Smjernice

Smjernice 4/2018 o akreditaciji certifikacijskih tijela u skladu s člankom 43. Opće uredbe o zaštiti podataka (2016/679)

Donesene 4. prosinca 2018.

Sadržaj

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 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,

DONIO JE SLJEDEĆE SMJERNICE:

1 UVOD

Općom uredbom o zaštiti podataka (Uredba (EU) 2016/679) („GDPR"), koja je stupila na snagu 25. svibnja 2018., utvrđuje se modernizirani okvir za zaštitu podataka u Europi koji se temelji na odgovornosti i poštovanju temeljnih prava. Za taj novi okvir važno je donijeti niz mjera kojima se pojednostavnjuje poštovanje odredbi Opće uredbe o zaštiti podataka. Tim su mjerama obuhvaćeni obvezni zahtjevi u posebnim okolnostima (uključujući imenovanje službenika za zaštitu podataka i provedbu procjena učinka na zaštitu podataka) i dobrovoljne mjere kao što su kodeks ponašanja i mehanizmi certificiranja.

U okviru uvođenja mehanizama certificiranja i pečata i oznaka za zaštitu podataka, u članku 43. stavku 1. Opće uredbe o zaštiti podataka od država članica zahtijeva se da osiguraju da je certifikacijska tijela koja izdaju certifikate na temelju članka 42. stavka 1. akreditiralo nadležno nadzorno tijelo ili nacionalno akreditacijsko tijelo ili oba ta tijela. 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.

Smislenim mehanizmima certificiranja može se poboljšati usklađenost s Općom uredbom o zaštiti podataka i transparentnost za ispitanike te odnosi među poduzećima (B2B), primjerice odnosi između voditelja obrade i izvršitelja obrade. Voditelji i izvršitelji obrade podataka imat će koristi od potvrđivanja koje provodi neovisna treća strana za potrebe dokazivanja usklađenosti njihovih postupaka obrade.[1]

U tom kontekstu Europski odbor za zaštitu podataka potvrđuje da je potrebno izdati smjernice u vezi s akreditacijom. Posebna vrijednost i svrha akreditacije proizlazi iz činjenice da se njome pruža autoritativna izjava o stručnosti certifikacijskih tijela kojom se omogućuje stvaranje povjerenja u mehanizam certificiranja.

Cilj je smjernica pružiti upute o tome kako tumačiti i provesti odredbe članka 43. Opće uredbe o zaštiti podataka. Konkretno, njima se nastoji pomoći državama članicama, nadzornim tijelima i nacionalnim akreditacijskim tijelima da uspostave dosljednu i usklađenu osnovu za akreditaciju certifikacijskih tijela koja izdaju certifikate u skladu s Općom uredbom o zaštiti podataka.

[1] U uvodnoj izjavi 100. Opće uredbe o zaštiti podataka navodi se da se uvođenjem mehanizama certificiranja može povećati transparentnost i usklađenost s Uredbom i tako omogućiti ispitanicima brzu procjenu razine zaštite podataka za relevantne proizvode i usluge.

2 PODRUČJE PRIMJENE SMJERNICA

Ovim se smjernicama:

- utvrđuje svrha akreditacije u kontekstu Opće uredbe o zaštiti podataka;
- objašnjavaju načini koji su na raspolaganju za akreditaciju certifikacijskih tijela u skladu s člankom 43. stavkom 1. i utvrđuju ključna pitanja koja je potrebno uzeti u obzir;
- osigurava okvir za utvrđivanje dodatnih zahtjeva za akreditaciju kad akreditaciju provodi nacionalno akreditacijsko tijelo i
- osigurava okvir za utvrđivanje zahtjeva za akreditaciju kad akreditaciju provodi nadzorno tijelo.

Smjernice ne predstavljaju priručnik o postupcima za akreditaciju certifikacijskih tijela u skladu s Općom uredbom o zaštiti podataka. Njima se ne razvija novi tehnički standard za akreditaciju certifikacijskih tijela za potrebe Opće uredbe o zaštiti podataka.

Smjernice se upućuju:

- državama članicama, koje moraju zajamčiti da je certifikacijska tijela akreditiralo nadzorno tijelo i/ili nacionalno akreditacijsko tijelo;
- nacionalnim akreditacijskim tijelima koja provode akreditaciju certifikacijskih tijela u skladu s člankom 43. stavkom 1. točkom (b);
- nadležnom nadzornom tijelu koje utvrđuje „dodatne zahtjeve" uz zahtjeve iz norme ISO/IEC 17065/2012[2] kad akreditaciju provodi nacionalno akreditacijsko tijelo u skladu s člankom 43. stavkom 1. točkom (b);
- Europskom odboru za zaštitu podataka pri davanju mišljenja o zahtjevu za akreditaciju i odobravanju tog zahtjeva koji određuju nadležna nadzorna tijela u skladu s člankom 43. stavkom 3., člankom 70. stavkom 1. točkom (p) i člankom 64. stavkom 1. točkom (c);
- nadležnom nadzornom tijelu koje određuje zahtjeve za akreditaciju kad akreditaciju provodi nadzorno tijelo u skladu s člankom 43. stavkom 1. točkom (a);
- drugim dionicima kao što su potencijalna certifikacijska tijela ili vlasnici programa certificiranja koji osiguravaju kriterije i postupke certificiranja[3].

Definicije

Sljedećim definicijama nastoji se promicati zajedničko razumijevanje osnovnih elemenata postupka akreditacije. Treba ih smatrati referentnim točkama te imati na umu da one ne predstavljaju nepobitne tvrdnje. Te se definicije temelje na postojećim regulatornim okvirima i normama, posebno na relevantnim odredbama Opće uredbe o zaštiti podataka i norme ISO/IEC 17065/2012.

---

[2] Međunarodna organizacija za normizaciju: Ocjenjivanje sukladnosti – zahtjevi za tijela koja provode certifikaciju proizvoda, procesa i usluga.

[3] Nositelj programa organizacija je koju je moguće identificirati i koja je postavila kriterije certificiranja i zahtjeve prema kojima se ocjenjuje sukladnost. Akreditaciju izdaje organizacija koja provodi procjene (članak 43. stavak 4.) prema zahtjevima programa certificiranja i izdaje certifikate (tj. certifikacijsko tijelo, također poznato kao tijelo za ocjenjivanje sukladnosti). Organizacija koja provodi procjene mogla bi biti ista organizacija koja je razvila program i koja je njegov vlasnik, ali mogu postojati slučajevi u kojima je jedna organizacija vlasnik programa, a druga (ili više njih) provodi procjene.

Za potrebe ovih smjernica upotrebljavaju se sljedeće definicije:

za „akreditaciju" certifikacijskih tijela vidjeti odjeljak 3. o tumačenju akreditacije u smislu članka 43. Opće uredbe o zaštiti podataka;

„dodatni zahtjevi" znači zahtjevi koje utvrđuje nadzorno tijelo koje je nadležno i u odnosu na koje se provodi akreditacija[4];

„certifikacija" znači procjena i nepristrano potvrđivanje treće strane[5] da je dokazano ispunjavanje kriterija za certificiranje;

„certifikacijsko tijelo" znači tijelo[6] treće strane za ocjenjivanje sukladnosti[7] koje upravlja mehanizmima certificiranja[8];

„program certificiranja" znači sustav certificiranja koji se odnosi na određene proizvode, procese i usluge na koje se primjenjuju isti posebni zahtjevi, posebna pravila i postupci;[9]

„kriteriji" ili kriteriji certificiranja znači kriteriji prema kojima se provodi certifikacija (ocjenjivanje sukladnosti);[10]

„nacionalno akreditacijsko tijelo" znači jedino tijelo u državi članici imenovano u skladu s Uredbom (EZ-a) br. 765/2008 Europskog parlamenta i Vijeća koje provodi akreditaciju s ovlaštenjem koje mu je dala država[11].

3 TUMAČENJE „AKREDITACIJE" ZA POTREBE ČLANKA 43. OPĆE UREDBE O ZAŠTITI PODATAKA

Općom uredbom o zaštiti podataka ne definira se akreditiranje. Člankom 2. stavkom 10. Uredbe (EZ) br. 765/2008, kojim se utvrđuju opći zahtjevi za akreditaciju, akreditacija se definira kao

„potvrđivanje od strane nacionalnoga akreditacijskog tijela da tijelo za ocjenjivanje sukladnosti zadovoljava zahtjeve utvrđene usklađenim normama i, kad je to primjenjivo, neke druge dodatne zahtjeve, uključujući one utvrđene u odgovarajućim sektorskim programima, za provedbu posebnih radnji za ocjenjivanje sukladnosti."

U skladu s normom ISO/IEC 17011

---

[4] Članak 43. stavci 1., 3. i 6.

[5] Imajte na umu da je u skladu s normom ISO 17000 potvrđivanje treće strane (certifikacija) „primjenjiva na sve predmete ocjenjivanja sukladnosti" (5.5.) „osim na sama tijela za ocjenjivanje sukladnosti na koja se primjenjuje akreditacija" (5.6.).

[6] Vidjeti normu ISO 17000, odjeljak 2.5: „tijelo koje obavlja usluge ocjenjivanja sukladnosti"; ISO 17011: „tijelo koje obavlja usluge ocjenjivanja sukladnosti i koje može biti predmet akreditacije"; ISO 17065, odjeljak 3.12.

[7] Radnje ocjenjivanja sukladnosti treće strane provodi organizacija koja je neovisna o osobi ili organizaciji koja pruža predmet akreditacije i o interesu korisnika za taj predmet, vidjeti normu ISO 17000, odjeljak 2.4.

[8] Članak 42. stavak 1., članak 42. stavak 5. Opće uredbe o zaštiti podataka.

[9] Vidjeti odjeljak 3.9 u vezi s Prilogom B normi ISO 17065.

[10] Vidjeti članak 42. stavak 5.

[11] Vidjeti članak 2. stavak 11. Uredbe (EZ) br. 765/2008/EC.

„akreditacija se odnosi na potvrđivanje treće strane u vezi s tijelom za ocjenjivanje sukladnosti kojim se službeno dokazuje njegova nadležnost za obavljanje određenih zadaća ocjenjivanja sukladnosti".

Člankom 43. stavkom 1. predviđa se sljedeće:

„Ne dovodeći u pitanje zadaće i ovlasti nadležnog nadzornog tijela iz članaka 57. i 58., certifikacijska tijela s odgovarajućim stupnjem stručnosti iz područja zaštite podataka, nakon što se o tome obavijesti nadležno tijelo kako bi ono moglo prema potrebi izvršavati svoje ovlasti na temelju članka 58. stavka 2. točke (h), izdaje i obnavlja certificiranje. Države članice osiguravaju da je ta certifikacijska tijela akreditiralo jedno ili oba sljedeća tijela:

(a) nadzorno tijelo koje je nadležno u skladu s člankom 55. ili člankom 56.;
(b) nacionalno akreditacijsko tijelo imenovano u skladu s Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća u skladu s normom ISO/IEC 17065/2012 i s dodatnim zahtjevima koje određuje nadzorno tijelo koje je nadležno u skladu s člankom 55. ili člankom 56."

U pogledu Opće uredbe o zaštiti podataka, zahtjevi za akreditaciju temeljit će se na:

- normi ISO/IEC 17065/2012 i „dodatnim zahtjevima" koje određuje nadzorno tijelo nadležno u skladu s člankom 43. stavkom 1. točkom (b), ako akreditaciju provodi nacionalno akreditacijsko tijelo, i nadzorno tijelo, ako samo provodi akreditaciju.

U oba slučaja konsolidirani uvjeti moraju obuhvaćati zahtjeve navedene u članku 43. stavku 2.

Europski odbor za zaštitu podataka priznaje da je svrha akreditacije pružiti autoritativnu izjavu o nadležnosti tijela za obavljanje certifikacije (radnje ocjenjivanja sukladnosti)[12]. Akreditacija u smislu Opće uredbe o zaštiti podataka podrazumijeva sljedeće:

potvrđivanje[13] od strane nacionalnoga akreditacijskog tijela i/ili nadzornog tijela da je certifikacijsko tijelo[14] kvalificirano provesti certifikaciju u skladu s člancima 42. i 43. Opće uredbe o zaštiti podataka, uzimajući u obzir normu ISO/IEC 17065/2012 i dodatne zahtjeve koje je uspostavilo nadzorno tijelo ili Odbor.

4 AKREDITACIJA U SKLADU S ČLANKOM 43. STAVKOM 1. OPĆE UREDBE O ZAŠTITI PODATAKA

Člankom 43. stavkom 1. priznaje se da postoji nekoliko mogućnosti za akreditaciju certifikacijskih tijela. Općom uredbom o zaštiti podataka zahtijeva se da nadzorna tijela i države članice definiraju postupak akreditacije certifikacijskih tijela. Ovim se odjeljkom utvrđuju načini za akreditaciju navedeni u članku 43.

[12] Vidjeti uvodnu izjavu 15. Uredbe (EZ) br. 765/2008/EZ.
[13] Vidjeti članak 2. stavak 10. Uredbe (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište.
[14] Vidjeti definiciju pojma „akreditacija" u skladu s normom ISO 17011.

4.1 Uloga država članica

Člankom 43. stavkom 1. zahtijeva se od država članica *da osiguraju* da su certifikacijska tijela akreditirana, ali se dopušta da svaka država članica utvrdi tko bi trebao biti odgovoran za provođenje ocjenjivanja koje prethodi akreditaciji. Na temelju članka 43. stavka 1. dostupne su tri mogućnosti, odnosno akreditaciju može provoditi:

(1) samo nadzorno tijelo, na temelju vlastitih zahtjeva;
(2) samo nacionalno akreditacijsko tijelo imenovano u skladu s Uredbom (EZ) br. 765/2008 i u skladu s normom ISO/IEC 17065/2012 te s dodatnim zahtjevima koje određuje nadležno nadzorno tijelo ili
(3) nadzorno tijelo i nacionalno akreditacijsko tijelo (te u skladu sa svim zahtjevima navedenima u prethodnom odjeljku 2.).

Pojedina država članica odlučuje hoće li nacionalno akreditacijsko tijelo ili nadzorno tijelo, ili oba tijela zajedno, provoditi te akreditacijske djelatnosti, ali u svakom slučaju potrebno je zajamčiti odgovarajuće resurse[15].

4.2 Interakcija s Uredbom (EZ) 765/2008

Europski odbor za zaštitu podataka primjećuje da se člankom 2. stavkom 11. Uredbe (EZ) br. 765/2008 nacionalno akreditacijsko tijelo definira kao „jedino tijelo u državi članici koje provodi akreditaciju s ovlaštenjem koje mu je dala država".

Može se smatrati da članak 2. stavak 11. nije u skladu s člankom 43. stavkom 1. Opće uredbe o zaštiti podataka, kojim se dopušta da akreditaciju provodi tijelo koje nije nacionalno akreditacijsko tijelo države članice. Europski odbor za zaštitu podataka smatra da se zakonodavstvom EU-a namjeravalo odstupiti od općeg načela da akreditaciju provodi isključivo nacionalno tijelo za akreditaciju, dajući nadzornim tijelima iste ovlasti u pogledu akreditacije certifikacijskih tijela. Stoga je članak 43. stavak 1. *lex specialis* u odnosu na članak 2. stavak 11. Uredbe 765/2008.

4.3 Uloga nacionalnog akreditacijskog tijela

Člankom 43. stavkom 1. točkom (b) predviđa se da nacionalno akreditacijsko tijelo provodi akreditaciju certifikacijskih tijela u skladu s normom ISO/IEC 17065/2012 i dodatnim zahtjevima koje je utvrdilo nadležno nadzorno tijelo.

Radi jasnoće, Europski odbor za zaštitu podataka napominje da posebna upućivanja na članak 43. stavak 1. točku (b) podrazumijevaju da se „ti zahtjevi" odnose na „dodatne uvjete" koje određuje nadležno nadzorno tijelo u skladu s člankom 43. stavkom 1. točkom (b) i zahtjeve utvrđene u članku 43. stavku 2.

U postupku provođenja akreditacije nacionalna akreditacijska tijela primjenjuju dodatne zahtjeve koje utvrđuju nadzorna tijela.

Certifikacijsko tijelo s važećom akreditacijom u skladu s normom ISO/IEC 17065/2012 za programe certificiranja koji nisu povezani s Općom uredbom o zaštiti podataka koje želi proširiti opseg svoje akreditacije kako bi se njome obuhvatili certifikati koji se izdaju u skladu s Općom uredbom o zaštiti

[15] Vidjeti članak 4. stavak 9. Uredbe (EZ) 765/2008.

podataka morat će ispuniti dodatne uvjete koje određuje nadzorno tijelo ako akreditaciju provodi nacionalno akreditacijsko tijelo. Ako akreditaciju za certificiranje u okviru Opće uredbe o zaštiti podataka pruža samo nadležno nadzorno tijelo, certifikacijsko tijelo koje podnosi zahtjev za akreditaciju mora ispunjavati zahtjeve koje određuje nadležno nadzorno tijelo.

4.4 Uloga nadzornog tijela

Europski odbor za zaštitu podataka ističe da se člankom 57. stavkom 1. točkom (q) predviđa da nadzorno tijelo *provodi* akreditaciju certifikacijskog tijela u skladu s člankom 43. kao „zadaću nadzornog tijela" u skladu s člankom 57., a člankom 58. stavkom 3. točkom (e) predviđa se da nadzorno tijelo ima ovlasti u vezi s odobravanjem te savjetodavne ovlasti akreditirati certifikacijska tijela u skladu s člankom 43. Tekstom članka 43. stavka 1. osigurava se određena fleksibilnost, a akreditacijsku funkciju nadzornog tijela potrebno je tumačiti kao zadaću samo ako je to prikladno. Za objašnjavanje te točke može se primijeniti pravo države članice. Međutim, u postupku akreditacije koju provodi nacionalno akreditacijsko tijelo člankom 43. stavkom 2. točkom (a) zahtijeva se da certifikacijsko tijelo nadležnom nadzornom tijelu na zadovoljavajući način dokaže svoju neovisnost i stručnost u predmetu certificiranja koje pruža.[16]

Ako država članica propisuje da certifikacijska tijela mora akreditirati nadzorno tijelo, nadzorno tijelo treba uspostaviti zahtjeve za akreditaciju, uključujući, ali ne ograničavajući se na, zahtjeve navedene u članku 43. stavku 2. U usporedbi s obvezama koje se odnose na akreditaciju certifikacijskog tijela koju provode nacionalna akreditacijska tijela, u članku 43. pruža se manje uputa o zahtjevima za akreditaciju kad nadzorno tijelo samo provodi akreditaciju. Kako bi se pridonijelo usklađenom pristupu akreditaciji, kriteriji 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.

Ako država članica propisuje da certifikacijska tijela moraju akreditirati nacionalna akreditacijska tijela, nadzorno tijelo trebalo bi odrediti dodatne zahtjeve kojima se dopunjuju postojeće konvencije u području akreditacija predviđene Uredbom (EZ) 765/2008 (pri čemu se članci od 3. do 14. odnose na organizaciju i akreditaciju tijela za ocjenjivanje sukladnosti) i tehnička pravila kojima se opisuju metode i postupci certifikacijskih tijela. S obzirom na to, u Uredbi (EZ) 765/2008 predviđaju se dodatne smjernice: člankom 2. stavkom 10. definira se akreditacija i upućuje se na „usklađene norme" i „neke druge dodatne zahtjeve, uključujući one utvrđene u odgovarajućim sektorskim programima". Iz toga proizlazi da dodatni zahtjevi koje je uspostavilo nadzorno tijelo trebaju obuhvaćati posebne zahtjeve i biti usmjereni na olakšavanje procjene, između ostaloga neovisnosti i razine stručnosti iz područja zaštite podataka koju posjeduju certifikacijska tijela, primjerice, njihovu sposobnost ocjenjivanja i odobravanja postupaka obrade osobnih podataka koje provode voditelj obrade i izvršitelj obrade u skladu s člankom 42. stavkom 1. Time je obuhvaćena stručnost potrebna za sektorske programe te u pogledu zaštite temeljnih prava i sloboda fizičkih osoba, osobito njihova prava na zaštitu osobnih podataka.[17] Prilogom ovim Smjernicama može se pridonijeti informiranju nadležnih nadzornih tijela pri

[16] Dodatni uvjeti koje je utvrdilo nadzorno tijelo u skladu s člankom 43. stavkom 1. točke (b) trebaju sadržavati zahtjeve u pogledu neovisnosti i stručnosti. Vidjeti i Prilog 1. Smjernicama.
[17] Članak 1. stavak 2. Opće uredbe o zaštiti podataka.

utvrđivanju „dodatnih zahtjeva” u skladu s člankom 43. stavkom 1. točkom (b) i člankom 43. stavkom 3.

Člankom 43. stavkom 6. predviđa se da „nadzorno tijelo u lako dostupnom obliku objavljuje zahtjeve iz stavka 3. ovog članka i kriterije certificiranja iz članka 42. stavka 5.”. Stoga se, kako bi se zajamčila transparentnost, objavljuju svi kriteriji i zahtjevi koje odobrava nadzorno tijelo. U pogledu kvalitete certifikacijskih tijela i povjerenja u njih bilo bi poželjno da su svi zahtjevi za akreditaciju lako dostupni javnosti.

4.5 Nadzorno tijelo koje djeluje kao certifikacijsko tijelo

Člankom 42. stavkom 5. predviđa se da nadzorno tijelo može izdati certifikate, ali Općom uredbom o zaštiti podataka ne zahtijeva se njegova akreditacija kako bi ispunilo zahtjeve u skladu s Uredbom (EZ) 765/2008. Europski odbor za zaštitu podataka ističe da u skladu s člankom 43. stavkom (1) točkom (a), a posebno člankom 58. stavkom 2. točkom (h), člankom 58. stavkom 3. točkama (a), (e) i (f) nadzorna tijela imaju ovlasti za provođenje akreditacije i certifikacije te istodobno pružanje savjeta i, prema potrebi, povlačenje certifikata ili da certifikacijskim tijelima mogu naložiti da ne izdaju certifikate.

U nekim situacijama može biti primjereno ili potrebno odvojiti uloge i dužnosti u području akreditacije i certifikacije, primjerice ako u državi članici istodobno postoje nadzorno tijelo i druga certifikacijska tijela te svako od tih tijela izdaje isti niz certifikata. Nadzorno tijelo stoga bi trebalo poduzeti dostatne organizacijske mjere za odvajanje zadaća koje se provode u skladu s Općom uredbom o zaštiti podataka radi učvršćivanja i olakšavanja mehanizama certificiranja te istodobno poduzeti mjere predostrožnosti kako bi se izbjegli sukobi interesa koji bi mogli proizaći iz tih zadaća. Osim toga, države članice i nadzorna tijela trebali bi pri izradi nacionalnog prava i postupaka u vezi s akreditacijom i certificiranjem u skladu s Općom uredbom o zaštiti podataka uzeti u obzir usklađivanje na europskoj razini.

4.6 Zahtjevi za akreditaciju

U Prilogu ovim Smjernicama pružaju se upute o načinu utvrđivanja dodatnih zahtjeva za akreditaciju. Njime se utvrđuju relevantne odredbe u Općoj uredbi o zaštiti podataka i predlažu zahtjevi koje bi nadzorna tijela i nacionalna akreditacijska tijela trebala razmotriti kako bi se zajamčila usklađenost s Općom uredbom o zaštiti podataka.

Kao što je prethodno utvrđeno, ako certifikacijska tijela akreditira nacionalno akreditacijsko tijelo u skladu s Uredbom (EZ) 765/2008, norma ISO/IEC 17065/2012 postaje relevantna norma akreditacije koja se dopunjava dodatnim zahtjevima koje utvrđuje nadzorno tijelo. Člankom 43. stavkom 2. odražavaju se opće odredbe norme ISO/IEC 17065/2012 s obzirom na zaštitu temeljnih prava u skladu s Općom uredbom o zaštiti podataka. U okviru iz Priloga članak 43. stavak 2. i norma ISO/IEC 17065/2012 upotrebljavaju se kao osnova za utvrđivanje zahtjeva uz dodatne kriterije koji se odnose na procjenu stručnosti certifikacijskih tijela iz područja zaštite podataka i njihove sposobnost za poštovanje prava i sloboda fizičkih osoba u pogledu obrade osobnih podataka kao što je sadržano u Općoj uredbi o zaštiti podataka. Europski odbor za zaštitu podataka ističe da je posebno usredotočen na jamčenje odgovarajuće razine stručnosti certifikacijskih tijela u području zaštite podataka u skladu s člankom 43. stavkom 1.

Dodatni zahtjevi za akreditaciju koje je uspostavilo nadzorno tijelo primjenjivat će se na sva certifikacijska tijela koja podnose zahtjev za akreditaciju. Akreditacijsko tijelo ocijenit će je li to certifikacijsko tijelo sposobno obavljati djelatnosti certificiranja u skladu s dodatnim zahtjevima i

predmetom certifikacije. Utvrđuju se posebni sektori ili područja certificiranja za koje se akreditira certifikacijsko tijelo.

Europski odbor za zaštitu podataka ujedno ističe da je osim zahtjeva iz norme ISO/IEC 17065/2012 potrebna i posebna stručnost iz područja zaštite podataka ako druga, vanjska tijela kao što su laboratoriji ili revizori obavljaju dijelove ili sastavnice djelatnosti certificiranja u ime akreditiranog certifikacijskog tijela. U tim slučajevima ta vanjska tijela nije moguće akreditirati samo na temelju Opće uredbe o zaštiti podataka. Međutim, kako bi se zajamčila prikladnost tih tijela za djelatnost koju obavljaju u ime akreditiranih certifikacijskih tijela, akreditirano certifikacijsko tijelo mora zajamčiti da i vanjsko tijelo raspolaže razinom stručnosti iz područja zaštite podataka koja se zahtijeva od tog akreditiranog tijela u pogledu relevantne djelatnosti koju obavlja te da tu razinu stručnosti može dokazati.

Okvir za utvrđivanje dodatnih zahtjeva za akreditaciju kako je prikazan u Prilogu ovim Smjernicama ne predstavlja priručnik o postupcima za postupak akreditacije koji provodi nacionalno akreditacijsko tijelo ili nadzorno tijelo. Njime se osiguravaju smjernice o strukturi i metodologiji, a time i paket alata za nadzorna tijela radi utvrđivanja dodatnih zahtjeva za akreditaciju.

Za Europski odbor za zaštitu podataka,

Predsjednica

(Andrea Jelinek)