljavati normu ISO 17065 i dodatne zahtjeve koje određuje irsko nadzorno tijelo, nakon što ih irsko nadzorno tijelo odobri, nakon mišljenja Odbora o nacrtu zahtjeva za akreditaciju certifikacijskih tijela.

U skladu s člankom 10. stavkom 2. Poslovnika Odbora, zbog složenosti pitanja predsjednica Odbora je odlučila produljiti za još šest tjedana prvotni rok za usvajanje mišljenja od osam tjedana.

Procjena

Opće obrazloženje Europskog odbora za zaštitu podataka o podnesenom nacrtu odluke

Svrha ovog mišljenja je procijeniti zahtjeve za akreditaciju koje je izradilo nadzorno tijelo, u odnosu na normu ISO 17065 ili na cijeli skup zahtjeva, u svrhu omogućavanja nacionalnom akreditacijskom tijelu ili nadzornom tijelu, kako je utvrđeno u članku 43. stavku 1. Opće uredbe, da akreditira certifikacijsko tijelo odgovorno za izdavanje i obnavljanje certifikata u skladu s člankom 42. Opće uredbe. To ne dovodi u pitanje zadaće i ovlasti nadležnog nadzornog tijela. U ovom konkretnom slučaju Odbor primjećuje da je irsko nadzorno tijelo odlučilo obratiti se svojem nacionalnom akreditacijskom tijelu radi izdavanja akreditacije, sastavivši dodatne zahtjeve u skladu sa Smjernicama, koje bi trebalo koristiti njegovo nacionalno akreditacijsko tijelo prilikom izdavanja akreditacije.

Ova procjena dodatnih zahtjeva irskog nadzornog tijela usmjerena je na ispitivanje izmjena (dodataka ili brisanja) u odnosu na Smjernice, a posebno njihov Prilog 1. Nadalje, mišljenje Europskog odbora za zaštitu podataka usredotočeno je i na sve aspekte koji mogu utjecati na dosljedan pristup u akreditaciji certifikacijskih tijela.

2 Smjernice 4/2018 o akreditaciji certifikacijskih tijela u skladu s člankom 43. Opće uredbe o zaštiti podataka (2016/39), točka 39. Dostupno na: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_hr

Treba napomenuti da je cilj Smjernica o akreditaciji certifikacijskih tijela pružiti pomoć nadzornim tijelima tijekom određivanja zahtjeva za akreditaciju. Prilog Smjernicama ne predstavlja akreditacijske zahtjeve kao takve. Stoga, nadzorno tijelo treba odrediti zahtjeve za akreditaciju za certifikacijska tijela na onaj način koji omogućuje njihovu praktičnu i dosljednu primjenu kako to zahtijeva kontekst nadzornog tijela.

Odbor priznaje činjenicu da, uzimajući u obzir njihovu stručnost, nacionalnim akreditacijskim tijelima treba pružiti određenu slobodu prilikom određivanja posebnih odredbi unutar primjenjivih zahtjeva za akreditaciju. Međutim, Odbor smatra potrebnim naglasiti da, ako se uvedu bilo kakvi dodatni zahtjevi, oni trebaju biti određeni na način koji omogućava njihovu praktičnu, dosljednu primjenu i preispitivanje prema potrebi.

Odbor napominje da norme ISO, osobito norma ISO 17065, podliježu pravima intelektualnog vlasništva te se stoga u ovom Mišljenju neće pozivati na tekst s time povezanog dokumenta. Shodno tomu, Odbor je odlučio upućivati, gdje je to potrebno, na određene dijelove norme ISO, bez reproduciranja njezina teksta.

Konačno, Odbor je obavio svoju procjenu u skladu sa strukturom predviđenom u Prilogu 1. Smjernicama (dalje u tekstu „Prilog"). Ako ovo Mišljenje ne sadrži očitovanje o određenom članku nacrta zahtjeva za akreditaciju irskog nadzornog tijela, to znači da Odbor nema primjedbe i ne traži od irskog nadzornog tijela da poduzme daljnje korake.

Ovo mišljenje ne sadrži očitovanja o onim stavkama koje je podnijelo irsko nadzorno tijelo koje su izvan područja primjene članka 43. stavka 2. Opće uredbe, kao što su upućivanja na nacionalno zakonodavstvo. Unatoč tomu, Odbor napominje da nacionalno zakonodavstvo treba biti u skladu s Općom uredbom gdje je to potrebno.

Glavne točke za procjenu (članak 43. stavak 2. Opće uredbe i Prilog 1. Smjernicama Europskog odbora za zaštitu podataka) o tome pružaju li zahtjevi za akreditaciju mogućnost dosljedne procjene sljedećeg:

1. obuhvaćanje svih ključnih područja, kako su istaknuta u Prilogu Smjernicama, i razmatranje svakog odstupanja od Priloga
2. neovisnost certifikacijskog tijela
3. sukobi interesa certifikacijskog tijela
4. stručnost certifikacijskog tijela
5. primjerene zaštitne mjere kojima se osigurava da certifikacijsko tijelo prikladno primjenjuje uvjete Opće uredbe za certifikaciju
6. postupci za izdavanje, periodično preispitivanje i povlačenje certificiranja u skladu s Općom uredbom i
7. transparentno postupanje s pritužbama na kršenja certifikacije.

Uzimajući u obzir da:

1. u članku 43. stavku 2. Opće uredbe navodi se popis područja akreditacije koja certifikacijsko tijelo mora obuhvatiti da bi dobilo akreditaciju;

2. u članku 43. stavku 3. Opće uredbe navodi se da zahtjeve za akreditaciju certifikacijskih tijela mora odobriti nadležno nadzorno tijelo;

3. u članku 57. stavku 1. točkama (p) i (q) Opće uredbe određuje se da nadležno nadzorno tijelo mora sastaviti i objaviti zahtjeve za akreditaciju certifikacijskih tijela i može odlučiti samostalno provesti akreditaciju certifikacijskih tijela;

4. u članku 64. stavku 1. točki (c) Opće uredbe navodi se da Odbor daje mišljenje kada nadzorno tijelo namjerava odobriti zahtjeve za akreditaciju certifikacijskog tijela u skladu s člankom 43. stavkom 3.;

5. ako akreditaciju provodi nacionalno akreditacijsko tijelo u skladu s normom ISO/IEC 17065/2012, moraju se primijeniti i dodatni zahtjevi koje je utvrdilo nadležno nadzorno tijelo;

6. u Prilogu 1. Smjernicama o akreditaciji certifikacije predviđeni su predloženi zahtjevi koje nadzorno tijelo za zaštitu podataka mora izraditi i koji se primjenjuju kada nacionalno tijelo za akreditaciju akreditira certifikacijsko tijelo;

Odbor donosi sljedeće mišljenje:

UVODNA ODREDBA (članak 0. nacrta zahtjeva za akreditaciju irskog nadzornog tijela)

Odbor potvrđuje činjenicu da uvjeti suradnje kojima se uređuje odnos između nacionalnog akreditacijskog tijela i njegova nadzornog tijela za zaštitu podataka nisu zahtjev za akreditaciju certifikacijskih tijela sami po sebi. Međutim, radi potpunosti i transparentnosti, Odbor smatra da ti uvjeti suradnje, ako postoje, moraju biti objavljeni u formatu koji nadzorno tijelo smatra odgovarajućim.

POJMOVI I DEFINICIJE

Odbor primjećuje da nije ažurirano upućivanje na smjernice za akreditaciju kao „WP 261”. Europski odbor za zaštitu podataka usvojio je Smjernice 4/2018 o akreditaciji certifikacijskih tijela u skladu s člankom 43. Opće uredbe o zaštiti podataka (2016/679). Stoga Odbor potiče irsko nadzorno tijelo da izmijeni tekst i uvede upućivanje na Smjernice 4/2018.

OPĆE NAPOMENE

Odbor primjećuje da nacrt zahtjeva irskog nadzornog tijela više puta upućuje na „nadležno nadzorno tijelo". Budući da je nadležno nadzorno tijelo u ovom slučaju irsko nadzorno tijelo, Odbor potiče irsko nadzorno tijelo da zamijeni to upućivanje na „Povjerenstvo za zaštitu podataka" ili „irsko nadzorno tijelo", radi izbjegavanja zabune.

Odbor potvrđuje da nacrt zahtjeva irskog nadzornog tijela uključuje odjeljak o pojmovima i definicijama. Međutim, neki se pojmovi u dokumentu ne upotrebljavaju dosljedno (npr. „predmet procjene" i „uvjeti procjene"). Da bi se izbjegla zabuna, Odbor potiče irsko nadzorno tijelo da upotrebljava dosljednu terminologiju u nacrtu zahtjeva.

OPĆI ZAHTJEVI ZA AKREDITACIJU (članak 4. nacrta zahtjeva za akreditaciju)

U odnosu na članak 7. pododjeljka 4.1.2. nacrta zahtjeva za akreditaciju irskog nadzornog tijela, Odbor smatra da je tekst donekle nejasan u odnosu na to kome se podnose razlozi za odobrenje certifikacije. Nadalje, upućivanje na „olakšavanje" registracije također je nejasno. Stoga Odbor potiče irsko nadzorno tijelo da ponovno izradi taj dio radi postizanja veće jasnoće.

STRUKTURNI ZAHTJEVI (članak 5. nacrta zahtjeva za akreditaciju)

Odbor primjećuje da nacrt zahtjeva za akreditaciju irskog nadzornog tijela upućuje na imenovanje „osobe na odgovarajućem položaju koja je odgovorna za nadgledanje sukladnosti sa zaštitom podataka i upravljanje informacijama." Upućivanje na odgovarajuću višu funkciju treba pojasniti u pogledu iskustva i opsega ovlasti. Štoviše, djelokrug rada te osobe čini se sličnim djelokrugu rada službenika za zaštitu podataka. Odbor potiče irski nadzorni odbor da jasno utvrdi djelokrug rada te osobe i odredi odgovarajuće iskustvo.

ZAHTJEVI KOJI SE TIČU RESURSA (članak 6. nacrta zahtjeva za akreditaciju)

U vezi s osobljem certifikacijskog tijela (pododjeljak 6.1.) Odbor primjećuje da zahtjevi za osoblje tehničke stručnosti koje je odgovorno za donošenje odluka uključuju najmanje 5 godina stručnog iskustva povezanog s predmetom certifikacije, dok bi osoblje odgovorno za procjene trebalo imati najmanje 2 godine stručnog iskustva. Slično tome, osoblje pravne stručnosti koje donosi odluke mora imati najmanje 5 godina stručnog iskustva, dok osobe nadležne za procjene moraju imati najmanje 2 godine iskustva. Odbor primjećuje da se znatno razlikuje traženi najmanji broj godina stručnog iskustva između osoblja nadležnog za odlučivanje i osoblja nadležnog za procjenu. U tom pogledu Odbor smatra da bi trebalo staviti naglasak na različite vrste stručnosti umjesto na broj godina stručnog iskustva. Prema mišljenju Odbora procjenitelji bi trebali imati više specijalističke stručnosti i stručnog iskustva u tehničkim postupcima (npr. revizijama i certifikacijama), dok bi donositelji odluka trebali imati općenitiju i sveobuhvatniju stručnost te stručno iskustvo u zaštiti podataka. S obzirom na to, Odbor potiče irsko nadzorno tijelo da stavi veći naglasak na različita materijalna znanja i/ili iskustva procjenitelja i donositelja odluka te da smanji razlike u traženim godinama iskustva.

POSTUPOVNI ZAHTJEVI (članak 7. nacrta zahtjeva za akreditaciju)

U odnosu na pododjeljak 7.10. nacrta zahtjeva za akreditaciju irskog nadzornog tijela („Promjene koje utječu na certifikaciju") Odbor primjećuje da nema upućivanja na postupke promjena koje treba usuglasiti, u skladu sa stavkom 7.10. Priloga. Odbor potiče irsko nadzorno tijelo da uključi takvo upućivanje i da spomene neke od postupaka koje bi se moglo uvesti (npr. prijelazna razdoblja, postupak odobrenja kod nadležnog nadzornog tijela...). Uz to, Odbor smatra da su promjene u tehnološkim dostignućima također relevantne i mogle bi utjecati na certifikaciju. Stoga Odbor potiče

irsko nadzorno tijelo da uključi ovu mogućnost u popis promjena koje utječu na certifikaciju. Konačno, Odbor pozdravlja uključivanje povreda osobnih podataka i kršenja Opće uredbe na popis promjena koje utječu na certifikaciju. Međutim, da bi se osigurala jasnoća, Odbor potiče irsko nadzorno tijelo da odredi da se povrede osobnih podataka i povrede Opće uredbe uzmu u obzir samo u onoj mjeri u kojoj se odnose na certifikaciju.

Što se tiče promjena koje utječu na certifikaciju (pododjeljak 7.10. nacrta zahtjeva irskog nadzornog tijela), osobito pete točke, Odbor primjećuje da irsko nadzorno tijelo upućuje na „primjenjive obvezujuće odluke Europskog odbora za zaštitu podataka" kao i na članak 39. Poslovnika Europskog odbora za zaštitu podataka, što uključuje „sve konačne dokumente koje je donio Europski odbor za zaštitu podataka". Da bi se osiguralo jasno razumijevanje onoga što se podrazumijeva pod „odlukama Europskog odbora za zaštitu podataka", Odbor potiče irsko nadzorno tijelo da pojasni to upućivanje. Primjer bi mogao biti upućivanje na „dokumente koje je usvojio Europski odbor za zaštitu podataka".

Odbor primjećuje da pododjeljak 7.11. nacrta zahtjeva irskog nadzornog tijela (okončanje, ograničenje, obustava ili povlačenje certifikacije) ne sadrži obvezu certifikacijskog tijela da prihvati odluke i naredbe irskog nadzornog tijela da povuče ili ne izda certifikaciju nekom podnositelju ako zahtjevi za certifikaciju nisu ispunjeni ili više nisu ispunjeni. Stoga Odbor preporučuje irskom nadzornom tijelu da uključi takvu obvezu.

Zaključci/preporuke

Nacrt zahtjeva za akreditaciju irskog nadzornog tijela može dovesti do nedosljedne provedbe akreditacije certifikacijskih tijela, te je potrebno unijeti sljedeće izmjene:

U pogledu „postupovnih zahtjeva", Odbor preporučuje da irsko nadzorno tijelo:

1. uključi, u pododjeljak 7.11., obvezu certifikacijskog tijela da prihvati odluke i naredbe irskog nadzornog tijela da povuče ili ne izda certifikaciju nekom podnositelju ako zahtjevi za certifikaciju nisu ili više nisu ispunjeni.

Završne napomene

Ovo mišljenje upućuje se irskom nadzornom tijelu i bit će objavljeno u skladu s člankom 64. stavkom 5. točkom (b) Opće uredbe.

U skladu s člankom 64. stavcima 7. i 8. Opće uredbe irsko nadležno tijelo dužno je u roku od dva tjedna od primitka mišljenja obavijestiti predsjednika elektroničkim putem o tome hoće li izmijeniti svoj nacrt popisa ili će ga zadržati. U istom je roku dužno dostaviti izmijenjeni nacrt popisa ili, ako ne namjerava uzeti u obzir mišljenje Odbora, dostaviti odgovarajuće razloge zbog kojih ne namjerava uzeti u obzir ovo mišljenje u cijelosti ili djelomično.

Irsko nadzorno tijelo dužno je priopćiti konačnu odluku Odboru radi uključivanja u evidenciju odluka koje podliježu mehanizmu konzistentnosti, u skladu s člankom 70. stavkom 1. točkom (y) Opće uredbe.

Za Europski odbor za zaštitu podataka

Predsjednica

Usvojeno

(Andrea Jelinek)