Usmernenia

Usmernenia 4/2018 o akreditácii certifikačných subjektov podľa článku 43 všeobecného nariadenia o ochrane údajov (2016/679)

Verzia 3.0

4. jún 2019

Prijaté

História verzií

Verzia 3.0	4. jún 2019	Zahrnutie prílohy 1 (verzia 2.0 prílohy 1 prijatá 4. júna 2019 po verejnej konzultácii)
Verzia 2.0	4. decembra 2018	Prijatie usmernení po verejnej konzultácii – k tomu istému dátumu bola prijatá na verejné konzultácie príloha 1 (verzia 1.0)
Verzia 1.0	6. februára 2018	Prijatie usmernení WP29 (verzia na uverejnenie a konzultácie). Túto verziu schválil EDPB 25. mája 2018.

Obsah

Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679/EÚ z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES,

Po preskúmaní výsledkov verejnej konzultácie o usmerneniach, ktorá sa uskutočnila vo februári 2018, a o prílohe, ktorá sa uskutočnila v období od 14. decembra 2018 do 1. februára 2019, na základe článku 70 ods. 4 všeobecného nariadenia o ochrane údajov

PRIJAL TIETO USMERNENIA

1 ÚVOD

1. Všeobecné nariadenie o ochrane údajov [nariadenie (EÚ) 2016/679] (ďalej len „všeobecné nariadenie o ochrane údajov“), ktoré nadobudlo účinnosť 25. mája 2018, stanovuje modernizovaný rámec ochrany údajov v Európe, ktorý je v súlade so zásadou zodpovednosti a so základnými právami. Ústredným prvkom tohto nového rámca je celý rad opatrení, ktoré uľahčujú dodržiavanie ustanovení všeobecného nariadenia o ochrane údajov. Patria k nim povinné požiadavky pre prípad určitých konkrétnych okolností (napr. prípad vymenovania zodpovedných osôb a vykonávania posúdení vplyvu na ochranu údajov) a dobrovoľné opatrenia, ako sú napr. kódexy správania a certifikačné mechanizmy.

2. Ako súčasť zavedenia certifikačných mechanizmov a pečatí a značiek ochrany údajov sa v článku 43 ods. 1 všeobecného nariadenia o ochrane údajov od členských štátov vyžaduje, aby zabezpečili, aby certifikačné subjekty udeľujúce certifikáciu podľa článku 42 ods. 1 boli akreditované buď od príslušného dozorného orgánu, alebo od národného akreditačného orgánu alebo od oboch z týchto orgánov. Ak akreditáciu vykonáva národný akreditačný orgán v súlade s normou ISO/IEC 17065/2012, musia sa uplatňovať aj dodatočné požiadavky stanovené príslušným dozorným orgánom.

3. Zmysluplné certifikačné mechanizmy môžu zlepšiť dodržiavanie všeobecného nariadenia o ochrane údajov a transparentnosť vo vzťahu k dotknutým osobám a v oblasti vzťahov medzi podnikmi (B2B), napríklad medzi prevádzkovateľmi a sprostredkovateľmi. Prevádzkovatelia a sprostredkovatelia budú môcť využiť nezávislú atestáciu tretích strán na účely preukázania zhody ich spracovateľských operácií[1].

4. V tejto súvislosti Európsky výbor pre ochranu údajov (EDPB) uznáva, že je potrebné poskytnúť usmernenia týkajúce sa akreditácie. Konkrétna hodnota a účel akreditácie spočíva v tom, že

[1] V odôvodnení 100 všeobecného nariadenia o ochrane údajov sa uvádza, že vytvorenie certifikačných mechanizmov môže viesť k zlepšeniu transparentnosti a posilneniu súladu s nariadením a môže dotknutým osobám umožniť posúdiť úroveň ochrany údajov v prípade relevantných produktov a služieb.

poskytuje vierohodné vyhlásenie o spôsobilosti certifikačných subjektov, ktoré umožňuje vytváranie dôvery v certifikačný mechanizmus.

5. Cieľom usmernení je poskytnúť návod, ako interpretovať a vykonávať ustanovenia článku 43 všeobecného nariadenia o ochrane údajov. Majú predovšetkým pomôcť členským štátom, dozorným orgánom a národným akreditačným orgánom vytvoriť konzistentný a harmonizovaný základ pre akreditáciu certifikačných subjektov, ktoré vydávajú certifikácie v súlade so všeobecným nariadením o ochrane údajov.

2 ROZSAH PÔSOBNOSTI USMERNENÍ

6. Týmito usmerneniami:

- sa v kontexte všeobecného nariadenia o ochrane údajov stanovuje účel akreditácie,
- ozrejmujú sa možné spôsoby akreditácie certifikačných subjektov v súlade s článkom 43 ods. 1, a určujú kľúčové otázky, ktoré je potrebné zvážiť,
- sa upravuje rámec na stanovenie dodatočných požiadaviek na akreditáciu, ak akreditáciu vykonáva národný akreditačný orgán a
- sa upravuje rámec na stanovenie požiadaviek na akreditáciu, ak akreditáciu vykonáva dozorný orgán.

7. Tieto usmernenia nepredstavujú procesnú príručku pre akreditáciu certifikačných subjektov v súlade so všeobecným nariadením o ochrane údajov. Ich predmetom nie je vypracovanie novej technickej normy pre akreditáciu certifikačných subjektov na účely všeobecného nariadenia o ochrane údajov.

8. Tieto usmernenia sú určené:

- členským štátom, ktoré musia zabezpečiť akreditáciu certifikačných subjektov zo strany dozorných orgánov a/alebo národných akreditačných orgánov,
- národným akreditačným orgánom, ktoré vykonávajú akreditáciu certifikačných subjektov podľa článku 43 ods. 1 písm. b),
- príslušným dozorným orgánom, ktoré stanovujú „dodatočné požiadavky“ k požiadavkám obsiahnutým v norme ISO/IEC 17065/2012[2], ak akreditáciu vykonáva národný akreditačný orgán podľa článku 43 ods. 1 písm. b),
- EDPB pri vydávaní stanoviska k požiadavkám na akreditáciu príslušných dozorných orgánov podľa článku 43 ods. 3, článku 70 ods. 1 písm. p) a článku 64 ods. 1 písm. c) a schvaľovaní týchto požiadaviek,
- príslušnému dozornému orgánu, ktorý špecifikuje požiadavky na akreditáciu, ak akreditáciu vykonáva dozorný orgán podľa článku 43 ods. 1 písm. a),
- iným zainteresovaným stranám, ako sú napríklad budúce certifikačné subjekty alebo vlastníci certifikačných schém, ktorí stanovujú kritériá a postupy certifikácie[3].

[2] Medzinárodná organizácia pre normalizáciu: Posudzovanie zhody – Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb.

[3] Vlastník schémy je identifikovateľná organizácia, ktorá stanovila kritériá certifikácie a požiadavky, na základe ktorých sa má posudzovať zhoda. Akreditácia sa týka organizácie, ktorá na základe požiadaviek certifikačnej

9. Vymedzenie pojmov

10. Cieľom tohto vymedzenia pojmov je podporiť spoločné chápanie základných prvkov akreditačného procesu. Mali by sa považovať za referenčné pojmy, pričom si nenárokujú, že voči nim nemožno mať výhrady. Toto vymedzenie pojmov je založené na existujúcich regulačných rámcoch a normách, najmä na príslušných ustanoveniach všeobecného nariadenia o ochrane údajov a normy ISO/IEC 17065/2012.

11. Na účely týchto usmernení sa uplatňuje toto vymedzenie pojmov:

12. *„akreditácia“* certifikačných subjektov – pozri oddiel 3 o výklade pojmu „akreditácia“ na účely článku 43 všeobecného nariadenia o ochrane údajov;

13. *„dodatočné požiadavky“* sú požiadavky stanovené dozorným orgánom, ktorý je príslušný a na základe ktorých sa akreditácia vykonáva[4];

14. *„certifikácia“* je posúdenie a nestranná atestácia[5] treťou stranou o tom, že bolo preukázané splnenie kritérií certifikácie;

15. *„certifikačný subjekt“* je tretia strana, ktorá je orgánom[6] posudzovania zhody[7] a ktorá prevádzkuje certifikačné mechanizmy[8];

16. „*certifikačná schéma*“ je certifikačný systém týkajúci sa špecifikovaných produktov, procesov a služieb, na ktoré sa vzťahujú tie isté osobitné požiadavky, osobitné pravidlá a postupy[9],

17. „kritériá“ alebo kritériá certifikácie sú kritériá, na základe ktorých sa vykonáva certifikácia (posudzovanie zhody)[10],

18. „vnútroštátny akreditačný orgán“ (tu ako „národný akreditačný orgán“) je jediný orgán v členskom štáte vymenovaný v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 765/2008, ktorý vykonáva akreditáciu na základe právomoci, ktorú mu udelil štát[11].

---

schémy vykonáva posúdenia (článok 43 ods. 4) a ktorá vydáva certifikáty (t. j. certifikačný subjekt, známy aj ako orgán posudzovania zhody). Organizácia, ktorá vykonáva posúdenia, by mohla byť tá istá ako organizácia, ktorá schému vyvinula a vlastní, ale mohli by existovať dohody, kde jedna organizácia vlastní schému a iná organizácia (alebo viaceré iné organizácie) vykonáva posúdenia.

[4] Článok 43 ods. 1, 3 a 6

[5] Treba poznamenať, že podľa normy ISO 17000 atestácia treťou stranou (certifikácia) „sa týka všetkých objektov posudzovania zhody" [5.5] „okrem samých orgánov posudzovania zhody, ktoré sa podrobujú akreditácii.“ [5.6].

[6] Činnosť posudzovania zhody treťou stranou vykonáva organizácia nezávislá od osoby alebo organizácie poskytujúcej objekt, alebo od užívateľových záujmov na objekte, pozri ISO 17000, 2.4.

[7] Pozri ISO 17000, 2.5: „orgán, ktorý vykonáva služby posudzovania zhody“, ISO 17011: „orgán poskytujúci služby posudzovania zhody, ktorý môže byť predmetom akreditácie“, ISO 17065, 3.12.

[8] Články 42 ods. 1 a 42 ods. 5 všeobecného nariadenia o ochrane údajov.

[9] Pozri 3.9 v spojení s prílohou B normy ISO 17065.

[10] Pozri článok 42 ods. 5.

[11] Pozri článok 2 ods. 11 nariadenia (ES) č. 765/2008.

3 VÝKLAD POJMU „AKREDITÁCIA“ NA ÚČELY ČLÁNKU 43 VŠEOBECNÉHO NARIADENIA O OCHRANE ÚDAJOV

19. Vo všeobecnom nariadení o ochrane údajov sa pojem „akreditácia“ nevymedzuje. V článku 2 ods. 10 nariadenia (ES) č. 765/2008, ktorým sa ustanovujú všeobecné požiadavky na akreditácie, sa akreditácia vymedzuje ako

20. „je potvrdenie *[v týchto usmerneniach preložené ako „atestácia“]* vnútroštátneho *[v týchto usmerneniach preložené ako „národného“]* akreditačného orgánu o tom, že orgán posudzovania zhody spĺňa požiadavky vykonávať špecifické činnosti posudzovania zhody stanovené harmonizovanými normami a v prípade potreby akékoľvek dodatočné požiadavky vrátane tých, ktoré sú stanovené v príslušných sektorových systémoch *[v týchto usmerneniach preložené ako „schémach“]*;“

21. Podľa normy ISO/IEC 17011

22. „akreditácia je atestácia treťou stranou týkajúca sa orgánu posudzovania zhody, poskytujúca oficiálne preukázanie spôsobilosti vykonávať špecifické úlohy posudzovania zhody;“

23. V článku 43 ods. 1 sa stanovuje:

24. „[b]ez toho, aby boli dotknuté úlohy a právomoci príslušného dozorného orgánu podľa článkov 57 a 58, certifikačné subjekty, ktoré majú primeranú úroveň odborných znalostí vo vzťahu k ochrane údajov, vydajú a obnovia certifikáciu po tom, ako informujú dozorný orgán, aby mu umožnili uplatniť jeho právomoci podľa článku 58 ods. 2 písm. h). Členské štáty zabezpečia, aby boli tieto certifikačné subjekty akreditované jedným či oboma z týchto orgánov:

    (a) dozorným orgánom, ktorý je príslušný podľa článku 55 alebo 56;
    (b) národným akreditačným orgánom vymenovaným v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 765/2008 v súlade s normou ISO/IEC 17065/2012 a s dodatočnými požiadavkami stanovenými dozorným orgánom, ktorý je príslušný podľa článku 55 alebo 56.

25. Pokiaľ ide o všeobecné nariadenie o ochrane údajov, požiadavky na akreditáciu sa budú riadiť:

- normou ISO/IEC 17065/2012 a „dodatočnými požiadavkami“ stanovenými dozorným orgánom, ktorý je príslušný v súlade s článkom 43 ods. 1 písm. b), ak akreditáciu vykonáva národný akreditačný orgán, a dozorným orgánom, ak vykonáva akreditáciu sám.

26. V oboch prípadoch musia konsolidované požiadavky zahŕňať požiadavky uvedené v článku 43 ods. 2.

27. EDPB uznáva, že účelom akreditácie je poskytnúť vierohodné vyhlásenie o spôsobilosti orgánu vykonávať certifikáciu (činnosti posudzovania zhody)[12]. Akreditácia sa v zmysle všeobecného nariadenia o ochrane údajov chápe ako:

[12] Pozri odôvodnenie 15 nariadenia (ES) č. 765/2008.

28. atestácia[13] národným akreditačným orgánom a/alebo dozorným orgánom o tom, že certifikačný subjekt[14] má kvalifikáciu na vykonávanie certifikácie podľa článkov 42 a 43 všeobecného nariadenia o ochrane údajov pri zohľadnení normy ISO/IEC 17065/2012 a dodatočných požiadaviek stanovených dozorným orgánom a/alebo Výborom.

4 AKREDITÁCIA V SÚLADE S ČLÁNKOM 43 ODS. 1 VŠEOBECNÉHO NARIADENIA O OCHRANE ÚDAJOV

29. V článku 43 ods. 1 sa uznáva, že existuje niekoľko možností akreditácie certifikačných subjektov. Vo všeobecnom nariadení o ochrane údajov sa od dozorných orgánov a členských štátov vyžaduje, aby vymedzili proces akreditácie certifikačných subjektov. V tomto oddiele sa uvádzajú spôsoby akreditácie podľa článku 43.

4.1 Úloha členských štátov

30. V článku 43 ods. 1 sa vyžaduje, aby členské štáty *zabezpečili* akreditáciu certifikačných subjektov, ale každému členskému štátu sa umožňuje určiť, kto by mal byť zodpovedný za vykonanie posúdenia vedúceho k akreditácii. Na základe článku 43 ods. 1 sú k dispozícii tri možnosti; akreditáciu vykoná:

1. výlučne dozorný orgán, a to na základe svojich vlastných požiadaviek;
2. výlučne národný akreditačný orgán vymenovaným v súlade s nariadením (ES) č. 765/2008 a na základe normy ISO/IEC 17065/2012 a v súlade s dodatočnými požiadavkami stanovenými príslušným dozorným orgánom, alebo
3. dozorný orgán aj národný akreditačný orgán (a v súlade so všetkými požiadavkami uvedenými v bode 2).

31. Je na individuálnom členskom štáte, aby rozhodol, či predmetné akreditačné činnosti vykoná národný akreditačný orgán alebo dozorný orgán, resp. tieto orgány spoločne, v každom prípade by však mal zabezpečiť, aby boli poskytnuté primerané zdroje[15].

4.2 Interakcia s nariadením (ES) č. 765/2008

32. EDPB poznamenáva, že v článku 2 ods. 11 nariadenia (ES) č. 765/2008 sa vnútroštátny *[v týchto usmerneniach preložené ako „národný“]* akreditačný orgán vymedzuje ako *„jediný* orgán v členskom štáte, ktorý vykonáva akreditáciu na základe právomoci, ktorú mu udelil štát“.

33. Článok 2 ods. 11 by sa mohol považovať za nezlučiteľný s článkom 43 ods. 1 všeobecného nariadenia o ochrane údajov, ktorý umožňuje akreditáciu prostredníctvom iného orgánu, než je národný akreditačný orgán členského štátu. EDPB sa domnieva, že zámerom právnych predpisov EÚ bolo odchýliť sa od všeobecnej zásady, podľa ktorej akreditáciu vykonáva výlučne národný akreditačný orgán tým, že dávajú dozorným orgánom rovnakú právomoc, pokiaľ ide o akreditáciu certifikačných subjektov. Článok 43 ods. 1 je teda *lex specialis* vo vzťahu k článku 2 ods. 11 nariadenia (ES) č. 765/2008.

[13] Pozri článok 2 ods. 10 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh
[14] Pozri vymedzenie pojmu „akreditácia“ podľa normy ISO 17011.
[15] Pozri článok 4 ods. 9 nariadenia (ES) č. 765/2008.

4.3 Úloha národného akreditačného orgánu

34. V článku 43 ods. 1 písm. b) sa stanovuje, že národný akreditačný orgán akredituje certifikačné subjekty v súlade s normou ISO/IEC 17065/2012 a v súlade s dodatočnými požiadavkami stanovenými príslušným dozorným orgánom.

35. V záujme jasnosti EDPB konštatuje, že osobitný odkaz na „podľa odseku 1 písm. b) tohto článku“ obsiahnutý v článku 43 ods. 3 znamená, že „tieto požiadavky“ odkazujú na „dodatočné požiadavky“ stanovené príslušným dozorným orgánom podľa článku 43 ods. 1 písm. b) a požiadavky stanovené v článku 43 ods. 2.

36. V procese akreditácie národné akreditačné orgány uplatňujú dodatočné požiadavky, ktoré stanovia dozorné orgány.

37. Certifikačný subjekt s existujúcou akreditáciou podľa normy ISO/IEC 17065/2012 pre certifikačné schémy nesúvisiace so všeobecným nariadením o ochrane údajov, ktorý chce rozšíriť oblasť akreditácie tak, aby zahŕňala certifikáciu vydávanú v súlade so všeobecným nariadením o ochrane údajov, musí spĺňať dodatočné požiadavky stanovené dozorným orgánom, ak akreditáciu rieši národný akreditačný orgán. Ak akreditáciu na certifikáciu podľa všeobecného nariadenia o ochrane údajov ponúka len príslušný dozorný orgán, certifikačný subjekt, ktorý žiada o akreditáciu, musí spĺňať požiadavky stanovené príslušným dozorným orgánom.

4.4 Úloha dozorného orgánu

38. EDPB poznamenáva, že v článku 57 ods. 1 písm. q) sa stanovuje, že dozorný orgán *vykonáva* akreditáciu certifikačného subjektu podľa článku 43 ako „úlohu dozorného orgánu“ podľa článku 57 a že v článku 58 ods. 3 písm. e) sa stanovuje, že dozorný orgán má povoľovaciu a poradnú právomoc akreditovať certifikačné subjekty podľa článku 43. Znenie článku 43 ods. 1 poskytuje určitú flexibilitu a akreditačnú funkciu dozorného orgánu treba chápať ako úlohu len v príslušných prípadoch. Na objasnenie tohto bodu sa môžu použiť právne predpisy členského štátu. Od certifikačného subjektu sa však v procese akreditácie národným akreditačným orgánom podľa článku 43 ods. 2 písm. a) vyžaduje, aby k spokojnosti príslušného dozorného orgánu preukázal svoju nezávislosť a odborné znalosti vo vzťahu k predmetu, v súvislosti s ktorým ponúka certifikačný mechanizmus[16].

39. Ak členský štát stanoví, že certifikačné subjekty majú byť akreditované dozorným orgánom, dozorný orgán by mal stanoviť požiadavky na akreditáciu, ktoré okrem iného zahrnú požiadavky uvedené v článku 43 ods. 2. V porovnaní s povinnosťami týkajúcimi sa akreditácie certifikačných subjektov národnými akreditačnými orgánmi sa v článku 43 poskytuje menej pokynov v súvislosti s požiadavkami na akreditáciu, keď dozorný orgán vykonáva akreditáciu sám. V záujme prispievania k harmonizovanému prístupu k akreditácii by sa kritériá na akreditáciu, ktoré používa dozorný orgán, mali riadiť normou ISO/IEC 17065 a mali by byť doplnené o dodatočné požiadavky, ktoré dozorný orgán stanoví podľa článku 43 ods. 1 písm. b). EDPB konštatuje, že v článku 43 ods. 2 písm. a) až e) sa odrážajú a spresňujú požiadavky normy ISO 17065, čo prispeje ku konzistentnosti.

40. Ak členský štát stanoví, že certifikačné subjekty majú byť akreditované národnými akreditačnými orgánmi, dozorný orgán by mal stanoviť dodatočné požiadavky dopĺňajúce

[16] V dodatočných požiadavkách stanovených dozorným orgánom podľa článku 43 ods. 1 písm. b) by sa mali stanoviť požiadavky na nezávislosť a odborné znalosti. Pozri aj prílohu 1 k usmerneniam.

existujúce dojednania o akreditácii stanovené v nariadení (ES) č. 765/2008 (keď sa články 3 – 14 týkajú organizácie a fungovania akreditácie orgánov posudzovania zhody) a technické pravidlá, v ktorých sa opíšu metódy a postupy certifikačných subjektov. V tomto kontexte sa v nariadení (ES) č. 765/2008 stanovuje ďalšie usmernenie: V článku 2 ods. 10 sa vymedzuje akreditácia a odkazuje sa na „harmonizované normy" a „akékoľvek dodatočné požiadavky vrátane tých, ktoré sú stanovené v príslušných sektorových systémoch *[v týchto usmerneniach preložené ako „schémach"]*". Z toho vyplýva, že dodatočné požiadavky stanovené dozorným orgánom by mali zahŕňať osobitné požiadavky a mali by byť zamerané na uľahčenie posudzovania, a to okrem iného, nezávislosti a úrovne odborných znalostí certifikačných subjektov v oblasti ochrany údajov, napr. pokiaľ ide o ich schopnosť vyhodnotiť a certifikovať spracúvanie osobných údajov prevádzkovateľmi a sprostredkovateľmi podľa článku 42 ods. 1. Patrí sem aj spôsobilosť požadovaná v prípade sektorových schém a so zreteľom na ochranu základných práv a slobôd fyzických osôb, a najmä na ich právo na ochranu osobných údajov[17]. Príloha k týmto usmerneniam môže byť pre príslušné dozorné orgány užitočným zdrojom informácií pri stanovovaní „dodatočných požiadaviek" v súlade s článkami 43 ods. 1 písm. b) a 43 ods. 3.

41. V článku 43 ods. 6 sa stanovuje, že „[d]ozorný orgán zverejní požiadavky uvedené v odseku 3 tohto článku a kritériá uvedené v článku 42 ods. 5 v ľahko dostupnej forme." Preto sa v záujme transparentnosti všetky kritériá a požiadavky schválené dozorným orgánom uverejnia. Pokiaľ ide o kvalitu a dôveru v certifikačné subjekty, bolo by žiaduce, aby všetky požiadavky na akreditáciu boli pre verejnosť ľahko dostupné.

4.5 Dozorný orgán ako certifikačný subjekt

42. V článku 42 ods. 5 sa stanovuje, že dozorný orgán môže vydávať certifikácie, ale vo všeobecnom nariadení o ochrane údajov sa nevyžaduje, aby bol akreditovaný na splnenie požiadaviek podľa nariadenia (ES) č. 765/2008. EDPB konštatuje, že článok 43 ods. 1 písm. a) a najmä článok 58 ods. 2 písm. h) a článok 3 písm. a) a e) až f) umožňujú dozorným orgánom vykonávať akreditáciu a certifikáciu a zároveň poskytovať poradenstvo a v prípade potreby odňať certifikácie alebo nariadiť certifikačným subjektom, aby certifikácie nevydali.

43. Môžu sa vyskytnúť situácie, keď je vhodné, resp. nutné oddelenie úloh v oblasti akreditácie od certifikačných úloh a povinností, napríklad, ak v členskom štáte existuje dozorný orgán a iné certifikačné subjekty, pričom oba vydávajú rovnaký rozsah certifikácií. Dozorné orgány by preto mali prijať dostatočné organizačné opatrenia na oddelenie úloh podľa všeobecného nariadenia o ochrane údajov s cieľom zakotviť a uľahčiť certifikačné mechanizmy a zároveň prijať preventívne opatrenia na zabránenie konfliktom záujmov, ktoré môžu vyplývať z týchto úloh. Okrem toho by mali členské štáty a dozorné orgány pri formulovaní vnútroštátnych právnych predpisov a postupov týkajúcich sa akreditácie a certifikácie v súlade so všeobecným nariadením o ochrane údajov pamätať na harmonizáciu na európskej úrovni.

4.6 Požiadavky na akreditáciu

44. V prílohe k týmto usmerneniam sa uvádza usmernenie, ako určiť dodatočné požiadavky na akreditáciu. Identifikujú sa v ňom príslušné ustanovenia všeobecného nariadenia o ochrane údajov a navrhujú požiadavky, ktoré by dozorné orgány a národné akreditačné orgány mali zvážiť na zabezpečenie súladu so všeobecným nariadením o ochrane údajov.

[17] Článok 1 ods. 2 všeobecného nariadenia o ochrane údajov.

45. Ako už bolo uvedené, v prípade, že certifikačné subjekty sú akreditované národným akreditačným orgánom podľa nariadenia (ES) č. 765/2008, relevantnou akreditačnou normou bude norma ISO/IEC 17065/2012 doplnená o dodatočné požiadavky stanovené dozorným orgánom. V článku 43 ods. 2 sa odrážajú všeobecné ustanovenia normy ISO/IEC 17065/2012 so zreteľom na ochranu základných práv podľa všeobecného nariadenia o ochrane údajov. Rámec v prílohe používa článok 43 ods. 2 a normu ISO/IEC 17065/2012 ako základ na identifikáciu požiadaviek a ďalších kritérií týkajúcich sa posudzovania odborných znalostí certifikačných subjektov v oblasti ochrany údajov a ich schopnosti rešpektovať práva a slobody fyzických osôb pri spracúvaní osobných údajov ako je zakotvené vo všeobecnom nariadení o ochrane údajov. EDPB konštatuje, že tento rámec je osobitne zameraný na zabezpečenie toho, aby certifikačné subjekty mali primeranú úroveň odborných znalostí v oblasti ochrany údajov v súlade s článkom 43 ods. 1.

46. Dodatočné požiadavky na akreditáciu stanovené dozorným orgánom sa budú vzťahovať na všetky certifikačné subjekty, ktoré žiadajú o akreditáciu. Akreditačný orgán vyhodnotí, či je tento certifikačný subjekt spôsobilý vykonávať certifikačnú činnosť v súlade s dodatočnými požiadavkami a predmetom certifikácie. Musí sa odkazovať na konkrétne odvetvia alebo oblasti certifikácie, pre ktoré je certifikačný subjekt akreditovaný.

47. EDPB takisto poznamenáva, že okrem požiadaviek normy ISO/IEC 17065/2012 sa navyše vyžadujú osobitné odborné znalosti v oblasti ochrany údajov aj od iných, externých orgánov ako sú napr. laboratóriá alebo audítori, ak vykonávajú v mene akreditovaného certifikačného subjektu časti alebo súčasti certifikačných činností. V týchto prípadoch nie je možná akreditácia týchto externých orgánov podľa samotného všeobecného nariadenia o ochrane údajov. S cieľom zabezpečiť vhodnosť týchto orgánov pre ich činnosť v mene akreditovaných certifikačných subjektov je však potrebné, aby akreditovaný certifikačný subjekt zabezpečil, aby odborné znalosti v oblasti ochrany údajov požadované pre akreditovaný orgán boli tiež splnené a preukázané aj v prípade externého orgánu, pokiaľ ide o príslušnú vykonávanú činnosť.

48. Rámec na určenie dodatočných požiadaviek na akreditáciu uvedených v prílohe k týmto usmerneniam nepredstavuje procesnú príručku pre akreditačný proces, ktorý vykonáva národný akreditačný orgán alebo dozorný orgán. Poskytuje usmernenia týkajúce sa štruktúry a metodiky, a teda aj súbor nástrojov pre dozorné orgány s cieľom určiť dodatočné požiadavky na akreditáciu.

PRÍLOHA 1

V prílohe 1 sa uvádzajú usmernenia týkajúce sa špecifikácie „dodatočných“ požiadaviek na akreditáciu v súvislosti s normou ISO/IEC 17065/2012 a v súlade s článkom 43 ods. 1 písm. b) a článkom 43 ods. 3 všeobecného nariadenia o ochrane údajov.

V tejto prílohe sa stanovujú navrhované požiadavky, ktoré dozorný orgán pre ochranu údajov navrhne, a ktoré sa uplatnia počas akreditácie certifikačného subjektu národným akreditačným orgánom, resp. príslušným dozorným orgánom[18]. Tieto dodatočné požiadavky sa pred schválením podľa článku 64 ods. 1 písm. c) oznámia Európskemu výboru pre ochranu údajov.

Táto príloha by sa mala vykladať v spojení s normou ISO/IEC 17065/2012. Čísla oddielov, ktoré sa tu používajú, zodpovedajú číslam použitým v norme ISO/IEC 17065/2012. Ak akreditáciu podľa článku 43 ods. 1 písm. a) vykonávajú dozorné orgány, osvedčeným postupom by bolo postupovať podľa možnosti podľa tohto prístupu. Tým sa podporí harmonizácia akreditácie na úrovni EÚ.

Bez ohľadu na ďalej uvedené usmernenia alebo chýbajúce usmernenia ku ktorejkoľvek položke normy ISO/IEC 17065/2012, príslušný dozorný orgán môže podľa vnútroštátnych právnych predpisov stanoviť ďalšie dodatočné požiadavky týkajúce sa týchto položiek.

0 ÚVOD

[Tento oddiel sa vzťahuje na prípadne dohodnuté Podmienky spolupráce medzi národným akreditačným orgánom a dozorným orgánom pre ochranu údajov, napr. kto by mal byť zodpovedný za prijímanie žiadostí, resp. ako organizovať uznanie schválených kritérií v rámci akreditačného procesu.]

1 ROZSAH PÔSOBNOSTI[19]

Rozsah pôsobnosti normy ISO/IEC 17065/2012 sa uplatňuje v súlade so všeobecným nariadením o ochrane údajov. Usmernenia o akreditácii a certifikácii poskytujú ďalšie informácie. Národný akreditačný orgán a príslušný dozorný orgán by v rámci akreditačného postupu mali pri posudzovaní zohľadniť predmet certifikačného mechanizmu (napr. certifikácia operácií spracúvania v rámci cloudových služieb), a to najmä pokiaľ ide o kritériá, odborné znalosti a metodiku vyhodnocovania. Široký rozsah pôsobnosti normy ISO/IEC 17065/2012, ktorá sa vzťahuje na výrobky, procesy a služby, by nemal znížiť požiadavky alebo prevážiť nad požiadavkami všeobecného nariadenia o ochrane údajov; napr. mechanizmus riadenia nemôže byť jediným prvkom mechanizmu certifikácie, keďže certifikácia musí zahŕňať spracúvanie osobných údajov, t. j. spracovateľské operácie. Podľa článku 42 ods. 1 sa certifikácia v súvislosti so všeobecným nariadením o ochrane údajov vzťahuje len na spracovateľské operácie prevádzkovateľov a sprostredkovateľov.

[18] Pre informácie o procese schvaľovania kritérií certifikácie pozri oddiel 4 usmernení o certifikácii.
[19] Číslovanie odkazuje na normu ISO/IEC 17065/2012.

2 ODKAZY NA NORMY

Všeobecné nariadenie o ochrane údajov má prednosť pred normou ISO/IEC 17065/2012. Ak sa v dodatočných požiadavkách alebo v rámci certifikačného mechanizmu odkazuje na iné normy ISO, vykladajú sa v súlade s požiadavkami stanovenými vo všeobecnom nariadení o ochrane údajov.

3 POJMY A ICH VYMEDZENIE

V súvislosti s touto prílohou sa uplatňujú podmienky a vymedzenie pojmov obsiahnuté v usmerneniach k akreditácii (dokument WP 261) a k certifikácii (dokument EDPB 1/2018), pričom majú prednosť pred vymedzením pojmov v normách ISO.

4 VŠEOBECNÉ POŽIADAVKY NA AKREDITÁCIU

4.1 Zákonné a zmluvné požiadavky

4.1.1 Zákonná zodpovednosť

Certifikačný subjekt by mal byť schopný národnému akreditačnému orgánu alebo príslušnému dozornému orgánu (kedykoľvek) preukázať, že má k dispozícii aktualizované postupy preukazujúce súlad s právnymi povinnosťami stanovenými v podmienkach akreditácie vrátane dodatočných požiadaviek pokiaľ ide o uplatňovanie nariadenia (EÚ) 2016/679. Je potrebné poznamenať, že keďže certifikačný subjekt je sám prevádzkovateľom/sprostredkovateľom, musí byť schopný preukázať, že jeho postupy a opatrenia, ktoré sú osobitne určené na kontrolu osobných údajov klientskej organizácie a na nakladanie s nimi v rámci certifikačného procesu, sú v súlade s nariadením (EÚ) 2016/679.

Príslušný dozorný orgán sa môže rozhodnúť, že doplní ďalšie požiadavky a postupy na kontrolu súladu certifikačných subjektov so všeobecným nariadením o ochrane údajov v čase pred akreditáciou.

4.1.2 Dohoda o certifikácii

Minimálne požiadavky na dohodu o certifikácii sa doplnia týmito bodmi:

certifikačný subjekt musí okrem požiadaviek stanovených v norme ISO/IEC 17065/2012 navyše preukázať, že v jeho dohodách o certifikácii:

1. sa od žiadateľa požaduje, aby vždy dodržiaval všeobecné požiadavky na certifikáciu v zmysle bodu 4.1.2.2 písm. a) normy ISO/IEC 17065/2012 a kritériá schválené príslušným dozorným orgánom alebo EDPB v súlade s článkom 43 ods. 2 písm. b) a článkom 42 ods. 5;
2. sa od žiadateľa požaduje, aby zachoval voči príslušnému dozornému orgánu úplnú transparentnosť v súvislosti s postupom certifikácie vrátane zmluvne dôverných záležitostí súvisiacich s dodržiavaním ochrany údajov podľa článku 42 ods. 7 a článku 58 ods. 1 písm. c);
3. sa neznižuje zodpovednosť žiadateľa za súlad s nariadením (EÚ) 2016/679 a že tieto dohody nemajú vplyv na úlohy a právomoci dozorných orgánov, ktoré sú príslušné v súlade s článkom 42 ods. 5;
4. sa od žiadateľa požaduje, aby poskytol certifikačnému subjektu všetky informácie a prístup k spracovateľským činnostiam, ktoré sú potrebné na vykonanie postupu certifikácie podľa článku 42 ods. 6;

5. sa od žiadateľa požaduje, aby dodržiaval platné lehoty a postupy. V dohode o certifikácii sa musí stanoviť, že lehoty a postupy vyplývajúce napríklad z programu certifikácie alebo iných právnych predpisov sa musia dodržiavať;
6. pokiaľ ide o bod 4.1.2.2 písm. c) č. 1 normy ISO/IEC 17065/2012, v týchto dohodách sa stanovujú pravidlá platnosti, obnovy a odobratia podľa článkov 42 ods. 7 a 43 ods. 4 vrátane pravidiel, ktorými sa stanovujú vhodné intervaly na prehodnotenie alebo preskúmanie (správnosti) v súlade s článkom 42 ods. 7;
7. sa certifikačnému subjektu umožňuje zverejniť všetky informácie potrebné na udelenie certifikácie podľa článkov 42 ods. 8 a 43 ods. 5;
8. sú obsiahnuté aj pravidlá týkajúce sa potrebných opatrení na prešetrovanie sťažností v zmysle bodu 4.1.2.2 písm. c) č. 2, pričom podľa písm. j) obsahujú aj výslovné vyhlásenia o štruktúre a postupe manažérstva sťažností v súlade s článkom 43 ods. 2 písm. d);
9. okrem minimálnych požiadaviek uvedených v bode 4.1.2.2 normy ISO/IEC 17065/2012, ak dôsledky zrušenia alebo pozastavenia akreditácie pre certifikačný subjekt majú vplyv na klienta, v takom prípade by sa v týchto dohodách o certifikácii mali riešiť aj dôsledky pre zákazníka;
10. sa od žiadateľa požaduje, aby informoval certifikačný subjekt v prípade významných zmien v jeho skutočnej alebo právnej situácii a v produktoch, procesoch a službách, ktorých sa certifikácia týka.

4.1.3 Používanie pečatí a značiek ochrany údajov

Certifikáty, pečate a značky sa používajú len v súlade s článkami 42 a 43 a s usmerneniami pre akreditáciu a certifikáciu.

4.2 Manažérstvo nestrannosti

Akreditačný orgán navyše zabezpečí, aby okrem požiadavky obsiahnutej v bode 4.2 normy ISO/IEC 17065/2012:

1. certifikačný subjekt spĺňal dodatočné požiadavky príslušného dozorného orgánu [podľa článku 43 ods. 1 písm. b)]

   a) v súlade s článkom 43 ods. 2 písm. a) poskytol osobitný dôkaz o svojej nezávislosti. Toto platí najmä v súvislosti s dôkazmi o financovaní certifikačného subjektu, a to v rozsahu, v akom sa to týka uistenia o jeho nestrannosti;

   b) jeho úlohy a povinnosti neviedli ku konfliktu záujmov podľa článku 43 ods. 2 písm. e);

2. certifikačný subjekt nemal žiadne relevantné prepojenie so zákazníkom, ktorého posudzuje.

4.3 Záväzky a financovanie

Akreditačný orgán okrem požiadavky stanovenej v bode 4.3.1 normy ISO/IEC 17065/2012 tiež pravidelne zabezpečuje, aby certifikačný subjekt disponoval primeranými opatreniami (napr. poistenie alebo rezervy) na pokrytie svojich záväzkov v geografických regiónoch, v ktorých pôsobí.

4.4 Nediskriminačné podmienky

Dozorný orgán môže stanoviť dodatočné požiadavky, ak je to v súlade s vnútroštátnymi právnymi predpismi.

4.5 Dôvernosť

Dozorný orgán môže stanoviť dodatočné požiadavky, ak je to v súlade s vnútroštátnymi právnymi predpismi.

4.6 Verejne dostupné informácie

Akreditačný orgán okrem požiadavky obsiahnutej v bode 4.6 normy ISO/IEC 17065/2012 navyše vyžaduje od certifikačného subjektu prinajmenšom, aby:

1. všetky verzie (súčasné a predchádzajúce) schválených kritérií v zmysle článku 42 ods. 5 boli uverejnené a ľahko verejne dostupné (to platí aj pre všetky postupy certifikácie); vo všeobecnosti platí, že sa musí uvádzať príslušné obdobie ich platnosti;
2. sa informácie o vybavovaní sťažností a odvolaní zverejňovali podľa článku 43 ods. 2 písm. d).

5 POŽIADAVKY NA ŠTRUKTÚRU, ČLÁNOK 43 ODS. 4 [„RIADNE“ POSÚDENIE]

5.1 Organizačná štruktúra a vrcholový manažment

Dozorný orgán môže stanoviť dodatočné požiadavky.

5.2 Mechanizmy na zachovanie nestrannosti

Dozorný orgán môže stanoviť dodatočné požiadavky.

6 POŽIADAVKY NA ZDROJE

6.1 Pracovníci certifikačného subjektu

Akreditačný orgán okrem požiadavky obsiahnutej v oddiele 6 normy ISO/IEC 17065/2012 navyše zabezpečí, aby v prípade každého certifikačného subjektu jeho pracovníci:

1. preukázali primerané a priebežné odborné znalosti (vedomosti a skúsenosti) týkajúce sa ochrany údajov podľa článku 43 ods. 1;
2. boli nezávislí a mali priebežné odborné znalosti týkajúce sa predmetu certifikácie podľa článku 43 ods. 2 písm. a) a neboli v konflikte záujmov podľa článku 43 ods. 2 písm. e);
3. sa zaviazali dodržiavať kritériá uvedené v článku 42 ods. 5 podľa článku 43 ods. 2 písm. b);
4. mali relevantné a primerané znalosti a skúsenosti v oblasti uplatňovania právnych predpisov na ochranu údajov;
5. mali relevantné a primerané znalosti a skúsenosti, pokiaľ ide o relevantné technické a organizačné opatrenia na ochranu údajov;
6. boli schopní preukázať skúsenosti v oblastiach uvedených v dodatočných požiadavkách 6.1.1, 6.1.4 a 6.1.5, a to konkrétne:

pokiaľ ide o pracovníkov s technickými znalosťami:

- že získali kvalifikáciu v príslušnej oblasti technických znalostí prinajmenšom na úrovni EQF[20] 6, resp. že majú uznaný chránený titul (napr. Dipl. Ing.) v rámci príslušného regulovaného povolania alebo že majú značnú odbornú prax.
- *Pracovníci zodpovední za rozhodnutia o certifikácii* musia mať značné odborné skúsenosti pri určovaní a vykonávaní opatrení na ochranu údajov.

[20] Pozri nástroj na porovnávanie kvalifikačného rámca na adrese https://ec.europa.eu/ploteus/en/compare?

- *Pracovníci zodpovední za vyhodnotenia* musia mať odbornú prax v oblasti technickej ochrany údajov a vedomosti a skúsenosti v súvislosti s porovnateľným postupom (napr. certifikácie/audity) a v príslušných prípadoch musia byť zaregistrovaní.

Pracovníci musia prostredníctvom kontinuálneho profesijného rozvoja preukázať, že si udržiavajú osobitné vedomosti v predmetnej oblasti v rámci technických a audítorských zručností.

pokiaľ ide o pracovníkov s právnymi znalosťami:

- štúdium práva na univerzite uznanej EÚ alebo štátom v trvaní najmenej osem semestrov vrátane akademického titulu magister (LL.M.), resp. titulu, ktorý mu je rovnocenný, alebo značnú odbornú prax.
- *Pracovníci zodpovední za rozhodnutia o certifikácii* musia preukázať značnú odbornú prax v oblasti právnych predpisov na ochranu údajov a byť registrovaní podľa požiadaviek členského štátu.
- *Pracovníci zodpovední za vyhodnotenia* musia preukázať minimálne dva roky odbornej praxe v oblasti práva na ochranu údajov a mať vedomosti a skúsenosti v súvislosti s porovnateľnými postupmi (napr. certifikácie/audity), pričom musia byť registrovaní, ak to členský štát vyžaduje.
    - pracovníci musia prostredníctvom kontinuálneho profesijného rozvoja preukázať, že si udržiavajú osobitné vedomosti v predmetnej oblasti v rámci technických a audítorských zručností.

6.2 Zdroje informácií na hodnotenie

Dozorný orgán môže stanoviť dodatočné požiadavky, ak je to v súlade s vnútroštátnymi právnymi predpismi.

7 POŽIADAVKY NA PROCES, ČLÁNOK 43 ODS. 2 PÍSM. C) A D)

7.1 Všeobecne

Akreditačný orgán okrem požiadavky obsiahnutej v oddiele 7.1 normy ISO/IEC 17065/2012 je tiež povinný zabezpečiť ďalej uvedené:

1. certifikačné subjekty pri predkladaní žiadosti dodržiavajú dodatočné požiadavky príslušného dozorného orgánu [podľa článku 43 ods. 1 písm. b)], aby úlohy a povinnosti neviedli ku konfliktu záujmov v zmysle článku 43 ods. 2 písm. b);
2. pred tým, ako certifikačný subjekt začne prevádzkovať schválenú európsku pečať ochrany údajov v novom členskom štáte zo satelitnej kancelárie, túto skutočnosť oznámia dotknutým dozorným orgánom.

7.2 Žiadosť

Okrem bodu 7.2 normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby:

1. predmet certifikácie (cieľ hodnotenia, ToE) bol v žiadosti podrobne opísaný. Do tohto opisu musia byť zahrnuté aj rozhrania a prenosy do iných systémov a iným organizáciám, ako aj protokoly a iné záruky;
2. v žiadosti sa uvedie, či sa využívajú sprostredkovatelia, a ak sú žiadateľom sprostredkovatelia, opíše sa ich zodpovednosť a úlohy, pričom žiadosť musí obsahovať príslušnú zmluvu (-y) prevádzkovateľ/sprostredkovateľ.

7.3 Preskúmanie žiadosti

Okrem bodu 7.3 normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby:

1. sa v dohode o certifikácii stanovili záväzné metódy vyhodnotenia so zreteľom na cieľ hodnotenia (ToE);
2. sa pri posudzovaní existencie dostatočných odborných znalostí podľa bodu 7.3 písm. e) v náležitom rozsahu zohľadnili technické aj právne znalosti v oblasti ochrany údajov.

7.4 Vyhodnocovanie

Okrem bodu 7.4 normy ISO/IEC 17065/2012 sa navyše v certifikačných mechanizmoch opisujú dostatočné metódy vyhodnotenia súladu spracovateľskej operácie či spracovateľských operácií s kritériami certifikácie, a to v príslušných prípadoch aj pokiaľ ide o:

1. metódu na posúdenie nevyhnutnosti a primeranosti spracovateľských operácií vo vzťahu k ich účelu a príslušným dotknutým osobám;
2. metódu vyhodnotenia krytia, zloženia a posudzovania všetkých rizík, ktoré posudzujú prevádzkovateľ a sprostredkovateľ, pokiaľ ide o právne dôsledky podľa článkov 30, 32, 35 a 36 všeobecného nariadenia o ochrane údajov, a so zreteľom na vymedzenie technických a organizačných opatrení podľa článkov 24, 25 a 32 všeobecného nariadenia o ochrane údajov, pokiaľ sa uvedené články vzťahujú na predmet certifikácie a
3. metódu na posúdenie prostriedkov nápravy vrátane záruk, právnych poistiek a postupov na zabezpečenie ochrany osobných údajov v súvislosti so spracúvaním, ktoré sa má pripísať predmetu certifikácie, a to na preukázanie toho, že sú splnené právne požiadavky stanovené v kritériách a
4. dokumentáciu metód a zistení.

Od certifikačného subjektu by sa malo vyžadovať, aby zabezpečil, že tieto metódy vyhodnotenia budú štandardizované a všeobecne použiteľné. To znamená, že pri porovnateľných cieľoch hodnotenia (ToEs) sa budú používať porovnateľné metódy vyhodnotenia. Akúkoľvek odchýlku od tohto postupu musí odôvodniť certifikačný subjekt.

Okrem bodu 7.4.2 normy ISO/IEC 17065/2012 by sa malo navyše povoliť, aby vyhodnotenie vykonávali externí experti, ktorých uznal certifikačný subjekt.

Okrem bodu 7.4.5 normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby bolo možné certifikáciu ochrany údajov v súlade s článkami 42 a 43 všeobecného nariadenia o ochrane údajov, ktorá už pokrýva časť predmetu certifikácie, zahrnúť do aktuálnej certifikácie. Nebude však dostačujúca na to, aby úplne nahradila (čiastočné) vyhodnotenia. Certifikačný subjekt je povinný overiť súlad s kritériami. Uznanie si v každom prípade bude vyžadovať poskytnutie úplnej hodnotiacej správy alebo informácií, ktoré umožnia vyhodnotenie predchádzajúcej certifikačnej činnosti a jej výsledkov. Vyhlásenie o certifikácii alebo podobné osvedčenia o certifikácii by sa nemali považovať za dostačujúce na to, aby nahrádzali správu.

Okrem bodu 7.4.6 normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby certifikačný subjekt vo svojom certifikačnom mechanizme podrobne stanovoval, akým spôsobom informácie požadované v bode 7.4.6 informujú zákazníka (žiadateľa o certifikáciu) o nesúlade s certifikačným mechanizmom. V tejto súvislosti by sa mal vymedziť prinajmenšom charakter týchto informácií a ich načasovanie.

Okrem bodu 7.4.9 normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby dokumentácia bola na požiadanie dozorného orgánu pre ochranu údajov sprístupnená v plnom rozsahu.

7.5 Preskúmanie

Okrem bodu 7.5 normy ISO/IEC 17065/2012 sa navyše vyžadujú postupy na udeľovanie, pravidelné preskúmavanie a zrušenie príslušných certifikácií podľa článku 43 ods. 2 a článku 43 ods. 3.

7.6 Certifikačné rozhodnutie

Okrem bodu 7.6.1 normy ISO/IEC 17065/2012 by mal certifikačný subjekt v rámci svojich postupov tiež podrobne stanoviť, ako je zabezpečená jeho nezávislosť a zodpovednosť, pokiaľ ide o individuálne certifikačné rozhodnutia.

7.7 Certifikačná dokumentácia

Okrem bodu 7.7.1 písm. e) normy ISO/IEC 17065/2012 a v súlade s článkom 42 ods. 7 všeobecného nariadenia o ochrane údajov by sa malo navyše vyžadovať, aby obdobie platnosti certifikácií nepresiahlo tri roky.

Okrem bodu 7.7.1 písm. e) normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby sa zdokumentovalo aj časové obdobie zamýšľaného monitorovania v zmysle oddielu 7.9.

Okrem bodu 7.7.1 písm. f) normy ISO/IEC 17065/2012 by mal certifikačný subjekt v certifikačnej dokumentácii tiež povinne uvádzať predmet certifikácie (uvedenie stavu verzie dokumentu alebo podobných vlastností).

7.8 Zoznam certifikovaných produktov

Okrem bodu 7.8 normy ISO/IEC 17065/2012 by sa od certifikačného subjektu malo navyše vyžadovať, aby informácie o certifikovaných produktoch, procesoch a službách sprístupnil interne aj verejne. Certifikačný subjekt poskytne verejnosti zhrnutie hodnotiacej správy. Cieľom tohto zhrnutia je napomôcť transparentnosti, pokiaľ ide o to, čo bolo certifikované, a ako to bolo posudzované. V zhrnutí sa ozrejmia tieto skutočnosti:

a) rozsah pôsobnosti certifikácie, pričom sa takisto uvedie zmysluplný opis predmetu certifikácie (cieľ hodnotenia, ToE);

b) príslušné kritériá certifikácie (vrátane verzie alebo funkčného stavu);

c) vykonané metódy vyhodnotenia a skúšky a

d) výsledok či výsledky.

Okrem bodu 7.8 normy ISO/IEC 17065/2012 a podľa článku 43 ods. 5 všeobecného nariadenia o ochrane údajov certifikačný subjekt tiež informuje príslušné dozorné orgány o dôvodoch udelenia alebo zrušenia požadovanej certifikácie.

7.9 Dozor

Okrem bodov 7.9.1, 7.9.2 a 7.9.3 normy ISO/IEC 17065/2012 a v súlade s článkom 43 ods. 2 písm. c) všeobecného nariadenia o ochrane údajov by sa malo navyše vyžadovať, aby na zachovanie certifikácie počas monitorovacieho obdobia boli pravidelné monitorovacie opatrenia povinné.

7.10 Zmeny ovplyvňujúce certifikáciu

Okrem bodov 7.10.1 a 7.10.2 normy ISO/IEC 17065/2012 by medzi zmeny ovplyvňujúce certifikáciu, ktoré má posúdiť certifikačný subjekt, mali tiež patriť: zmeny právnych predpisov o ochrane údajov, prijatie delegovaných aktov Európskej komisie v súlade s článkami 43 ods. 8 a 43 ods. 9, rozhodnutia Európskeho výboru pre ochranu údajov a súdne rozhodnutia týkajúce sa ochrany údajov. Medzi postupy v súvislosti s týmito zmenami, ktoré sa majú dohodnúť, by mali patriť: prechodné obdobia, postup schválenia príslušným dozorným orgánom, opätovné posúdenie príslušného predmetu certifikácie a primerané opatrenia na zrušenie certifikácie, ak certifikovaná spracovateľská operácia už nie je v súlade s aktualizovanými kritériami.

7.11 Ukončenie, zúženie rozsahu, pozastavenie alebo odňatie certifikácie

Okrem kapitoly 7.11.1 normy ISO/IEC 17065/2012 by sa od certifikačného subjektu malo navyše vyžadovať, aby bezodkladne písomne informoval príslušný dozorný orgán a v príslušných prípadoch národný akreditačný orgán o prijatých opatreniach a o pokračovaní, obmedzeniach, pozastavení a odňatí certifikácie.

Podľa článku 58 ods. 2 písm. h) sa od certifikačného subjektu vyžaduje, aby sa riadil rozhodnutiami a príkazmi príslušného dozorného orgánu na odňatie alebo nevydanie certifikácie zákazníkovi (žiadateľovi), ak nie sú splnené, resp. prestali byť splnené, požiadavky na certifikáciu.

7.12 Záznamy

Certifikačný subjekt by mal byť povinný uchovávať všetku dokumentáciu v úplnej a zrozumiteľnej forme, tak, aby bola aktuálna a aby mohla byť predmetom auditu.

7.13 Sťažnosti a odvolania, článok 43 ods. 2 písm. d)

Okrem bodu 7.13.1 normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby certifikačný subjekt vymedzil:

a) kto môže podávať sťažnosti alebo námietky;

b) kto ich spracúva na strane certifikačného subjektu;

c) aké overenia sa uskutočnia v tejto súvislosti a

d) možnosti konzultácií so zainteresovanými stranami.

Okrem bodu 7.13.2 normy ISO/IEC 17065/2012 by sa malo navyše vyžadovať, aby certifikačný subjekt vymedzil:

a) ako a komu sa takéto potvrdenie musí poskytnúť;

b) časové lehoty v tejto súvislosti a

c) aké procesy sa majú následne začať.

Certifikačný subjekt musí okrem bodu 7.13.1 normy ISO/IEC 17065/2012 navyše vymedziť, ako je zabezpečené oddelenie certifikačných činností a vybavovania odvolaní a sťažností.

8 POŽIADAVKY NA SYSTÉM MANAŽÉRSTVA

Všeobecnou požiadavkou na systém manažérstva podľa kapitoly 8 normy ISO/IEC 17065/2012 je, aby uplatňovanie všetkých požiadaviek z predchádzajúcich kapitol v rámci predmetu uplatňovania certifikačného mechanizmu akreditovaným certifikačným subjektom bolo dokumentované, vyhodnotené, kontrolované a monitorované nezávisle.

Základnou zásadou manažérstva je vymedziť systém, podľa ktorého sa ciele stanovia účinne a efektívne, a to najmä realizácia certifikačných služieb prostredníctvom vhodných špecifikácií. To si vyžaduje transparentnosť a overiteľnosť vykonávania akreditačných požiadaviek certifikačným subjektom a jeho trvalý súlad s nimi.

Na tento účel musí systém manažérstva špecifikovať metodiku na dosiahnutie a kontrolu týchto požiadaviek v súlade s právnymi predpismi o ochrane údajov a na ich priebežnú kontrolu zo strany samotného akreditovaného orgánu.

Tieto zásady manažérstva a ich zdokumentované vykonávanie musia byť transparentné, pričom akreditovaný certifikačný subjekt ich musí poskytnúť v súlade s akreditačným postupom podľa článku 58 a následne na žiadosť dozorného orgánu pre ochranu údajov kedykoľvek počas vyšetrovania vo

forme auditov v oblasti ochrany údajov podľa článku 58 ods. 1 písm. b) alebo preskúmania certifikácií vydaných v súlade s článkom 42 ods. 7 podľa článku 58 ods. 1 písm. c).

Najmä akreditovaný certifikačný subjekt musí trvalo a nepretržite zverejňovať, ktoré certifikácie boli vykonané na akom základe (resp. certifikačné mechanizmy alebo schémy), ako dlho sú certifikácie platné, a na základe akého rámca a za akých podmienok (odôvodnenie 100).

8.1 Požiadavky na všeobecný systém manažérstva

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

8.2 Dokumentácia systému manažérstva

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

8.3 Riadenie dokumentov

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

8.4 Riadenie záznamov

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

8.5 Preskúmanie manažmentom

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

8.6 Interné audity

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

8.7 Nápravné činnosti

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

8.8 Preventívne činnosti

Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

9 ĎALŠIE DODATOČNÉ POŽIADAVKY[21]

9.1 Aktualizácia metód vyhodnotenia

Certifikačný subjekt zavedie postupy na usmerňovanie aktualizácie metód vyhodnotenia žiadosti, ktoré sa majú uplatňovať v kontexte vyhodnotenia podľa bodu 7.4. Aktualizácia sa musí uskutočniť v prípade zmien právneho rámca, príslušného rizika či rizík, stavu techniky a nákladov na realizáciu technických a organizačných opatrení.

[21] Príslušný dozorný orgán môže stanoviť a doplniť ďalšie dodatočné požiadavky podľa vnútroštátnych právnych predpisov.

9.2 Udržiavanie odborných znalostí

Certifikačné subjekty zavedú postupy na zabezpečenie odbornej prípravy svojich zamestnancov s cieľom aktualizovať ich zručnosti, pričom sa zohľadní vývoj uvedený v bode 9.1.

9.3 Zodpovednosti a kompetencie

9.3.1 Komunikácia medzi certifikačným orgánom a jeho zákazníkmi

Zavedú sa postupy na zavedenie vhodných postupov a štruktúr na účely komunikácie medzi certifikačným subjektom a jeho zákazníkom. Tieto postupy budú zahŕňať:

1. vedenie dokumentácie o úlohách a zodpovednostiach akreditovaného certifikačného subjektu na účely:
    a) žiadostí o informácie, alebo
    b) umožnenia kontaktu v prípade sťažnosti týkajúcej sa certifikácie;
2. zachovanie procesu podávania žiadostí na účely:
    a) informácie o stave žiadosti;
    b) vyhodnotení príslušným dozorným orgánom, pokiaľ ide o:
        i. spätnú väzbu;
        ii. rozhodnutia príslušného dozorného orgánu.

9.3.2 Dokumentácia činností vyhodnotenia

Dozorný orgán môže sformulovať dodatočné požiadavky.

9.3.3 Manažment vybavovania sťažností

Vybavovanie sťažností bude zavedené ako neoddeliteľná súčasť systému manažérstva, v rámci ktorého sa vykonávajú najmä požiadavky uvedené v bude 4.1.2.2 písm. c), 4.1.2.2 písm. j), 4.6 písm. d) a v bode 7.13 normy ISO/IEC 17065/2012.

Príslušné sťažnosti a námietky by mali byť postúpené príslušnému dozornému orgánu.

9.3.4 Manažérstvo odňatia

Postupy v prípade pozastavenia alebo odňatia akreditácie sa začlenia do systému manažérstva certifikačného subjektu, a to aj pokiaľ ide o otázku oznámení adresovaných zákazníkom.