Smjernice

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

Verzija 3.0

4. lipnja 2019.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Doneseno

Povijest inačice

Verzija 3.0	4. lipnja 2019.	Uključuje Prilog 1. (verziju 2.0 Priloga 1. donesenog 4. lipnja 2019. nakon javnog savjetovanja)
Verzija 2.0	4. prosinca 2018.	Donošenje Smjernica nakon javnog savjetovanja – istog je datuma donesen Prilog 1. (verzija 1.0) za javno savjetovanje
Verzija 1.0	6. veljače 2018.	Radna skupina iz članka 29. donosi Smjernice (verziju za javno savjetovanje). Ovu je verziju priznao Europski odbor za zaštitu podataka 25. svibnja 2018.

Sadržaj

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,

uzimajući u razmatranje rezultate javnog savjetovanja o smjernicama održanog u veljači 2018. i o prilogu održanog od 14. prosinca 2018. do 1. veljače 2019., prema članku 70. stavku 4. Opće uredbe o zaštiti podataka,

DONIO JE SLJEDEĆE SMJERNICE:

1 UVOD

1. 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.
2. 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.
3. 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].
4. 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.

[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 procjenu razine zaštite podataka za relevantne proizvode i usluge.

5. 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.

2 PODRUČJE PRIMJENE SMJERNICA

6. 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.

7. 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.

8. 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].

[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.

9. Definicije

10. 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, posebice na relevantnim odredbama Opće uredbe o zaštiti podataka i normi ISO/IEC 17065/2012.

11. Za potrebe ovih smjernica upotrebljavaju se sljedeće definicije:

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

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

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

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

16. „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];

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

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

[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] 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.

[7] 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.

[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.

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

19. 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

20. „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”.

21. U skladu s normom ISO/IEC 17011

22. „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”.

23. Člankom 43. stavkom 1. predviđeno je sljedeće:

24. „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.”

25. 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.

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

27. 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:

28. 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

[12] Vidjeti uvodnu izjavu 15. Uredbe (EZ) br. 765/2008.
[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.

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

29. 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.

4.1 Uloga država članica

30. 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 or
(3) nadzorno tijelo i nacionalno akreditacijsko tijelo (te u skladu sa svim zahtjevima navedenima u prethodnom odjeljku 2.).

31. 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) br. 765/2008

32. 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".

33. 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 (EZ) br. 765/2008.

4.3 Uloga nacionalnog akreditacijskog tijela

34. 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.

---

[14] Vidjeti definiciju pojma „akreditacija" u skladu s normom ISO 17011.
[15] Vidjeti članak 4. stavak 9. Uredbe (EZ) br. 765/2008.

35. Radi jasnoće, Europski odbor za zaštitu podataka napominje da posebno upućivanje na članak 43. stavak 1. točku (b) podrazumijeva 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.

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

37. 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 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

38. 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].

39. 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 dopuniti 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.

40. 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) br. 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

[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.

obzirom na to, u Uredbi (EZ) br. 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 utvrđivanju „dodatnih zahtjeva" u skladu s člankom 43. stavkom 1. točkom (b) i člankom 43. stavkom 3.

41. 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

42. 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) br. 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.

43. 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

44. 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.

45. Kao što je prethodno utvrđeno, ako certifikacijska tijela akreditira nacionalno akreditacijsko tijelo u skladu s Uredbom (EZ) br. 765/2008, norma ISO/IEC 17065/2012 postaje relevantna norma akreditacije koja se dopunjava dodatnim zahtjevima koje utvrđuje nadzorno tijelo.

[17] Članak 1. stavak 2. Opće uredbe o zaštiti podataka.

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 sposobnosti 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.

46. 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.

47. 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.

48. 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.

PRILOG 1.

U Prilogu 1. nalaze se upute za specifikaciju „dodatnih“ zahtjeva za akreditaciju u odnosu na normu ISO/IEC 17065/2012 i u skladu s člankom 43. stavkom 1. točkom (b) i člankom 43. stavkom 3. Opće uredbe o zaštiti podataka.

U ovom se Prilogu nalaze predloženi zahtjevi koje će sastaviti nadzorno tijelo za zaštitu podataka i koji se primjenjuju tijekom akreditacije certifikacijskog tijela koju provodi nacionalno akreditacijsko tijelo ili nadležno nadzorno tijelo[18]. Ove je dodatne zahtjeve potrebno priopćiti Europskom odboru za zaštitu podataka prije odobrenja u skladu s člankom 64 stavkom 1. točkom (c).

Ovaj se Prilog treba tumačiti zajedno s normom ISO/IEC 17065/2012. Brojevi odjeljaka koji se ovdje upotrebljavaju odgovaraju brojevima u normi ISO/IEC 17065/2012. U slučajevima u kojima nadzorna tijela provode akreditaciju u skladu s člankom 43. stavkom 1. točkom (a), dobra bi praksa bila slijediti ovaj pristup gdje je praktično. Time će se podržati akreditacija koja je usklađena u cijelom EU-u.

Bez obzira na sljedeće upute ili nepostojanje uputa o bilo kojoj stavki iz norme ISO/IEC 17065/2012, nadležno nadzorno tijelo može formulirati daljnje dodatne zahtjeve koji se odnose na ove stavke ako su u skladu s nacionalnim pravom.

0 PREFIKS

[Ovaj je odjeljak namijenjen Uvjetima suradnje koji su dogovoreni, ako je primjenjivo, između nacionalnog akreditacijskog tijela i nadležnog nadzornog tijela za zaštitu podataka, npr. o tome tko bi trebao biti odgovoran za primanje prijavnih obrazaca ili o tome kako organizirati priznanje odobrenih kriterija u okviru postupka akreditacije.]

1 PODRUČJE PRIMJENE[19]

Područje primjene norme ISO/IEC 17065/2012 primijenit će se u skladu s Općom uredbom o zaštiti podataka. Dodatne informacije nalaze se u smjernicama o akreditaciji i certifikaciji. Područje primjene mehanizma certificiranja (na primjer, certifikacija postupaka obrade u usluzi u oblaku) treba se uzeti u obzir u procjeni koju provodi nacionalno akreditacijsko tijelo i nadležno nadzorno tijelo tijekom postupka akreditacije, posebice u odnosu na kriterije, stručnost i metodologiju ocjenjivanja. Široko područje primjene norme ISO/IEC 17065/2012 koje obuhvaća proizvode, procese i usluge ne bi trebalo smanjiti zahtjeve Opće uredbe o zaštiti podataka ili prijeći preko njih, npr. mehanizam upravljanja ne može biti jedini element mehanizma certificiranja jer certifikacija mora uključivati obradu osobnih podataka, tj. postupke obrade. U skladu s člankom 42. stavkom 1. Opće uredbe o zaštiti podataka certifikacija je primjenjiva samo na postupke obrade voditelja i izvršitelja obrade.

[18] Za informacije o procesu odobrenja za kriterije certificiranja pogledajte odjeljak 4. smjernica o certificiranju.
[19] Numeriranje se odnosi na normu ISO/IEC 17065/2012.

2 NORMATIVNI IZVORI

Opća uredba o zaštiti podataka ima prednost nad normom ISO/IEC 17065/2012. Ako se u dodatnim zahtjevima ili mehanizmom certificiranja spominju druge ISO norme, one se tumače u skladu sa zahtjevima iz Opće uredbe o zaštiti podataka.

3 POJMOVI I DEFINICIJE

U kontekstu ovog Priloga primjenjuju se pojmovi i definicije smjernica o akreditaciji (WP 261) i certifikaciji (Europski odbor za zaštitu podataka 1/2018) i imaju prednost nad definicijama iz ISO normi.

4 OPĆI ZAHTJEVI ZA AKREDITACIJU

4.1 Pravna i ugovorna pitanja

4.1.1 Pravna odgovornost

Certifikacijsko tijelo bi trebalo moći (u svakom trenutku) dokazati nacionalnom akreditacijskom tijelu ili certificiranom višem savjetniku da ima ažurirane postupke kojima dokazuje usklađenost s pravnim odgovornostima navedenima u uvjetima o akreditaciji, uključujući dodatne zahtjeve u pogledu primjene Uredbe (EU) 2016/679. S obzirom na to da je certifikacijsko tijelo voditelj/izvršitelj obrade, valja imati na umu da će on biti odgovoran za dokazivanje postupaka i mjera koji su usklađeni s Uredbom (EU) 2016/679, posebice u pogledu vođenja i obrade osobnih podataka organizacije klijenta u sklopu certifikacijskog procesa.

Certificirani viši savjetnik može odlučiti dodati daljnje zahtjeve i postupke da bi prije akreditiranja provjerio usklađenost certifikacijskih tijela s Općom uredbom o zaštiti podataka.

4.1.2 Ugovor o certificiranju („CA“)

Sljedećim se točkama dopunjavaju minimalni zahtjevi za ugovor o certificiranju:

Certifikacijsko tijelo dokazuje da se uz zahtjeve iz norme ISO/IEC 17065/2012 njegovim ugovorima o certifikaciji:

1. zahtijeva da se prijavitelj uvijek pridržava općih zahtjeva za certificiranje u smislu točke 4.1.2.2. lit. (a), norme ISO/IEC 17065/2012 i kriterija koje je odobrilo nadležno nadzorno tijelo ili Europski odbor za zaštitu podataka u skladu s člankom 43. stavkom 2. točkom (b) i člankom 42. stavkom 5.;
2. zahtijeva da prijavitelj dozvoli potpunu transparentnost nadležnom nadzornom tijelu u pogledu postupka certificiranja uključujući ugovorno povjerljiva pitanja povezana s usklađenosti sa zaštitom osobnih podataka prema članku 42. stavku 7. i članku 58. stavku 1. točki (c);
3. ne smanjuje odgovornost prijavitelja u pogledu sukladnosti s Uredbom (EU) 2016/679 i ne dovode u pitanje zadaće i ovlasti nadzornih tijela koja su nadležna u skladu s člankom 42. stavkom 5.;
4. zahtijeva da prijavitelj dostavi certifikacijskom tijelu sve podatke i omogući pristup aktivnostima obrade koje su potrebne za provedbu postupka certificiranja u skladu s člankom 42. stavkom 6.;

5. zahtijeva da se prijavitelj pridržava primjenjivih rokova i postupaka. Ugovorom o certificiranju potrebno je odrediti praćenje i pridržavanje rokova i postupaka koji su rezultat, na primjer, certifikacijskog programa ili drugih propisa;
6. u odnosu na točku 4.1.2.2. lit. (c) br. 1. norme ISO/IEC 17065/2012 navode pravila o valjanosti, obnavljanju i povlačenju u skladu s člankom 42. stavkom 7. i člankom 43.stavkom 4., uključujući pravila kojima se postavljaju odgovarajući intervali za ponovno ocjenjivanje ili analizu (redovitost) u skladu s člankom 42. stavkom 7.;
7. dozvoljava se certifikacijskom tijelu da otkrije sve podatke potrebne za odobrenje certifikacije u skladu s člankom 42. stavkom 8. i člankom 43. stavkom 5.;
8. uključuju pravila o potrebnim mjerama opreza za ispitivanje pritužbi u smislu točke 4.1.2.2. lit. (c) br.2., i dodatno, lit. (j), također će sadržavati eksplicitne izjave o strukturi i postupku za upravljanje pritužbama u skladu s člankom 43. stavkom 2. točkom (d);
9. osim minimalnih zahtjeva iz točke 4.1.2.2. norme ISO/IEC 17065/2012, ako posljedice povlačenja ili suspenzije akreditacije za certifikacijsko tijelo utječu na klijenta, u tom se slučaju također trebaju razmotriti posljedice za klijenta
10. zahtijeva da prijavitelj obavijesti certifikacijsko tijelo u slučaju znatnih promjena u njegovoj stvarnoj ili pravnoj situaciji i u njegovim proizvodima, procesima i uslugama iz certifikacije.

4.1.3 Uporaba pečata i oznaka za zaštitu podataka

Certifikati, pečati i oznake mogu se upotrebljavati samo u skladu s člancima 42. i 43. i smjernicama o akreditaciji i certificiranju.

4.2 Upravljanje nepristranosti

Akreditacijsko tijelo pored zahtjeva iz točke 4.2. norme ISO/IEC 17065/2012 osigurava

1. da se certifikacijsko tijelo pridržava dodatnih zahtjeva nadležnog nadzornog tijela (u skladu s člankom 43. stavkom 1. točkom (b))
    - **a.** u skladu s člankom 43. stavkom 2 točkom (a) pruži odvojeni dokaz o njegovoj nezavisnosti. To se posebice primjenjuje na dokaze o financiranju akreditacijskog tijela u mjeri koja se tiče osiguranja nepristranosti;
    - **b.** da njegove zadaće i obveze ne prouzrokuju sukob interesa u skladu s člankom 43. stavkom 2. točkom (e)
2. da certifikacijsko tijelo nije u relevantnoj vezi s klijentom kojeg ocjenjuje.

4.3 Odgovornost i financiranje

Osim zahtjeva iz točke 4.3.1. iz norme ISO/IEC 17065/2012, akreditacijsko tijelo redovito osigurava da certifikacijsko tijelo ima uspostavljene odgovarajuće mjere (npr. osiguranje ili rezerve) za pokrivanje svojih obveza u geografskim regijama u kojima djeluje.

4.4 Nediskriminirajući uvjeti

Nadzorno tijelo može formulirati dodatne zahtjeve ako je to u skladu s nacionalnim pravom.

4.5 Povjerljivost

Nadzorno tijelo može formulirati dodatne zahtjeve ako je to u skladu s nacionalnim pravom.

4.6 Javno dostupne informacije

Akreditacijsko tijelo pored zahtjeva iz točke 4.6. norme ISO/IEC 17065/2012 od certifikacijskog tijela zahtijeva da najmanje

1. sve verzije (aktualne i prethodne) odobrenih kriterija primijenjenih u smislu članka 42. stavka 5. budu objavljene i lako dostupne javnosti, kao i svi certifikacijski postupci, a u kojima će se općenito navesti razdoblje valjanosti
2. podaci o postupcima obrade pritužbi i žalbi budu javno dostupni u skladu s člankom 43. stavkom 2. točkom (d).

5 STRUKTURNI ZAHTJEVI, ČLANAK 43. STAVAK 4. [„ODGOVARAJUĆE“ OCJENJIVANJE]

5.1 Organizacijska struktura i najviše rukovodstvo

Nadzorno tijelo može formulirati dodatne zahtjeve.

5.2 Mehanizmi za zaštitu nepristranosti

Nadzorno tijelo može formulirati dodatne zahtjeve.

6 ZAHTJEVI U VEZI S RESURSIMA

6.1 Osoblje u certifikacijskom tijelu

Akreditacijsko tijelo pored zahtjeva iz odjeljka 6. norme ISO/IEC 17065/2012 osigurava za svako certifikacijsko tijelo da njegovo osoblje:

1. pokaže odgovarajuću i aktualnu stručnost (znanje i iskustvo) u odnosu na zaštitu podataka u skladu s člankom 43. stavkom 1.;
2. ima neovisnost i aktualnu stručnost u pogledu objekta certificiranja u skladu s člankom 43. stavkom 2. točkom (a) i da ne postoji sukob interesa u skladu s člankom 43. stavkom 2. točkom (e);
3. obveže se poštovati kriterije iz članka 42. stavka 5. u skladu s člankom 43. stavkom 2. točkom (b);
4. ima relevantno i odgovarajuće znanje o primjeni zakona o zaštiti podataka te iskustvo u tome;
5. ima relevantno i odgovarajuće znanje o tehničkim i organizacijskim mjerama zaštite podataka kako je relevantno te iskustvo u tome;
6. može dokazati iskustvo u područjima iz dodatnih zahtjeva 6.1.1., 6.1.4. i 6.1.5., posebice

za osoblje s tehničkom stručnosti:

- da imaju kvalifikaciju u relevantnom području tehničke stručnosti minimalne razine 6 Europskog kvalifikacijskog okvira[20] ili priznatu zaštićenu titulu (npr. dipl. ing.) u relevantnoj reguliranoj profesiji ili imaju znatno profesionalno iskustvo.
- *Osoblje odgovorno za odluke o certificiranju* mora imati znatno profesionalno iskustvo u utvrđivanju i provedbi mjera zaštite podataka.
- *Osoblje odgovorno za ocjenjivanje* mora imati profesionalno iskustvo u tehničkoj zaštiti podataka te znanje i iskustvo u usporedivom postupku (npr. certifikacije/revizije) i mora biti registrirano, kako je primjenjivo.

[20] Okvirni alat za usporedbu kvalifikacija dostupan je na https://ec.europa.eu/ploteus/en/compare?

Osoblje mora dokazati da kroz kontinuirani profesionalni razvoj održava znanje iz tehničkih i revizorskih vještina specifično za domenu.

za osoblje s pravnom stručnosti:

- studiji prava na sveučilištu u državi EU-a ili na sveučilištu koje je priznala država koji traju najmanje osam semestara i uključuju akademsku titulu magistra (LL.M.) ili ekvivalentnu, ili znatno profesionalno iskustvo.
- *Osoblje odgovorno za odluke o certificiranju* mora dokazati znatno profesionalno iskustvo u pravu o zaštiti podataka i mora biti registrirano kako to zahtijeva država članica.
- *Osoblje odgovorno za ocjenjivanje* mora dokazati najmanje dvije godine profesionalnog iskustva u pravu o zaštiti podataka te znanje i iskustvo u usporedivim postupcima (npr. certifikacije/revizije) te mora biti registrirano kada to zahtijeva država članica.
    - Osoblje mora dokazati da kroz kontinuirani profesionalni razvoj održava znanje iz tehničkih i revizorskih vještina specifično za domenu.

6.2 Resursi za ocjenjivanje

Nadzorno tijelo može formulirati dodatne zahtjeve ako je to u skladu s nacionalnim pravom.

7 ZAHTJEVI PROCESA, ČLANAK 43. STAVAK 2. TOČKE (C) I (D)

7.1 Općenito

Akreditacijsko tijelo pored zahtjeva iz odjeljka 7.1. norme ISO/IEC 17065/2012 od certifikacijskog tijela zahtijeva da osigura da:

1. certifikacijska tijela budu usklađena s dodatnim zahtjevima nadležnog nadzornog tijela (u skladu s člankom 43. stavkom 1. točkom (b)) pri slanju prijave tako da zadaće i obveze ne uzrokuju sukob interesa u skladu s člankom 43. stavkom 2. točkom (b);
2. obavijeste relevantnog certifikacijskog višeg savjetnika prije nego što neko certifikacijsko tijelo počne upotrebljavati odobreni europski pečat za zaštitu podataka u novoj državi članici iz područnog ureda.

7.2 Prijava

Pored stavke 7.2. norme ISO/IEC 17065/2012 potrebno je zahtijevati da

1. objekt certificiranja (Cilj ocjenjivanja) bude detaljno opisan u prijavi. To ujedno uključuje sučelja i prebacivanje na druge sustave i organizacije, protokole i druga osiguranja;
2. u prijavi bude navedeno upotrebljavaju li se izvršitelji obrade, a kada su izvršitelji obrade prijavitelj, opisat će se njihove odgovornosti i zadaće i prijava će sadržavati relevantne ugovore za voditelja obrade i izvršitelja obrade.

7.3 Analiza prijave

Pored stavke 7.3. norme ISO/IEC 17065/2012 potrebno je zahtijevati da

1. ugovor o certificiranju sadržava obvezujuće metode ocjenjivanja u odnosu na Cilj ocjenjivanja
2. procjena u stavci 7.3. (e) o postojanju dovoljne količine stručnosti u odgovarajućoj mjeri uzme u obzir i tehničku i pravnu stručnost u zaštiti podataka.

7.4 Ocjenjivanje

Pored stavke 7.4. norme ISO/IEC 17065/2012, mehanizmi certificiranja obuhvaćat će opis dostatnih metoda ocjenjivanja za ocjenjivanje sukladnosti postupaka obrade s kriterijima certificiranja, uključujući, na primjer, gdje je primjenjivo:

1. metodu za ocjenjivanje nužnosti i proporcionalnosti postupaka obrade u odnosu na njihovu svrhu i ispitanike u pitanju;
2. metodu za ocjenjivanje pokrivenosti, sastava i ocjenjivanja svih rizika koje razmatra voditelj obrade i izvršitelj obrade u odnosu na pravne posljedice u skladu s člancima 30., 32., 35. i 36. Opće uredbe o zaštiti podataka te u odnosu na definiciju tehničkih i organizacijskih mjera u skladu s člancima 24., 25. i 32. Opće uredbe o zaštiti podataka, u mjeri u kojoj se spomenuti članci primjenjuju na objekt certificiranja i
3. metodu za ocjenjivanje pravnih lijekova, uključujući jamstva, zaštitne mjere i postupke za osiguranje zaštite osobnih podataka u kontekstu obrade koja se pripisuje objektu certificiranja te da bi se pokazalo da su zadovoljeni pravni zahtjevi kako su navedeni u kriterijima i
4. dokumentaciju s metodama i rezultatima.

Od certifikacijskog bi se tijela trebalo zahtijevati da osigura standardizaciju ovih metoda ocjenjivanja te njihovu općenitu primjenjivost. To znači da se usporedive metode ocjenjivanja upotrebljavaju za usporedive Ciljeve ocjenjivanja. Svako odstupanje od tog postupka treba opravdati certifikacijsko tijelo.

Pored stavke 7.4.2. norme ISO/IEC 17065/2012, trebalo bi biti dozvoljeno da ocjenjivanje provode vanjski stručnjaci koje je priznalo certifikacijsko tijelo.

Pored stavke 7.4.5. norme ISO/IEC 17065/2012 trebalo bi zahtijevati da se certificiranje u vezi sa zaštitom podataka u skladu s člancima 42. i 43. Opće uredbe o zaštiti podataka, koje već pokriva objekt certificiranja, može uključiti u trenutačno certificiranje. Međutim, to neće biti dovoljno za potpuno zamjenjivanje (djelomičnih) ocjenjivanja. Certifikacijsko tijelo obvezno je provjeriti sukladnost s kriterijima. U svakom slučaju za priznavanje je potrebno cjelokupno evaluacijsko izvješće ili podaci kojima je omogućeno ocjenjivanje prethodne aktivnosti certificiranja te njezini rezultati. Izjava o certificiranju ili slični certifikati o certificiranju ne bi se smjeli smatrati dovoljnom zamjenom za izvješće.

Pored stavke 7.4.6. norme ISO/IEC 17065/2012, trebalo bi zahtijevati da certifikacijsko tijelo detaljno navede u svom mehanizmu certificiranja način na koji se podacima traženima u stavci 7.4.6. pružaju informacije klijentu (prijavitelju za certificiranje) o nesukladnostima iz mehanizma certifikacije. U tom je kontekstu potrebno definirati najmanje vrstu tih informacija i vrijeme njihova davanja.

Pored stavke 7.4.9. norme ISO/IEC 17065/2012, trebalo bi zahtijevati da dokumentacija bude u potpunosti dostupna nadzornom tijelu za zaštitu podataka na zahtjev.

7.5 Analiza

Pored stavke 7.5. norme ISO/IEC 17065/2012, zahtijevaju se postupci za odobrenja, redovitu analizu i opoziv certifikacija u skladu s člankom 43. stavkom 2 i člankom 43. stavkom 3.

7.6 Odluka o certificiranju

Pored točke 7.6.1. norme ISO/IEC 17065/2012, trebalo bi zahtijevati da certifikacijsko tijelo detaljno navede u svojim postupcima način osiguranja njegove neovisnosti i odgovornosti u pogledu pojedinačnih odluka o certificiranju.

7.7 Dokumentacija za certificiranje

Pored stavke 7.7.1.e norme ISO/IEC 17065/2012 i u skladu s člankom 42. stavkom 7 Opće uredbe o zaštiti podataka, trebalo bi zahtijevati da razdoblje valjanosti certifikacija ne prelazi tri godine.

Pored stavke 7.7.1.e norme ISO/IEC 17065/2012, trebalo bi zahtijevati da se također dokumentira namjeravani nadzor u smislu odjeljka 7.9.

Pored stavke 7.7.1.f norme ISO/IEC 17065/2012, trebalo bi zahtijevati da certifikacijsko tijelo imenuje objekt certificiranja u dokumentaciji za certificiranje (uz navod o statusu verzije i sličnim značajkama, ako je primjenjivo).

7.8 Direktorij certificiranih proizvoda

Pored stavke 7.8. norme ISO/IEC 17065/2012, trebalo bi zahtijevati da certifikacijsko tijelo omogući dostupnima podatke o certificiranim proizvodima, procesima i uslugama na internoj razini te javnoj. Certifikacijsko tijelo će javno objaviti izvršni sažetak evaluacijskog izvješća. Cilj je ovog izvršnog sažetka pridonijeti transparentnosti onog što je certificirano i načina na koji je ocijenjeno. U sažetku će se razjasniti primjerice:

(a) opseg certifikacija i smisleni opis objekta certificiranja

(b) kriteriji certificiranja (uključujući verziju ili funkcionalni status)

(c) metode ocjenjivanja i provedeni testovi i

(d) rezultati.

Pored stavke 7.8. norme ISO/IEC 17065/2012 i u skladu s člankom 43. stavkom 5. Opće uredbe o zaštiti podataka, certifikacijsko tijelo informira nadležna nadzorna tijela o razlozima davanja ili opozivanja tražene certifikacije.

7.9 Nadzor

Pored točaka 7.9.1., 7.9.2. i 7.9.3. norme ISO/IEC 17065/2012 i u skladu s člankom 43. stavkom 2. točkom (c) Opće uredbe o zaštiti podataka, trebalo bi zahtijevati da mjere redovitog nadzora budu obvezne kako bi se certifikacija zadržala tijekom razdoblja nadzora.

7.10 Promjene koje utječu na certifikaciju

Pored točaka 7.10.1. i 7.10.2. norme EN ISO/IEC 17065/2012, promjene koje utječu na certifikaciju koju razmatra certifikacijsko tijelo uključuju sljedeće: izmjene zakona o zaštiti podataka, donošenje delegiranih akata Europske komisije u skladu s člankom 43. stavkom 8. i člankom 43. stavkom 9., odluke Europskog odbora za zaštitu podataka i sudske odluke u pogledu zaštite podataka. Postupci u vezi s promjenama mogli bi uključivati: tranzicijska razdoblja, proces odobrenja pri nadležnom nadzornom tijelu, ponovno ocjenjivanje relevantnog objekta certificiranja i odgovarajuće mjere za opozivanje certifikacije ako certificirani postupak obrade više nije u skladu s ažuriranim kriterijima.

7.11 Istek, smanjenje, suspenzija ili povlačenje certifikacije

Pored poglavlja 7.11.1. norme ISO/IEC 17065/2012, trebalo bi zahtijevati da certifikacijsko tijelo informira nadležno nadzorno tijelo i nacionalno akreditacijsko tijelo, gdje je relevantno, odmah i pisanim putem, o poduzetim mjerama i o nastavku, ograničenjima, suspenziji i povlačenju certifikacije.

Prema članku 58. stavku 2 točki (h) zahtijeva se od certifikacijskog tijela da prihvati odluke i naloge nadležnog nadzornog tijela o povlačenju ili neizdavanju certifikacije klijentu (prijavitelju) ako zahtjevi za certificiranje nisu (više) zadovoljeni.

7.12 Evidencije

Trebalo bi zahtijevati od certifikacijskog tijela da dokumentacija koju drži kod sebe bude potpuna, razumljiva, ažurirana i prikladna za reviziju.

7.13 Pritužbe i žalbe, članak 43. stavak 2 točka (d)

Pored stavke 7.13.1. norme ISO/IEC 17065/2012, trebalo bi zahtijevati da certifikacijsko tijelo definira

(a) tko može uložiti pritužbe ili prigovore

(b) tko ih obrađuje u ime certifikacijskog tijela

(c) koje su verifikacije u ovom kontekstu uspostavljene i

(d) mogućnosti za savjetovanje zainteresiranih strana.

Pored stavke 7.13.2. norme ISO/IEC 17065/2012, trebalo bi zahtijevati da certifikacijsko tijelo definira

(a) kako i kome se ti podaci moraju davati

(b) vremensko ograničenje i

(c) koje je procese potrebno nakon toga započeti.

Pored stavke 7.13.1. norme ISO/IEC 17065/2012, certifikacijsko tijelo mora definirati način osiguranja odvojenosti aktivnosti certificiranja i obrade žalbi i pritužbi.

8 ZAHTJEVI SUSTAVA UPRAVLJANJA

Općeniti je zahtjev sustava upravljanja prema poglavlju 8. norme ISO/IEC 17065/2012 da se na neovisnoj razini dokumentira, ocijeni, kontrolira i nadzire provedba svih zahtjeva iz prethodnih poglavlja u okviru područja primjene prijave za mehanizam certificiranja.

Osnovno je načelo upravljanja definirati sustav kojim se ciljevi djelotvorno i učinkovito postavljaju, posebice: provedbu usluge certificiranja – s pomoću odgovarajućih specifikacija. Za to je potrebno da certifikacijsko tijelo omogući transparentnost i dokazivost provedbe zahtjeva za akreditaciju te da je uvijek usklađeno s njima.

U tu se svrhu u sustavu upravljanja mora navesti metodologija za zadovoljavanje i kontroliranje tih zahtjeva u skladu s propisima o zaštiti podataka te za njihovu neprestanu provjeru kod samog akreditacijskog tijela.

Navedena načela upravljanja i njihova dokumentirana provedba moraju biti transparentni te ih akreditirano certifikacijsko tijelo mora otkriti u akreditacijskom postupku u skladu s člankom 58., a nakon toga na zahtjev nadzornog tijela za zaštitu podataka u bilo kojem trenutku tijekom ispitivanja u obliku revizije u vezi sa zaštitom podataka u skladu s člankom 58. stavkom 1. točkom (b) ili revizije certifikacija koje su izdane u skladu s člankom 42. stavkom 7. prema članku 58. stavku 1. točki (c).

Posebice, akreditirano certifikacijsko tijelo mora stalno i redovito objavljivati informacije o tome koje je certificiranje provedeno i na kojoj osnovi (ili mehanizme ili programe certificiranja), koliko su dugo certifikacije valjane i prema kojem okviru i uvjetima (uvodna izjava 100.).

8.1 Opći zahtjevi sustava upravljanja

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

8.2 Dokumentacija sustava upravljanja

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

8.3 Upravljanje dokumentima

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

8.4 Nadzor nad evidencijama

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

8.5 Analiza koju provodi rukovodstvo

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

8.6 Unutarnje revizije

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

8.7 Korektivne mjere

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

8.8 Preventivne mjere

Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

9 DALJNJI DODATNI ZAHTJEVI21

9.1 Ažuriranje metoda ocjenjivanja

Certifikacijsko tijelo uspostavlja postupke za vođenje ažuriranja metoda ocjenjivanja za prijavu u kontekstu ocjenjivanja sukladno točki 7.4. Ažuriranje je potrebno provesti tijekom promjena u pravnom okviru, relevantnom riziku, posljednjim dostignućima i troškovima provedbe tehničkih i organizacijskih mjera.

9.2 Održavanje stručnosti

Certifikacijska tijela uspostavljaju postupke da bi osigurala obuku svojih zaposlenika s ciljem nadogradnje njihovih vještina, uzimajući u obzir razvoje navedene u točki 9.1.

9.3 Odgovornosti i nadležnosti

9.3.1 Komunikacija između certifikacijskog tijela i njegovih klijenata

Uspostavit će se postupci za provedbu odgovarajućih postupaka i komunikacijskih struktura između certifikacijskog tijela i njegova klijenta. To uključuje:

1. vođenje dokumentacije o zadaćama i odgovornostima koje vrši akreditirano certifikacijsko tijelo u svrhe

[21] Nadležno nadzorno tijelo može navesti i dodati daljnje dodatne zahtjeve ako su u skladu s nacionalnim pravom.

a. zahtjeva za informacije ili
b. da bi se omogućio kontakt u slučaju pritužbe na certifikaciju

2. vođenje procesa prijava u svrhe
    a. davanja informacija o stanju prijave
    b. ocjenjivanje od strane nadležnog nadzornog tijela u pogledu
        i. povratnih informacija
        ii. odluka nadležnog nadzornog tijela.

9.3.2 Dokumentacija o aktivnostima ocjenjivanja

Nadzorno tijelo može formulirati dodatne zahtjeve.

9.3.3 Upravljanje obradom pritužbi

Obrada pritužbi čini sastavni dio sustava upravljanja kojim se posebice provode zahtjevi iz točaka 4.1.2.2. lit. (c), 4.1.2.2. lit. (j), 4.6. lit. (d) i 7.13. norme ISO/IEC 17065/2012.

Potrebno je s nadležnim nadzornim tijekom podijeliti relevantne pritužbe i prigovore.

9.3.4 Upravljanje povlačenjem

Postupci u slučaju suspenzije ili povlačenja akreditacije integrirani su u sustav upravljanja certifikacijskog tijela, uključujući obavijesti klijentima.