Mišljenje 15/2020 o nacrtu odluke njemačkih nadležnih nadzornih tijela o odobravanju zahtjeva za akreditaciju certifikacijskog tijela u skladu s člankom 43. stavkom 3. Opće uredbe o zaštiti podataka

Doneseno 25. svibnja 2020.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Doneseno

Sadržaj

Europski odbor za zaštitu podataka

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 o zaštiti podataka"),

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 „GDPR") u čitavom Europskom gospodarskom prostoru. U skladu s člankom 64. stavkom 1. GDPR-a, 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 podataka ili nacionalno akreditacijsko tijelo primijeniti prilikom akreditacije certifikacijskog tijela. Iako Opća uredba o zaštiti podataka ne propisuje jedinstven skup zahtjeva za akreditaciju, tom se uredbom 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 (na temelju norme ISO 17065 i smjernicama Europskog odbora za zaštitu podataka o akreditaciji certifikacijskih tijela).

(2) U vezi s člankom 43. Opće uredbe o zaštiti podataka, nadležna nadzorna tijela donose zahtjeve za akreditaciju. No, ona moraju primijeniti mehanizam konzistentnosti kako bi se omogućilo stvaranje povjerenja u mehanizam certifikacije, posebno određivanjem zahtjeva visoke razine.

(3) Iako su zahtjevi za akreditaciju podložni mehanizmu konzistentnosti, to ne znači da bi zahtjevi trebali biti jednaki. Nadležna nadzorna tijela imaju 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 nedosljednosti 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

[1] Upućivanja na „Uniju" u ovom mišljenju trebaju se tumačiti kao upućivanja na „EGP".

u članku 43. stavku 2. U usporedbi s obvezama koje se odnose na akreditaciju certifikacijskih tijela koju provode nacionalna akreditacijska tijela, u članku 43. pruža se manje informacija o zahtjevima za akreditaciju kad nadzorno tijelo samostalno provodi akreditaciju. Kako bi se pridonijelo usklađenom pristupu akreditaciji, zahtjevi za akreditaciju koje primjenjuje nadzorno tijelo trebali bi se temeljiti na normi ISO/IEC 17065 i trebali bi se nadopuniti dodatnim zahtjevima koje određuje nadzorno tijelo u skladu s člankom 43. stavkom 1. točkom (b). Europski odbor za zaštitu podataka napominje da se u članku 43. stavku 2. točkama od (a) do (e) uzimaju u obzir i navode zahtjevi iz norme ISO 17065, čime će se pridonijeti dosljednosti.[2]

(6) Mišljenje Europskog odbora za zaštitu podataka donosi se na temelju članka 64. stavka 1. točke (c) i stavaka 3. i 8. Opće uredbe o zaštiti podataka zajedno 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. Kada predsjednik donese odluku, taj se rok može produljiti za dodatnih šest tjedana, uzimajući u obzir složenost predmeta.

DONIO JE SLJEDEĆE MIŠLJENJE:

1 SAŽETAK ČINJENICA

1. Njemačka nadzorna tijela na razini države i saveznih pokrajina podnijela su 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. Njemačko nacionalno akreditacijsko tijelo, DAkkS, provest će akreditaciju certifikacijskih tijela za certificiranje na temelju kriterija za certifikaciju iz Opće uredbe o zaštiti podataka. To znači da će za akreditaciju certifikacijskih tijela nacionalno akreditacijsko tijelo upotrebljavati normu ISO 17065 i dodatne zahtjeve koje određuju njemačka nadzorna tijela, nakon što ih njemačka nadzorna tijela odobre, na temelju mišljenja Odbora o nacrtu zahtjeva.

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

2 PROCJENA

2.1 Opće obrazloženje Europskog odbora za zaštitu podataka o podnesenom nacrtu odluke

3. Svrha je ovog mišljenja procijeniti zahtjeve za akreditaciju koje je utvrdilo nadzorno tijelo, s obzirom na normu ISO 17065 ili potpuni skup zahtjeva, u svrhu dopuštanja nacionalnom akreditacijskom tijelu ili nadzornom tijelu, kako je utvrđeno u članku 43. stavku 1. GDPR-a, da akreditira certifikacijsko tijelo odgovorno za izdavanje i obnavljanje certifikata u skladu s člankom 42. GDPR-a. Time se ne dovode u pitanje zadatci i ovlasti nadležnog nadzornog tijela. U ovom konkretnom slučaju Odbor napominje da

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

su njemačka nadzorna tijela odlučila zatražiti zajedničku akreditaciju od strane svojeg nacionalnog akreditacijskog tijela DAkkS-a i nadležnog nadzornog tijela, radi izdavanja akreditacije, odredivši dodatne zahtjeve u skladu sa Smjernicama, koje bi trebalo primijeniti prilikom izdavanja akreditacije.

4. Ova procjena dodatnih zahtjeva za akreditaciju njemačkih nadzornih tijela usmjerena je na ispitivanje izmjena (dodavanja 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.

5. 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, nadzorna tijela trebaju definirati zahtjeve za akreditaciju za certifikacijska tijela na način koji omogućuje njihovu praktičnu i dosljednu primjenu kako to zahtijeva kontekst nadzornih tijela.

6. Odbor je svjestan činjenice da, uzimajući u obzir njihovu stručnost, nacionalnim akreditacijskim tijelima i nadležnim nadzornim tijelima, prema potrebi, treba pružiti određenu slobodu prilikom definiranja određenih 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.

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

8. 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 odjeljku nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela, to znači da Odbor nema primjedbe i ne traži od njemačkih nadzornih tijela da poduzmu daljnje korake.

9. Ovo Mišljenje ne sadrži očitovanja o stavkama koje su podnijela njemačka nadzorna tijela, a koje su izvan područja primjene članka 43. stavka 2. Opće uredbe o zaštiti podataka, kao što su upućivanja na nacionalno zakonodavstvo. Unatoč tomu, Odbor napominje da nacionalno zakonodavstvo treba biti u skladu s Općom uredbom o zaštiti podataka gdje je to potrebno.

2.2 Glavne točke za procjenu (članak 43. stavak 2. GDPR-a i Prilog 1. Smjernicama Europskog odbora za zaštitu podataka) o tome je li zahtjevima za akreditaciju predviđena dosljedna procjena 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 kriterije GDPR-a za certifikaciju

6) postupci za izdavanje, periodično preispitivanje i povlačenje certificiranja u skladu s GDPR-om i

7) transparentno postupanje s pritužbama na kršenja certifikacije.

10. Uzimajući u obzir da:

a. u članku 43. stavku 2. GDPR-a navodi se popis područja akreditacije koja certifikacijsko tijelo mora obuhvatiti da bi dobilo akreditaciju;

b. u članku 43. stavku 3. GDPR-a navodi se da zahtjeve za akreditaciju certifikacijskih tijela mora odobriti nadležno nadzorno tijelo;

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

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

e. 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;

f. 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:

2.2.1 UVOD

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

2.2.2 POJMOVI I DEFINICIJE

12. Odbor primjećuje da su u poglavlju 3. („Definicije”) nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela određene dopuštene vrste programa certificiranja te je navedeno da moraju ispunjavati zahtjeve norme DIN EN ISO/IEC 17065. U tom pogledu trebalo bi istaknuti da je u člancima 5.1. i 5.2. Smjernica Europskog odbora za zaštitu podataka već sveobuhvatno navedeno što se može certificirati u skladu s Općom uredbom o zaštiti podataka. Stoga Odbor potvrđuje da namjera njemačkih nadzornih tijela nije ograničiti ono što je navedeno u Smjernicama i da se tvrdnje sadržane

u poglavlju 3. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela trebaju smatrati primjenjivima u kontekstu tih zahtjeva za akreditaciju.

2.2.3 OPĆE NAPOMENE

13. Odbor primjećuje da se u odjeljku o „općim napomenama“ nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela navodi „odobravanje (eng. authorization)” kriterija za certifikaciju od strane Europskog odbora za zaštitu podataka „u skladu s člankom 63. i člankom 64. stavkom 1. točkom (c) Opće uredbe o zaštiti podataka”. Odbor napominje da Općom uredbom o zaštiti podataka nije propisana nadležnost Europskog odbora za zaštitu podataka da „odobrava (eng. authorise)” kriterije za certifikaciju. Međutim, u skladu s prethodnim člancima, Europski odbor za zaštitu podataka može odobriti (eng. approve) kriterije za certifikaciju. Stoga Odbor preporučuje njemačkim nadzornim tijelima da izbrišu upućivanje na „odobravanje (eng. authorisation) od strane Europskog odbora za zaštitu podataka” kako bi nacrt bio u skladu s tekstom Opće uredbe o zaštiti podataka.

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

14. Kad je riječ o zahtjevu u pogledu pravne odgovornosti (članak 4.1. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela), Odbor primjećuje da, u popratnom dokumentu, njemačka nadzorna tijela pojašnjavaju da se od certifikacijskog tijela očekuje da ima uspostavljene ažurne postupke te stoga nema potrebe za dodavanjem daljnjih zahtjeva u tom pogledu. Međutim, Odbor smatra da očekivanje ne obvezuje certifikacijska tijela da imaju uspostavljene takve postupke. Kako je utvrđeno u članku 4.1.1. Priloga Smjernicama, certifikacijska tijela moraju imati uspostavljene ažurne postupke kojima se dokazuje usklađenost s pravnim odgovornostima utvrđenima u uvjetima akreditacije. Štoviše, certifikacijsko tijelo mora moći podnijeti dokaz o postupcima i mjerama usklađenim s Općom uredbom o zaštiti podataka, posebno za upravljanje i postupanje s osobnim podacima organizacije klijenata u okviru certifikacijskog postupka. Stoga, Odbor preporučuje njemačkim nadzornim tijelima da izmijene nacrt zahtjeva kako bi ga uskladili sa Smjernicama.

15. Kad je riječ o pododjeljku 4.1.2.2. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („sporazum o certificiranju”), Odbor primjećuje da nacrt zahtjeva za akreditaciju njemačkih nadzornih tijela ne uključuje obvezu omogućavanja potpune transparentnosti nadležnom nadzornom tijelu u pogledu certifikacijskog postupka, među ostalim ugovorno povjerljivih pitanja. Osim toga, ne postoji upućivanje na obvezu podnositelja zahtjeva da certifikacijskom tijelu pruži pristup svojim aktivnostima obrade osobnih podataka. Stoga, Odbor preporučuje njemačkim nadzornim tijelima da uključe prethodno navedene obveze u svoj nacrt.

16. Odbor primjećuje da izričito upućivanje na zadatke i ovlasti nadležnog nadzornog tijela (treća alineja u članku 4.1.2. Priloga) nije uključeno u pododjeljak 4.1.2.2. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela. Odbor smatra da bi to upućivanje trebalo dodati u nacrt zahtjeva te stoga preporučuje njemačkim nadzornim tijelima da u skladu s tim izmijene nacrt.

17. Nadalje, nacrt zahtjeva za akreditaciju njemačkih nadzornih tijela u pogledu sporazuma o certificiranju ne uključuje obvezu omogućavanja certifikacijskom tijelu da otkrije sve podatke potrebne za davanje certifikata u skladu s člankom 42. stavkom 8. i člankom 43. stavkom 5. Opće uredbe o zaštiti podataka (sedma alineja u članku 4.1.2. Priloga). Iako je ta obveza uključena u odjeljak o upravljanju postupcima nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela, Odbor smatra da bi ona trebala biti dio sporazuma o certificiranju, kako bi se ojačao njezin obvezujući učinak. Pritom, Odbor preporučuje

njemačkim nadzornim tijelima da uključe prethodno navedenu obvezu kao dio elemenata sporazuma o certificiranju.

18. Prema Prilogu, podnositelj zahtjeva mora obavijestiti certifikacijsko tijelo o značajnim promjenama svoje stvarne ili pravne situacije i svojih proizvoda, postupaka i usluga na koje se odnosi certifikacija (deseta alineja u članku 4.1.2. Priloga). Međutim, u nacrtu zahtjeva za akreditaciju njemačkih nadzornih tijela, šesta alineja pododjeljka 4.1.2.2. sadrži jedino obvezu obavještavanja certifikacijskog tijela o značajnim promjenama stvarnih ili pravnih okolnosti, ali u njoj se ne spominju izričito proizvodi, postupci i usluge. Odbor preporučuje njemačkim nadzornim tijelima da uključe takvo upućivanje, u skladu s Prilogom.

19. Kad je riječ o pododjeljku 4.2.7. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („postupanje s nepristranošću"), Odbor preporučuje ojačavanje kriterija primjenjivih na certifikacijska tijela koja pripadaju zasebnom pravnom subjektu ili kojima upravlja zasebni pravni subjekt tako da se uzme u obzir činjenica da svaka vrsta ekonomskog odnosa između certifikacijskog tijela i pravnog subjekta, ovisno o njegovim značajkama, može utjecati na nepristranost njegovih aktivnosti certificiranja.

20. Kad je riječ o članku 4.6. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („podatci dostupni javnosti"), Odbor primjećuje da ne postoji upućivanje na objavu svih verzija odobrenih kriterija i certifikacijskih postupaka. Stoga, Odbor potiče njemačka nadzorna tijela da izmijene nacrt zahtjeva za akreditaciju kako bi se izričito navelo da objava uključuje sve verzije odobrenih kriterija i certifikacijskih postupaka. Osim toga, Odbor primjećuje da je u drugom stavku članka 4.6. navedeno da se „programi certificiranja koje koristi certifikacijsko tijelo odobreni kriteriji u skladu s člankom 42. stavkom 5. Opće uredbe o zaštiti podataka u kojima je navedeno odobreno trajanje primjene *trebaju općenito objaviti*." Kako bi se izbjegla svaka nejasnoća, Odbor potiče njemačka nadzorna tijela da izbrišu riječ „općenito" i dodaju „i" između izraza „certifikacijsko tijelo" i „odobreni kriteriji".

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

21. Kad je riječ o zahtjevima stručnosti i konkretno pododjeljku 6.1.2.1. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („kompetencija osoblja"), Odbor primjećuje da za potrebno znanje u navedenim područjima nije navedeno da znanje mora biti relevantno i primjereno. Kako bi se osigurala dosljednost s razinom stručnosti propisanom u Prilogu, Odbor preporučuje njemačkim nadzornim tijelima da usklade tekst sa Smjernicama tako da propišu da znanje mora biti relevantno i primjereno.

22. Nadalje, Odbor primjećuje da zahtjevi za osoblje s tehničkom stručnošću odgovorno za donošenje odluka uključuju najmanje sedam godina stručnog iskustva ili pet godina stručnog iskustva u području tehničke zaštite podataka, ovisno o njihovoj razini obrazovanja, dok bi osoblje odgovorno za ocjenjivanje trebalo imati četiri godine stručnog iskustva ili dvije godine stručnog iskustva u području tehničke zaštite podataka i iskustva u postupku ispitivanja, ovisno o njihovoj razini obrazovanja. Slično tome, osoblje pravne struke koje donosi odluke mora imati najmanje pet godina stručnog iskustva u području prava o zaštiti podataka, dok osobe nadležne za ocjenjivanje moraju imati najmanje dvije godine iskustva u području prava o zaštiti podataka i postupcima revizije. Odbor primjećuje da se znatno razlikuje traženi najmanji broj godina stručnog iskustva između osoblja nadležnog za odlučivanje i osoblja nadležnog za ocjenjivanje. U tom pogledu, Odbor smatra da bi zahtjeve u pogledu kompetencija za procjenitelje i donositelje odluka trebalo prilagoditi uzimajući u obzir različite zadatke koje obavljaju, a ne broj godina stručnog iskustva. Odbor smatra da bi procjenitelji 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 njemačka nadzorna tijela da stave veći naglasak na različita materijalna znanja i/ili iskustva procjenitelja i donositelja odluka te da smanje razlike u traženim godinama iskustva.

23. Osim toga, Odbor smatra da bi znanje o sustavima upravljanja relevantnim za područje certificiranja trebalo proširiti na normu ISO/IEC 27701:2019 – Sigurnosne tehnike – Proširenje na norme ISO/IEC 27001 i ISO/IEC 27002 za upravljanje informacijama o privatnosti – Preporuke i smjernice, te potiče njemačka nadzorna tijela da uključe takvo upućivanje.

24. Konačno, kad je riječ o zahtjevima u pogledu obrazovanja tehničkog osoblja, Odbor smatra da je popis predmeta već prilagođen tehničkoj stručnosti propisanoj u Prilogu. Stoga, Odbor potiče njemačka nadzorna tijela da izbrišu upućivanje na „prirodne znanosti" s popisa predmeta u pogledu sveučilišnog obrazovanja tehničkog osoblja.

2.2.6 POSTUPOVNI ZAHTJEVI (poglavlje 7. nacrta zahtjeva za akreditaciju)

25. Odbor primjećuje da poglavlje 7. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela sadrži nekoliko upućivanja na izraz „njegovi kriteriji" (primjerice, u člancima 7.4., 7.6., 7.11. i 7.13.). Kako bi se izbjegla svaka nejasnoća, Odbor potiče njemačka nadzorna tijela da pojasne značenje tog izraza, primjerice, dodavanjem objašnjenja u Prilogu 1. (Pojmovnik).

26. Kad je riječ o članku 7.1. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („opće informacije"), Odbor primjećuje da ne postoji izričito upućivanje na obvezu certifikacijskog tijela da poštuje dodatne zahtjeve. Iako bi se iz teksta nacrta zahtjeva moglo zaključiti da postoji takva obveza, Odbor smatra da bi trebalo uključiti izričito upućivanje na prethodno navedenu obvezu. Stoga, Odbor preporučuje njemačkim nadzornim tijelima da izmijene nacrt u skladu s tim.

27. Odbor primjećuje da nacrt dodatnih zahtjeva za akreditaciju njemačkih nadzornih tijela ne sadrži nikakvo upućivanje na primjenu odobrenog Europskog pečata za zaštitu podataka, u skladu s člankom 7.1.2. Priloga. Odbor smatra da bi trebalo uključiti to upućivanje, posebice s obzirom na to da može biti potrebno provesti akreditaciju certifikacijskog tijela koje dodjeljuje Europske pečate za zaštitu podataka u svakoj državi članici u kojoj certifikacijsko tijelo ima poslovni nastan.[3] Stoga, Odbor preporučuje njemačkim nadzornim tijelima da uključe gore navedeno upućivanje. Primjerice, u nacrtu zahtjeva moglo bi se navesti sljedeće: „Nadležno tijelo obavještava se prije nego što certifikacijsko tijelo počne primjenjivati odobreni Europski pečat za zaštitu podataka u novoj državi članici iz pomoćnog ureda".

28. Odbor primjećuje da je u članku 7.2. („zahtjev") nacrtom zahtjeva za akreditaciju njemačkih nadzornih tijela predviđena situacija u kojoj se izvršitelji obrade podataka koriste za provođenje postupaka obrade osobnih podataka, u skladu s Prilogom Smjernicama. Međutim, Odbor napominje da, kada se koriste izvršitelji obrade, zahtjev treba sadržavati odgovarajući ugovor(e) s voditeljem/izvršiteljem obrade, kako je navedeno u Prilogu. Stoga, Odbor preporučuje njemačkim nadzornim tijelima da tekst usklade sa smjernicama dodavanjem upućivanja na ugovor(e) s voditeljem/izvršiteljem obrade.

[3] U tom pogledu, vidjeti Smjernice 1/2018, stavak 44.

Štoviše, Odbor potiče njemačka nadzorna tijela da razmotre je li u tom slučaju potrebno navesti upućivanje na zajedničke voditelje obrade i njihove posebne dogovore.

29. Odbor primjećuje da je u članku 7.2. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela navedeno da „voditelj i izvršitelj obrade imaju pravo podnijeti zahtjev za dodjelu certifikata". Mogućnost da izvršitelji obrade podnesu zahtjev za dodjelu certifikata ovisit će o konkretnom programu certificiranja. Stoga, kako bi se izbjegle nejasnoće, Odbor potiče njemačka nadzorna tijela da izbrišu prethodno navedeno upućivanje ili da pojasne da će mogućnost da se izvršiteljima obrade dodijeli certifikat ovisiti o opsegu programa certificiranja.

30. Kad je riječ o članku 7.3. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („zahtjevi za ocjenjivanje"), Odbor primjećuje da je u nacrtu zahtjeva za akreditaciju njemačkih nadzornih tijela navedeno: „planirane metode ocjenjivanja utvrđene su ugovorom [...]". Kako bi bilo jasno da je riječ o zahtjevu, Odbor potiče njemačka nadzorna tijela da ponovno izrade nacrt prvog stavka kako bi pojasnila da metode ocjenjivanja moraju biti uključene u sporazum o certificiranju, odnosno da ponovno izrade nacrt zahtjeva tako da glasi: „planirane metode ocjenjivanja moraju biti utvrđene ugovorom [...]". Osim toga, Odbor potiče njemačka nadzorna tijela da zamijene upućivanje na članak 7.3.1. točku b norme ISO 17065 člankom 7.3. norme 17065 kako bi uskladila tekst s Prilogom. Nadalje, Odbor primjećuje da se u četvrtom stavku upućuje na primjerene tehničke i pravne kompetencije. Radi jasnoće, Odbor potiče njemačka nadzorna tijela da dodaju tekst „u području zaštite osobnih podataka".

31. Odbor primjećuje da članak 7.4. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („metode ocjenjivanja") ne sadrži obvezu certifikacijskog tijela da opiše dostatne metode ocjenjivanja za procjenu usklađenosti postup(a)ka obrade s kriterijima za certifikaciju. Odbor preporučuje njemačkim nadzornim tijelima da izmijene nacrt zahtjeva kako bi uključila takvo upućivanje. Primjerice, moglo bi se dodati sljedeće: *„Certifikacijsko tijelo osigurava da su mehanizmima koji se koriste za davanje certifikata opisane dostatne metode ocjenjivanja za procjenu usklađenosti postup(a)ka obrade s kriterijima za certifikaciju*". Štoviše, kad je riječ o prvom području koje metode ocjenjivanja moraju obuhvaćati, Odbor smatra da se nužnost i razmjernost moraju, po potrebi, procijeniti i u odnosu na predmetne ispitanike. Konačno, Odbor primjećuje da ne postoji upućivanje na dokumentiranje metoda i zaključaka. Stoga, Odbor potiče njemačka nadzorna tijela da izmijene nacrt i izričito uključe takva upućivanja.

32. Kad je riječ o postojećim certifikatima (članak 7.4. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela), Odbor smatra da četvrta alineja na stranici 13 uzrokuje nejasnoće jer nije jasno koja je veza između razdoblja valjanosti trenutačnih i prethodnih certifikata ni kako se međusobno uklapaju. Osim toga, ne čini se izvedivim dovoditi u pitanje valjanost certifikata koji je prethodno izdalo drugo akreditirano certifikacijsko tijelo. Ukratko, bilo bi korisno u tom stavku pojasniti odnos među različitim navedenim elementima. Odbor preporučuje njemačkim nadzornim tijelima da izmijene nacrt konkretno pojašnjavajući da trajanje valjanosti certifikata o sukladnosti s Općom uredbom o zaštiti podataka ne smije biti uvjetovano valjanošću drugih vrsta certifikata.

33. Kad je riječ o članku 7.5. („vrednovanje") nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela, Odbor potiče njemačka nadzorna tijela da promijene naziv članka u „preispitivanje".

34. Kad je riječ o promjenama koje utječu na certificiranje (članak 7.10. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela), Odbor primjećuje da je u nacrtu zahtjeva za akreditaciju njemačkih nadzornih tijela utvrđeno sljedeće: „klijent se pravodobno obavještava o promjenama zakonskog okvira koje na njega utječu". Imajući na umu potrebu za očuvanjem nepristranosti certifikacijskog

tijela, Odbor potiče njemačka nadzorna tijela da preoblikuju tu rečenicu kako bi bilo jasno da se klijentu, pravodobno, pružaju opće informacije o promjenama koje mogu na njega utjecati. Osim toga, kako bi se osiguralo jasno razumijevanje onoga što se podrazumijeva pod „odlukama Europskog odbora za zaštitu podataka", Odbor potiče njemačka nadzorna tijela da pojasne to upućivanje. Primjer bi mogao biti upućivanje na „dokumente koje je donio Europski odbor za zaštitu podataka".

35. Odbor primjećuje da članak 7.11. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („prestanak, ograničenje, obustava ili povlačenje certifikata") ne sadrži obvezu certifikacijskog tijela da prihvati odluke i naredbe njemačkih nadzornih tijela o povlačenju ili neizdavanju certifikata nekom podnositelju ako zahtjevi za certifikaciju nisu ispunjeni ili više nisu ispunjeni. Stoga Odbor preporučuje njemačkim nadzornim tijelima da uključe takvu obvezu. Štoviše, Odbor potiče njemačka nadzorna tijela da zamijene riječ „ograničenje" riječju „smanjenje" u nazivu članka, u skladu s Prilogom Smjernicama.

2.2.7 DALJNJI DODATNI ZAHTJEVI

36. Kad je riječ o pododjeljku 8.11.3. nacrta zahtjeva za akreditaciju njemačkih nadzornih tijela („upravljanje pritužbama"), Odbor potiče njemačka nadzorna tijela da zamijene upućivanje na „opravdane pritužbe" upućivanjem na „obrazložene pritužbe" kako bi se osigurala veća jasnoća.

3 ZAKLJUČCI/PREPORUKE

37. Nacrt zahtjeva za akreditaciju njemačkih nadzornih tijela na razini države i saveznih pokrajina može dovesti do nedosljedne provedbe akreditacije certifikacijskih tijela, te je potrebno unijeti sljedeće izmjene:

38. U pogledu „općih napomena", Odbor preporučuje da njemačka nadzorna tijela:

    1) izbrišu upućivanje na „odobravanje (eng. authorisation) od strane Europskog odbora za zaštitu podataka" kako bi nacrt bio u skladu s tekstom Opće uredbe o zaštiti podataka.

39. U pogledu „općih zahtjeva za akreditaciju", Odbor preporučuje da njemačka nadzorna tijela:

    1) izmijene zahtjeve u pogledu pravne odgovornosti (pododjeljak 4.1.) kako bi ih uskladili sa smjernicama

    2) izmijene pododjeljak 4.1.2.2. kako bi se, u sporazum o certificiranju, uključila obveza omogućavanja potpune transparentnosti njemačkim nadzornim tijelima u pogledu certifikacijskog postupka i obveza pružanja certifikacijskom tijelu pristupa podnositeljevim aktivnostima obrade osobnih podataka

    3) uključe izričito upućivanje, u pododjeljak 4.1.2.2., na zadatke i ovlasti nadležnog nadzornog tijela, u skladu s Prilogom

    4) uključe, kao jedan od elemenata sporazuma o certificiranju, obvezu omogućavanja certifikacijskom tijelu da otkrije sve podatke potrebne za davanje certifikata u skladu s člankom 42. stavkom 8. i člankom 43. stavkom 5. Opće uredbe o zaštiti podataka

5) uključe izričito upućivanje na „proizvode, postupke i usluge na koje se odnosi certifikacija” u šestoj alineji pododjeljka 4.1.2.2.

6) ojačaju, u pododjeljku 4.2.7., kriterije primjenjive na certifikacijska tijela koja pripadaju zasebnom pravnom subjektu ili kojima upravlja zasebni pravni subjekt tako da se uzme u obzir činjenica da svaka vrsta ekonomskog odnosa između certifikacijskog tijela i pravnog subjekta, ovisno o njegovim značajkama, može utjecati na nepristranost njegovih aktivnosti certificiranja.

40. Kad je riječ o „zahtjevima u pogledu resursa”, Odbor preporučuje da njemačka nadzorna tijela:

1) usklade tekst pododjeljka 6.1.2.1. sa smjernicama tako da propišu da znanje mora biti relevantno i primjereno.

41. U pogledu „postupovnih zahtjeva”, Odbor preporučuje da njemačka nadzorna tijela:

1) izmijene članak 7.1. tako da sadrži izričito upućivanje na obvezu certifikacijskog tijela da poštuje dodatne zahtjeve

2) uključe upućivanje na primjenu Europskog pečata za zaštitu podataka

3) usklade tekst u članku 7.2. sa smjernicama dodavanjem upućivanja na ugovor(e) s voditeljem/izvršiteljem obrade

4) uključe u članak 7.4. obvezu certifikacijskog tijela da opiše dostatne metode ocjenjivanja za procjenu usklađenosti postup(a)ka obrade s kriterijima za certifikaciju

5) pojasne u članku 7.4. da trajanje valjanosti certifikata o sukladnosti s Općom uredbom o zaštiti podataka ne smije biti uvjetovano valjanošću drugih vrsta certifikata

6) uključe u članak 7.11. obvezu certifikacijskog tijela da prihvati odluke i naredbe njemačkih nadzornih tijela o povlačenju ili neizdavanju certifikata nekom podnositelju ako zahtjevi za certifikaciju više nisu ispunjeni.

4 ZAVRŠNE NAPOMENE

42. Ovo je mišljenje upućeno njemačkim nadzornim tijelima na razini države i saveznih pokrajina i bit će objavljeno u skladu s člankom 64. stavkom 5. točkom (b) Opće uredbe o zaštiti podataka.

43. U skladu s člankom 64. stavcima 7. i 8. Opće uredbe o zaštiti podataka, njemačka nadležna tijela dužna su priopćiti Predsjednici elektroničkim putem u roku od dva tjedna od primitka mišljenja hoće li izmijeniti svoj nacrt odluke ili će ga zadržati. U istom su roku dužna dostaviti izmijenjeni nacrt odluke ili, ako se ne namjeravaju pridržavati mišljenja Odbora, dostaviti odgovarajuće razloge zbog kojih se ne namjeravaju pridržavati ovog mišljenja, u cijelosti ili u dijelu.

44. Njemačka nadzorna tijela dužna su priopćiti konačnu odluku Odboru radi uključivanja u evidenciju odluka koje podliježu mehanizmu konzistentnosti, u skladu s člankom 70. stavkom 1. točkom (y) Opće uredbe o zaštiti podataka.

Doneseno

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)

Doneseno