Pokyny

Pokyny č. 4/2018 týkající se akreditace subjektů pro vydávání osvědčení podle článku 43 obecného nařízení o ochraně osobních údajů (2016/679)

Verze 3.0

4. června 2019

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Přijato

Historie verzí

Verze 3.0	4. června 2019	Zahrnutí přílohy 1 (verze 2.0 přílohy 1 přijaté dne 4. června 2019 po veřejné konzultaci)
Verze 2.0	4. prosince 2018	Přijetí pokynů po veřejné konzultaci – k témuž datu byla přijata příloha 1 (verze 1.0) k veřejné konzultaci
Verze 1.0	6. února 2018	Přijetí pokynů pracovní skupinou zřízenou podle článku 29 (verze pro veřejnou konzultaci). Tuto verzi schválil Evropský sbor pro ochranu osobních údajů dne 25. května 2018.

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. e) nařízení Evropského parlamentu a Rady 2016/679/EU ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES,

po zvážení výsledků veřejné konzultace o pokynech, která proběhla v únoru 2018, a o příloze, která proběhla od 14. prosince 2018 do 1. února 2019, podle čl. 70 odst. 4 obecného nařízení o ochraně osobních údajů,

PŘIJAL TYTO POKYNY:

1 ÚVOD

1. Nařízení o ochraně osobních údajů (nařízení (EU) 2016/679, dále jen „nařízení GDPR“), které vstoupilo v platnost dne 25. května 2018, poskytuje modernizovaný rámec pro dodržování právních předpisů pro ochranu osobních údajů v Evropě založený na odpovědnosti a základních právech. Pro tento nový rámec má zásadní význam řada opatření, která mají usnadnit dodržování ustanovení nařízení GDPR. Ta zahrnují povinné požadavky za specifických okolností (včetně jmenování pověřenců pro ochranu osobních údajů a provádění posouzení vlivu na ochranu osobních údajů) a dobrovolná opatření, jako jsou kodexy chování a mechanismy pro vydávání osvědčení.

2. Jako součást zavedení mechanismů pro vydávání osvědčení a zavedení pečetí a známek dokládajících ochranu údajů se v čl. 43 odst. 1 nařízení GDPR vyžaduje, aby členské státy zajistily, že subjekty pro vydávání osvědčení, které vydávají osvědčení podle čl. 42 odst. 1, jsou akreditovány buď příslušným dozorovým úřadem, nebo vnitrostátním akreditačním orgánem, nebo oběma. Pokud akreditaci provádí vnitrostátní akreditační orgán v souladu s normou ISO/IEC 17065/2012, je třeba rovněž uplatnit dodatečné požadavky stanovené příslušným dozorovým úřadem.

3. Smysluplné mechanismy pro vydávání osvědčení mohou zkvalitnit dodržování nařízení GDPR a transparentnost pro subjekty údajů a v rámci vztahů mezi podniky, například mezi správci a zpracovateli. Pro správce a zpracovatele údajů bude přínosné nezávislé ověření třetí stranou, které umožní prokázat soulad jejich operací zpracování s nařízením GDPR[1].

4. V této souvislosti Evropský sbor pro ochranu osobních údajů uznává, že je nezbytné poskytnout pokyny týkající se akreditace. Zvláštní hodnota a účel akreditace spočívá ve skutečnosti, že poskytuje oficiální stanovisko k odborné způsobilosti subjektů pro vydávání osvědčení, které umožňuje vytváření důvěry v mechanismus pro vydávání osvědčení.

[1] Ve 100. bodě odůvodnění nařízení GDPR se uvádí, že zavedení mechanismů pro vydávání osvědčení může zvýšit transparentnost a lépe zajistit soulad s nařízením, aby subjekty údajů mohly u příslušných produktů a služeb posoudit úroveň ochrany údajů.

5. Cílem těchto pokynů je poskytnout návod, jak interpretovat a provádět ustanovení článku 43 nařízení GDPR. Tyto pokyny mají zejména pomoci členským státům, dozorovým úřadům a vnitrostátním akreditačním orgánům stanovit jednotné, harmonizované východisko pro akreditaci subjektů, které vydávají osvědčení v souladu s nařízením GDPR.

2 OBLAST PŮSOBNOSTI POKYNŮ

6. Tyto pokyny:

- stanovují účel akreditace v souvislosti s nařízení GDPR,
- vysvětlují možné způsoby akreditace subjektů pro vydávání osvědčení v souladu s čl. 43 odst. 1 a identifikují klíčové otázky ke zvážení,
- poskytují rámec pro stanovení dodatečných požadavků na akreditaci, pokud akreditaci provádí vnitrostátní akreditační orgán, a
- poskytují rámec pro stanovení požadavků na akreditaci, pokud akreditaci provádí dozorový úřad.

7. Tyto pokyny nepředstavují příručku postupů pro akreditaci subjektů pro vydávání osvědčení v souladu s nařízením GDPR, ani nevytvářejí novou technickou normu pro akreditaci subjektů pro vydávání osvědčení pro účely nařízení GDPR.

8. Pokyny jsou určeny pro:

- členské státy, které musí zajistit, aby subjekty pro vydávání osvědčení byly akreditovány dozorovým úřadem a/nebo vnitrostátním akreditačním orgánem,
- vnitrostátní akreditační orgány, které provádějí akreditaci subjektů pro vydávání osvědčení podle čl. 43 odst. 1 písm. b),
- příslušný dozorový úřad, který určuje „dodatečné požadavky“ k požadavkům stanoveným normou ISO/IEC 17065/2012[2], pokud akreditaci provádí vnitrostátní akreditační orgán podle čl. 43 odst. 1 písm. b),
- Evropský sbor pro ochranu osobních údajů, pokud vydává stanovisko k požadavkům na akreditaci příslušného dozorového úřadu a pokud tyto požadavky schvaluje v souladu s čl. 43 odst. 3, čl. 70 odst. 1 písm. p) a čl. 64 odst. 1 písm. c),
- příslušný dozorový úřad, který stanovuje požadavky na akreditaci, pokud akreditaci provádí dozorový úřad podle čl. 43 odst. 1 písm. a),
- další zúčastněné strany, jako jsou potenciální subjekty pro vydávání osvědčení nebo vlastníci systémů vydávání osvědčení, kteří stanovují kritéria a postupy pro vydávání osvědčení[3].

[2] Mezinárodní organizace pro normalizaci: Posuzování shody – požadavky na orgány certifikující produkty, procesy a služby.

[3] Vlastník systému je identifikovatelná organizace, která stanovuje kritéria pro vydávání osvědčení a požadavky, podle nichž se má posuzovat shoda. Akreditace se týká organizace, která na základě požadavků systému vydávání osvědčení provádí posouzení (čl. 43 odst. 4) a vydává osvědčení (tedy subjekt pro vydávání osvědčení, známý též jako subjekt posuzování shody). Organizace, která provádí posouzení, by mohla být tatáž organizace, která vypracovala systém vydávání osvědčení a je jeho vlastníkem, mohly by však existovat situace, kdy jedna organizace vlastní systém vydávání osvědčení a jiná organizace (nebo více organizací) provádí posouzení.

9. Definice

10. Následující definice se snaží přispět k jednotnému výkladu základních prvků akreditačního procesu. Měly by být brány jako reference a nekladou si žádný nárok na nezpochybnitelnost. Tyto definice jsou založeny na stávajících regulačních rámcích a normách, zejména na příslušných ustanoveních nařízení GDPR a normy ISO/IEC 17065/2012.

11. Pro účely těchto pokynů se rozumí:

12. „*akreditací*“ subjektů pro vydávání osvědčení – viz bod 3 o výkladu pojmu akreditace pro účely článku 43 nařízení GDPR;

13. „*dodatečnými požadavky*“ požadavky, které stanoví příslušný dozorový úřad a podle kterých se provádí akreditace[4];

14. „*osvědčením*“ posouzení a nestranné ověření třetí stranou[5], že bylo prokázáno splnění kritérií pro vydávání osvědčení;

15. „*subjektem pro vydávání osvědčení*“ subjekt třetí strany, který je subjektem[6] posuzování shody[7] a který provozuje mechanismy pro vydávání osvědčení[8];

16. „*systémem vydávání osvědčení*“ systém vydávání osvědčení týkající se specifikovaných produktů, procesů a služeb, pro které platí stejné specifikované požadavky, specifická pravidla a postupy[9];

17. „kritérii“ nebo též kritérii pro vydávání osvědčení kritéria, na jejichž základě se osvědčení vydává (posouzení shody)[10];

18. „vnitrostátním akreditačním orgánem“ jediný orgán v daném členském státě určený v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008, který na základě státem delegované pravomoci provádí akreditaci[11].

3 VÝKLAD „AKREDITACE“ PRO ÚČELY ČLÁNKU 43 NAŘÍZENÍ GDPR

19. Nařízení GDPR „akreditaci“ nedefinuje. V čl. 2 bodě 10 nařízení (ES) č. 765/2008, kterým se stanoví obecné požadavky na akreditaci, je akreditace definována takto:

---

[4] Čl. 43 odst. 1, 3 a 6.

[5] Upozorňujeme, že podle normy ISO 17000 je potvrzení vydané třetí stranou (osvědčení) „použitelné na všechny předměty posuzování shody“ (bod 5.5) „s výjimkou samotných orgánů posuzujících shodu, u kterých je používána akreditace“ (bod 5.6).

[6] Viz bod 2.5 ISO 17000: „orgán, který vykonává služby v oblasti posuzování shody“ ISO 17011: „orgán, který vykonává služby v oblasti posuzování shody a který může být předmětem akreditace“, bod 3.12 normy ISO 17065.

[7] Činnost posuzování shody třetí stranou prováděná organizací, která je nezávislá na osobě nebo organizaci poskytující předmět a na uživatelském zájmu na tomto předmětu, viz bod 2.4 normy ISO 17000.

[8] Čl. 42 odst. 1 a 5 nařízení o GDPR.

[9] Viz bod 3.9 ve spojení s přílohou B normy ISO 17065.

[10] Viz čl. 42 odst. 5.

[11] Viz čl. 2 bod 11 nařízení (ES) č. 765/2008.

20. „potvrzení vnitrostátního akreditačního orgánu o tom, že subjekt posuzování shody splňuje požadavky stanovené harmonizovanými normami, a pokud je to relevantní, také veškeré další požadavky, včetně těch, které jsou stanoveny v příslušných odvětvových systémech, pro vykonávání konkrétní činnosti posuzování shody“.

21. V normě ISO/IEC 17011 se uvádí, že:

22. akreditací se rozumí „potvrzení vydané třetí stranou vztahující se k orgánu posuzování shody, které vyjadřuje formální potvrzení jeho kompetence provádět specifické činnosti posuzování shody“.

23. Čl. 43 odst. 1 stanoví:

24. „Aniž jsou dotčeny úkoly a pravomoci příslušného dozorového úřadu podle článků 57 a 58, osvědčení vydává a obnovuje subjekt pro vydávání osvědčení, který má příslušnou úroveň odborných znalostí ohledně ochrany údajů, a to poté, co informoval dozorový úřad s cílem umožnit případně výkon jeho pravomocí podle čl. 58 odst. 2 písm. h). Členské státy zajistí, aby byly tyto subjekty pro vydávání osvědčení akreditovány jedním nebo oběma z následujících orgánů:

    (a) dozorovým úřadem, který je příslušný podle článku 55 nebo 56, nebo
    (b) vnitrostátním akreditačním orgánem určeným v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008, v souladu s normou ISO/IEC 17065/2012 a s dodatečnými požadavky stanovenými dozorovým úřadem, který je příslušný podle článku 55 nebo 56.“

25. Pokud jde o nařízení GDPR, požadavky na akreditaci se budou řídit podle:

- normy ISO/IEC 17065/2012 a „dodatečných požadavků“ stanovených dozorovým úřadem, který je příslušný podle čl. 43 odst. 1 písm. b), pokud akreditaci provádí vnitrostátní akreditační orgán, a dozorovým úřadem, pokud akreditaci provádí sám tento úřad.

26. V obou případech musí konsolidované požadavky zahrnovat požadavky uvedené v čl. 43 odst. 2.

27. Evropský sbor pro ochranu osobních údajů uznává, že účelem akreditace je poskytnout oficiální stanovisko k odborné způsobilosti subjektu pro vydávání osvědčení (činnosti posuzování shody)[12]. Akreditaci z hlediska nařízení GDPR lze chápat jako:

28. osvědčování[13] toho, že subjekt pro vydávání osvědčení[14] je způsobilý k vydávání osvědčení podle článků 42 a 43 nařízení GDPR, prováděné vnitrostátním akreditačním orgánem a/nebo dozorovým úřadem, přičemž se zohlední norma ISO/IEC 17065/2012 a dodatečné požadavky stanovené dozorovým úřadem a/nebo Evropským sborem pro ochranu osobních údajů.

[12] Viz 15. bod odůvodnění nařízení (ES) č. 765/2008.
[13] Viz čl. 2 bod 10 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh.
[14] Viz definice termínu „akreditace“ podle normy ISO 17011.

4 AKREDITACE V SOULADU S ČL. 43 ODST. 1 NAŘÍZENÍ GDPR

29. Ustanovení čl. 43 odst. 1 připouští, že existuje několik možností akreditace subjektů pro vydávání osvědčení. Nařízení GDPR požaduje, aby dozorové úřady a členské státy definovaly postup akreditace subjektů pro vydávání osvědčení. Tato část stanoví způsoby akreditace uvedené v článku 43.

4.1 Úloha členských států

30. Ustanovení čl. 43 odst. 1 ukládá členským státům povinnost *zajistit*, aby byly subjekty pro vydávání osvědčení akreditovány, umožňuje však, aby si každý členský stát určil, kdo by měl odpovídat za provedení posouzení, na jehož základě se akreditace vydává. Podle čl. 43 odst. 1 existují tři možnosti, přičemž akreditaci provádí:

(1) pouze dozorový úřad na základě svých vlastních požadavků;
(2) pouze vnitrostátní akreditační orgán určený v souladu s nařízením (ES) č. 765/2008 a na základě normy ISO/IEC 17065/2012, jakož i v souladu s dodatečnými požadavky stanovenými příslušným dozorovým úřadem nebo
(3) jak dozorový úřad, tak vnitrostátní akreditační orgán (a v souladu se všemi požadavky uvedenými v podbodě 2 výše).

31. Je na jednotlivých členských státech, aby rozhodly, zda tyto akreditační činnosti bude provádět vnitrostátní akreditační orgán, nebo dozorový úřad, případně oba tyto orgány; každopádně by však měly zajistit, že budou k dispozici odpovídající zdroje[15].

4.2 Vztah k nařízení (ES) č. 765/2008

32. Evropský sbor pro ochranu osobních údajů konstatuje, že čl. 2 bod 11 nařízení (ES) č. 765/2008 definuje vnitrostátní akreditační orgán jako *„jediný* orgán v daném členském státě, který na základě státem delegované pravomoci provádí akreditaci“.

33. Čl. 2 bod 11 by mohl být považován za neslučitelný s čl. 43 odst. 1 nařízení GDPR, který umožňuje, aby akreditaci prováděl i jiný orgán než vnitrostátní akreditační orgán daného členského státu. Evropský sbor pro ochranu osobních údajů se domnívá, že záměrem právních předpisů EU je odchýlit se od obecné zásady, že by akreditaci měl provádět výhradně vnitrostátní akreditační orgán, a to tím, že se dozorovým úřadům svěří v souvislosti s akreditací subjektů pro vydávání osvědčení stejná pravomoc. Proto čl. 43 odst. 1 představuje *lex specialis* ve vztahu k čl. 2 bodu 11 nařízení č. 765/2008.

4.3 Úloha vnitrostátního akreditačního orgánu

34. Čl. 43 odst. 1 písm. b) stanoví, že vnitrostátní akreditační orgán bude akreditovat subjekty pro vydávání osvědčení v souladu s normou ISO/IEC 17065/2012 a dodatečnými požadavky stanovenými příslušným dozorovým úřadem.

35. Pro větší jasnost Evropský sbor pro ochranu osobních údajů konstatuje, že konkrétní odkaz na „odst. 1 písm. b)“ v čl. 43 odst. 3 znamená, že „tyto požadavky“ odkazují na „dodatečné požadavky“ stanovené příslušným dozorovým úřadem podle čl. 43 odst. 1 písm. b) a požadavky stanovené v čl. 43 odst. 2.

[15] Viz čl. 4 odst. 9 nařízení (ES) č. 765/2008.

36. V procesu akreditace uplatní vnitrostátní akreditační orgány dodatečné požadavky, které stanoví dozorové úřady.

37. Subjekt pro vydávání osvědčení se stávající akreditací na základě normy ISO/IEC 17065/2012 pro systémy vydávání osvědčení nesouvisející s nařízením GDPR, který by chtěl rozšířit rozsah své akreditace tak, aby zahrnovala osvědčení vydaná v souladu s nařízením GDPR, bude muset splnit dodatečné požadavky stanovené dozorovým úřadem, pokud bude akreditaci provádět vnitrostátní akreditační orgán. Pokud bude akreditaci pro vydávání osvědčení podle nařízení GDPR provádět pouze příslušný dozorový úřad, bude muset subjekt pro vydávání osvědčení žádající o akreditaci splnit požadavky stanovené tímto příslušným dozorovým úřadem.

4.4 Úloha dozorového úřadu

38. Evropský sbor pro ochranu osobních údajů konstatuje, že čl. 57 odst. 1 písm. q) stanoví, že dozorový úřad provádí akreditaci subjektu pro vydávání osvědčení v souladu s článkem 43 jakožto „úkol dozorového úřadu“ v souladu s článkem 57, a že čl. 58 odst. 3 písm. e) stanoví, že dozorový úřad má povolovací a poradní pravomoc akreditovat subjekty pro vydávání osvědčení podle článku 43. Znění čl. 43 odst. 1 umožňuje určitou pružnost, přičemž akreditační funkce dozorového úřadu by měla být chápána jako úkol pouze v příslušných případech. K objasnění této otázky může být použito právo členského státu. Přesto je v procesu akreditace vnitrostátním akreditačním orgánem po subjektu pro vydávání osvědčení v souladu s čl. 43 odst. 2 písm. a) požadováno, aby prokázal ke spokojenosti příslušného dozorového úřadu svoji nezávislost a odborné znalosti ohledně předmětu mechanismu vydávání osvědčení, který nabízí[16].

39. Pokud členský stát stanoví, že subjekty pro vydávání osvědčení má akreditovat dozorový úřad, měl by tento dozorový úřad stanovit požadavky na akreditaci, které budou mimo jiné zahrnovat požadavky uvedené v čl. 43 odst. 2. V porovnání s povinnostmi vztahujícími se k akreditaci subjektů pro vydávání osvědčení vnitrostátními akreditačními orgány uvádí článek 43 méně potřebných informací o požadavcích na akreditaci v případě, že akreditaci provádí sám dozorový úřad. V zájmu přispění k harmonizovanému přístupu k akreditaci by se akreditační kritéria uplatňovaná dozorovým úřadem měla řídit normou ISO/IEC 17065 a měla by být doplněna o dodatečné požadavky, které stanoví dozorový úřad v souladu s čl. 43 odst. 1 písm. b). Evropský sbor pro ochranu osobních údajů konstatuje, že ustanovení čl. 43 odst. 2 písm. a) až e) zohledňují a upřesňují požadavky normy ISO 17065, což přispěje k jednotnosti.

40. Pokud členský stát stanoví, že subjekty pro vydávání osvědčení mají být akreditovány vnitrostátními akreditačními orgány, dozorový úřad by měl stanovit dodatečné požadavky, jež budou doplňovat stávající ujednání ohledně akreditace uvedená v nařízení (ES) č. 765/2008 (kde se články 3 až 14 týkají organizace a provádění akreditací subjektů posuzování shody), a technická pravidla popisující metody a postupy subjektů pro vydávání osvědčení. V této souvislosti obsahuje nařízení (ES) č. 765/2008 další pokyny: čl. 2 bod 10 uvádí definici akreditace a odkazuje na „harmonizované normy“ a „veškeré další požadavky, včetně těch, které jsou stanoveny v příslušných odvětvových předpisech“. Z toho vyplývá, že dodatečné požadavky stanovené dozorovým úřadem by měly zahrnovat specifické požadavky

[16] Dodatečné požadavky stanovené dozorovým úřadem v souladu s čl. 43 odst. 1 písm. b) by měly upřesnit požadavky na nezávislost a odborné znalosti. Viz také příloha 1 těchto pokynů.

a měly by usilovat mimo jiné o snazší posuzování nezávislosti a úrovně odborných znalostí subjektů pro vydávání osvědčení v oblasti ochrany údajů, například jejich schopnosti hodnotit a vydávat osvědčení pro operace zpracování osobních údajů prováděné správci a zpracovateli v souladu s čl. 42 odst. 1. To zahrnuje odbornou způsobilost vyžadovanou pro odvětvové předpisy, a pokud jde o ochranu základních práv a svobod fyzických osob, a zejména jejich práva na ochranu osobních údajů[17]. Příloha těchto pokynů může napomoci příslušným dozorovým úřadům při stanovování „dodatečných požadavků" v souladu s čl. 43 odst. 1 písm. b) a čl. 43 odst. 3.

41. V čl. 43 odst. 6 se stanoví, že „[p]ožadavky podle odstavce 3 tohoto článku a kritéria pro vydávání osvědčení podle čl. 42 odst. 5 zveřejní dozorový úřad ve snadno přístupné formě". Proto se za účelem zajištění transparentnosti zveřejňují veškerá kritéria a požadavky, jež schválí dozorový úřad. Pokud jde o kvalitu subjektů pro vydávání osvědčení a důvěru v tyto subjekty, bylo by žádoucí, aby byly veškeré požadavky na akreditaci snadno dostupné veřejnosti.

4.5 Dozorový úřad působící jako subjekt pro vydávání osvědčení

42. V čl. 42 odst. 5 se stanoví, že dozorový úřad může vydávat osvědčení, nicméně nařízení GDPR nevyžaduje, aby byl pro splnění požadavků podle nařízení (ES) č. 765/2008 akreditován. Evropský sbor pro ochranu osobních údajů konstatuje, že čl. 43 odst. 1 písm. a), a zejména čl. 58 odst. 2 písm. h) a odst. 3 písm. a), e) a f), dávají dozorovým úřadům pravomoc provádět akreditaci i vydávat osvědčení a rovněž poskytovat poradenství, případně odebrat osvědčení nebo nařídit subjektu pro vydávání osvědčení, aby osvědčení nevydal.

43. Mohou nastat situace, kdy jsou oddělené úlohy a povinnosti týkající se akreditací a vydávání osvědčení vhodné nebo vyžadované, a to například pokud v daném členském státě existuje dozorový úřad i další subjekty pro vydávání osvědčení a všechny vydávají stejné typy osvědčení. Dozorové úřady by tedy měly přijmout dostatečná organizační opatření k oddělení úkolů podle nařízení GDPR, která upevní a zjednoduší mechanismy pro vydávání osvědčení a zároveň zajistí, aby se zabránilo střetům zájmů, které mohou z těchto úkolů vyplývat. Kromě toho by členské státy a dozorové úřady měly při vypracovávání vnitrostátních právních předpisů a postupů týkajících se akreditací a vydávání osvědčení v souladu s nařízením GDPR mít na paměti harmonizaci na evropské úrovni.

4.6 Požadavky na akreditaci

44. Příloha těchto pokynů popisuje, jak určit dodatečné požadavky na akreditaci. Uvádí příslušná ustanovení nařízení GDPR a navrhuje, které požadavky by dozorové úřady a vnitrostátní akreditační orgány měly zohlednit, aby zajistily dodržování nařízení GDPR.

45. Jak je stanoveno výše, jsou-li subjekty pro vydávání osvědčení akreditovány vnitrostátním akreditačním orgánem v souladu s nařízením (ES) č. 765/2008, pak norma ISO/IEC 17065/2012 bude příslušnou akreditační normou, kterou budou doplňovat dodatečné požadavky stanovené dozorovým úřadem. V čl. 43 odst. 2 se odrážejí obecná ustanovení normy ISO/IEC 17065/2012 s ohledem na ochranu základních práv podle nařízení GDPR. Rámec uvedený v příloze používá čl. 43 odst. 2 a normu ISO/IEC 17065/2012 jako základ pro určení požadavků a dalších kritérií týkajících se posuzování odborných znalostí subjektů pro vydávání osvědčení v oblasti ochrany údajů a jejich schopnosti dodržovat práva a svobody

[17] Čl. 1 odst. 2 nařízení GDPR.

fyzických osob s ohledem na zpracování osobních údajů zakotvené v nařízení GDPR. Evropský sbor pro ochranu osobních údajů konstatuje, že tento rámec má zejména zajistit, aby subjekty pro vydávání osvědčení měly příslušnou úroveň odborných znalostí týkajících se ochrany údajů v souladu s čl. 43 odst. 1.

46. Dodatečné požadavky na akreditaci stanovené dozorovým úřadem se budou vztahovat na všechny subjekty pro vydávání osvědčení, které požádají o akreditaci. Akreditační orgán posoudí, zda je dotčený subjekt pro vydávání osvědčení příslušný k vydávání osvědčení v souladu s dodatečnými požadavky a předmětem vydávání osvědčení. Budou uvedena konkrétní odvětví nebo oblasti osvědčování, pro které je daný subjekt pro vydávání osvědčení akreditován.

47. Evropský sbor pro ochranu osobních údajů rovněž konstatuje, že kromě požadavků normy ISO/IEC 17065/2012 jsou rovněž vyžadovány zvláštní odborné znalosti v oblasti ochrany údajů, pokud jiné, externí subjekty, například laboratoře nebo auditoři, provádějí některé části činností vydávání osvědčení jménem akreditovaného subjektu pro vydávání osvědčení. V takových případech není akreditace těchto externích subjektů podle samotného nařízení GDPR možná. Nicméně aby se zajistila vhodnost těchto subjektů pro jejich činnost jménem akreditovaných subjektů pro vydávání osvědčení, je nezbytné, aby akreditovaný subjekt pro vydávání osvědčení zaručil, že pokud jde o příslušnou prováděnou činnost, disponuje dotčený externí subjekt rovněž odbornými znalostmi v oblasti ochrany údajů, které se požadují po akreditovaném subjektu, a je schopen tyto znalosti prokázat.

48. Rámec pro určení dodatečných požadavků na akreditaci uvedený v příloze těchto pokynů nepředstavuje příručku postupů pro akreditační proces prováděný vnitrostátním akreditačním orgánem nebo dozorovým úřadem. Poskytuje návod týkající se struktury a metodiky, a tudíž i soubor nástrojů pro dozorové úřady ke stanovení dodatečných požadavků na akreditaci.

PŘÍLOHA 1

Příloha 1 obsahuje pokyny pro určení „dodatečných“ požadavků na akreditaci v souvislosti s normou ISO/IEC 17065/2012 a v souladu s čl. 43 odst. 1 písm. b) a čl. 43 odst. 3 nařízení GDPR.

V příloze se uvádějí navrhované požadavky, které vypracuje dozorový úřad pro ochranu údajů a které se použijí při akreditaci subjektu pro vydávání osvědčení vnitrostátním akreditačním orgánem nebo příslušným dozorovým úřadem[18]. Dozorový úřad tyto dodatečné požadavky před jejich schválením sdělí Evropskému sboru pro ochranu osobních údajů v souladu s čl. 64 odst. 1 písm. c).

Tato příloha by měla být vykládána ve spojení s normou ISO/IEC 17065/2012. Číslování jednotlivých bodů v této příloze odpovídá číslování použitému v normě ISO/IEC 17065/2012. Pokud orgány dozoru provádějí akreditaci podle čl. 43 odst. 1 písm. a), lze doporučit, aby byl tento přístup uplatňován, kdykoli je to proveditelné. Tím se podpoří harmonizovaná akreditace v celé EU.

Bez ohledu na následující pokyny či neexistenci pokynů ve vztahu k určitému bodu normy ISO/IEC 17065/2012 může příslušný dozorový úřad pro konkrétní bod stanovit další dodatečné požadavky, pokud je to v souladu s vnitrostátním právem.

0 ÚVOD

[Tento bod je zamýšlen pro případně dohodnuté podmínky spolupráce mezi vnitrostátním akreditačním orgánem a dozorovým úřadem pro ochranu údajů, které například upravují, kdo by měl být odpovědný za přijímání žádostí nebo jakým způsobem organizovat uznávání schválených kritérií v rámci akreditačního procesu.]

1 OBLAST PŮSOBNOSTI[19]

Oblast působnosti normy ISO/IEC 17065/2012 se uplatňuje v souladu s nařízením GDPR. Další informace poskytují pokyny týkající se akreditace a vydávání osvědčení. Vnitrostátní akreditační orgán a příslušný dozorový úřad by měly při provádění posouzení v rámci akreditačního procesu zohlednit rozsah mechanismu pro vydávání osvědčení (například osvědčení pro operace zpracování cloudových služeb), zejména pokud jde o kritéria, odbornou způsobilost a metodiku hodnocení. Široká oblast působnosti normy ISO/IEC 17065/2012 vztahující se na produkty, procesy a služby by neměla snižovat nebo převážit požadavky nařízení GDPR, např. mechanismus řízení nemůže být jediným prvkem mechanismu pro vydávání osvědčení, neboť vydávání osvědčení musí zahrnovat zpracování osobních údajů, tj. operace zpracování. V souladu s čl. 42 odst. 1 se vydávání osvědčení podle nařízení GDPR vztahuje pouze na operace zpracování prováděné správci a zpracovateli.

2 ODKAZY NA NORMY

Nařízení GDPR má přednost před normou ISO/IEC 17065/2012. Pokud se v dodatečných požadavcích nebo v rámci mechanismu pro vydávání osvědčení odkazuje na jiné normy ISO, musí být vykládány v souladu s požadavky stanovenými v nařízení GDPR.

---

[18] Informace o postupu schvalování kritérií pro vydávání osvědčení jsou obsaženy v bodě 4 pokynů pro vydávání osvědčení.

[19] Číslování odkazuje na normu ISO/IEC 17065/2012.

3 POJMY A DEFINICE

V rámci této přílohy se použijí podmínky a definice uvedené v pokynech týkajících se akreditace (WP 261) a vydávání osvědčení (Evropský sbor pro ochranu osobních údajů č. 1/2018), které mají přednost před definicemi norem ISO.

4 OBECNÉ POŽADAVKY NA AKREDITACI

4.1 Právní a smluvní záležitosti

4.1.1 Právní odpovědnost

Subjekt pro vydávání osvědčení by měl být schopen vnitrostátnímu akreditačnímu orgánu nebo příslušnému dozorovému úřadu (kdykoli) prokázat, že používá aktualizované postupy, které jsou v souladu s právními povinnostmi stanovenými v podmínkách akreditace, včetně dodatečných požadavků týkajících se uplatňování nařízení 2016/679/ES. Vzhledem k tomu, že subjekt pro vydávání osvědčení je sám správcem/zpracovatelem údajů, musí být schopen prokázat, že jím uplatňované postupy a opatření jsou v souladu s nařízením 2016/679/ES, zejména pokud jde o správu osobních údajů organizace klienta a nakládání s nimi v rámci procesu vydávání osvědčení.

Příslušný dozorový úřad může rozhodnout o doplnění dalších požadavků a postupů, na jejichž základě se před akreditací ověří, zda subjekty pro vydávání osvědčení splňují požadavky nařízení GDPR.

4.1.2 Dohoda o vydávání osvědčení

Minimální požadavky na dohodu o vydávání osvědčení se doplňují o tyto body:

Subjekt pro vydávání osvědčení musí kromě požadavků normy ISO/IEC 17065/2012 prokázat, že jeho dohody o vydávání osvědčení:

1. požadují, aby žadatel vždy dodržoval jak obecné požadavky na vydávání osvědčení ve smyslu bodu 4.1.2.2 písm. a) normy ISO/IEC 17065/2012, tak i kritéria schválená příslušným dozorovým úřadem nebo Evropským sborem pro ochranu osobních údajů v souladu s čl. 43 odst. 2 písm. b) a čl. 42 odst. 5;
2. požadují, aby žadatel zachoval vůči příslušnému dozorovému úřadu úplnou transparentnost, pokud jde o postup vydávání osvědčení, včetně smluvně důvěrných záležitostí souvisejících s dodržováním požadavků na ochranu údajů podle čl. 42 odst. 7 a čl. 58 odst. 1 písm. c);
3. nesnižují odpovědnost žadatele za soulad s nařízením 2016/679/ES a nejsou jím dotčeny úkoly a pravomoci dozorových úřadů, které jsou příslušné v souladu s čl. 42 odst. 5;
4. požadují, aby žadatel poskytl subjektu pro vydávání osvědčení veškeré informace a přístup ke svým činnostem zpracování, které jsou nezbytné pro provedení postupu vydávání osvědčení, v souladu s čl. 42 odst. 6;
5. požadují, aby žadatel dodržoval příslušné lhůty a postupy. V dohodě o vydávání osvědčení musí být uvedeno, že lhůty a postupy, které vyplývají například z programu pro vydávání osvědčení nebo z jiných předpisů, musí být dodržovány;
6. s ohledem na bod 4.1.2.2 písm. c) podbod 1 normy ISO/IEC 17065/2012 stanoví pravidla týkající se platnosti, obnovení a odebrání osvědčení podle čl. 42 odst. 7 a čl. 43 odst. 4, včetně pravidel stanovujících vhodné intervaly pro přehodnocení nebo přezkum (správnost) v souladu s čl. 42 odst. 7;

7. umožňují, aby subjekt pro vydávání osvědčení zveřejnil veškeré informace potřebné pro udělení osvědčení podle čl. 42 odst. 8 a čl. 43 odst. 5;
8. zahrnují pravidla pro nezbytná preventivní opatření týkající se šetření stížností ve smyslu bodu 4.1.2.2 písm. c) podbodu 2 a bodu 4.1.2.2 písm. j) a obsahují také výslovná prohlášení o struktuře a o postupu vyřizování stížností v souladu s čl. 43 odst. 2 písm. d);
9. kromě minimálních požadavků uvedených v bodě 4.1.2.2 normy ISO/IEC 17065/2012 by měly být rovněž řešeny důsledky pro klienta v případě, že se jej dotýká odebrání nebo pozastavení akreditace subjektu pro vydávání osvědčení;
10. požadují, aby žadatel informoval subjekt pro vydávání osvědčení v případě významných změn, pokud jde o jeho skutečnou nebo právní situaci a jeho produkty, procesy a služby, jichž se osvědčení týká.

4.1.3 Používání pečetí a známek dokládajících ochranu údajů

Osvědčení, pečeti a známky se použijí jen v případě, že je zajištěn soulad s články 42 a 43 a s pokyny týkajícími se akreditace a vydávání osvědčení.

4.2 Nestrannost a její řízení

Akreditační orgán zajistí, aby vedle požadavku stanoveného v bodě 4.2 normy ISO/IEC 17065/2012:

1. subjekt pro vydávání osvědčení splňoval dodatečné požadavky příslušného dozorového úřadu (podle čl. 43 odst. 1 písm. b))
    a. a v souladu s čl. 43 odst. 2 písm. a) předložil oddělené důkazy o své nezávislosti. Týká se to zejména důkazů o financování subjektu pro vydávání osvědčení ve vztahu k záruce nestrannosti;
    b. jeho úkoly a povinnosti nevedly ke střetu zájmů podle čl. 43 odst. 2 písm. e);
2. subjekt pro vydávání osvědčení neměl žádné relevantní spojení s klientem, kterého posuzuje.

4.3 Odpovědnost a financování

Akreditační orgán kromě požadavku uvedeného v bodě 4.3.1 normy ISO/IEC 17065/2012 pravidelně zajišťuje, aby měl subjekt pro vydávání osvědčení k dispozici vhodná opatření (např. pojištění či rezervy), jimiž bude moci krýt svoji odpovědnost v zeměpisných oblastech, v nichž působí.

4.4 Nediskriminační podmínky

Pokud je to v souladu s vnitrostátním právem, dozorový úřad může formulovat dodatečné požadavky.

4.5 Důvěrnost

Pokud je to v souladu s vnitrostátním právem, dozorový úřad může formulovat dodatečné požadavky.

4.6 Veřejně dostupné informace

Akreditační orgán kromě požadavku uvedeného v bodě 4.6 normy ISO/IEC 17065/2012 od subjektu pro vydávání osvědčení vyžaduje přinejmenším, aby:

1. všechny verze (současné i předchozí) schválených kritérií použitých ve smyslu čl. 42 odst. 5 i všechny postupy vydávání osvědčení byly zveřejněny a byly veřejnosti snadno dostupné, přičemž se v nich má obecně uvádět příslušná doba platnosti;
2. informace o postupech vyřizování stížností a o odvoláních byly zveřejněny v souladu s čl. 43 odst. 2 písm. d).

5 STRUKTURÁLNÍ POŽADAVKY, ČL. 43 ODST. 4 („ŘÁDNÉ“ POSOUZENÍ)

5.1 Organizační struktura a nejvyšší vedení

Dodatečné požadavky může stanovit dozorový úřad.

5.2 Mechanismy pro zajištění nestrannosti

Dodatečné požadavky může stanovit dozorový úřad.

6 POŽADAVKY NA ZDROJE

6.1 Pracovníci subjektu pro vydávání osvědčení

Akreditační orgán kromě požadavku uvedeného v bodě 6 normy ISO/IEC 17065/2012 zaručí, aby pracovníci každého subjektu pro vydávání osvědčení:

1. prokázali přiměřené a průběžné odborné znalosti (vědomosti a zkušenosti) týkající se ochrany údajů podle čl. 43 odst. 1;
2. jednali nezávisle a měli průběžné odborné znalosti týkající se předmětu osvědčení podle čl. 43 odst. 2 písm. a) a nedocházelo u nich ke střetu zájmů podle čl. 43 odst. 2 písm. e);
3. učinili závazek, že budou dodržovat kritéria uvedená v čl. 42 odst. 5 v souladu s čl. 43 odst. 2 písm. b);
4. měli relevantní a odpovídající znalosti a zkušenosti v oblasti uplatňování právních předpisů o ochraně údajů;
5. měli v příslušných případech relevantní a odpovídající znalosti a zkušenosti v oblasti technických a organizačních opatření na ochranu údajů.
6. mohli doložit zkušenosti v oblastech uvedených v dodatečných požadavcích bodů 6.1.1, 6.1.4 a 6.1.5, konkrétně:

pokud jde o pracovníky s technickou odborností:

- získali kvalifikaci v odpovídající oblasti technické odbornosti přinejmenším na úrovni 6 evropského rámce kvalifikací[20] nebo získali uznávaný chráněný titul (např. Dipl. Ing.) v rámci příslušného regulovaného povolání nebo měli rozsáhlé odborné zkušenosti,
- *pracovníci odpovědní za rozhodnutí o vydání osvědčení* měli rozsáhlé odborné zkušenosti v oblasti určování a provádění opatření na ochranu údajů,
- *pracovníci odpovědní za hodnocení* měli odborné zkušenosti v oblasti technické ochrany údajů a znalosti a zkušenosti týkající se srovnatelného postupu (např. osvědčení/audity), a je-li to požadováno, byli registrováni.

Pracovníci musí doložit, že si uchovávají specifické znalosti v oblasti technických a auditorských dovedností prostřednictvím soustavného profesního rozvoje.

Pokud jde o pracovníky s právní odborností:

- Právnické studium na vysoké škole uznané na úrovni EU nebo uznané státem, trvající alespoň osm semestrů včetně akademického magisterského titulu (LL.M.), nebo rovnocenné studium, případně rozsáhlé odborné zkušenosti.

[20] Viz srovnávací nástroj pro rámec kvalifikací na adrese https://ec.europa.eu/ploteus/en/compare?

- *Pracovníci odpovědní za rozhodnutí o vydání osvědčení* musí doložit rozsáhlé odborné zkušenosti v oblasti právních předpisů o ochraně údajů a být registrováni v souladu s požadavky daného členského státu.
- *Pracovníci odpovědní za hodnocení* doloží alespoň dvouletou odbornou praxi v oblasti práva týkajícího se ochrany údajů a prokáží znalosti a zkušenosti týkající se srovnatelných postupů (např. osvědčení/audity), a požaduje-li to členský stát, musí být registrováni.
    - Pracovníci musí prokázat, že si uchovávají specifické znalosti v oblasti technických a auditorských dovedností prostřednictvím soustavného profesního rozvoje.

6.2 Zdroje pro hodnocení

Pokud je to v souladu s vnitrostátním právem, dozorový úřad může formulovat dodatečné požadavky.

7 POŽADAVKY NA POSTUPY, ČL. 43 ODST. 2 PÍSM. C) A D)

7.1 Obecně

Akreditační orgán kromě požadavku uvedeného v bodě 7.1 normy ISO/IEC 17065/2012 zaručí:

1. aby subjekty pro vydávání osvědčení při předkládání žádostí dodržovaly dodatečné požadavky příslušného dozorového úřadu (podle čl. 43 odst. 1 písm. b)) tak, aby jejich úkoly a povinnosti nevedly ke střetu zájmů podle čl. 43 odst. 2 písm. b);
2. že informuje příslušný dozorový úřad před tím, než subjekt pro vydávání osvědčení začne používat schválenou evropskou pečeť ochrany údajů v novém členském státě ze satelitní kanceláře.

7.2 Uplatňování

Navíc k bodu 7.2 normy ISO/IEC 17065/2012 by se mělo požadovat, aby

1. předmět osvědčení (cíl hodnocení) byl v žádosti podrobně popsán. To zahrnuje rovněž rozhraní a předávání do jiných systémů a organizací, protokoly a další záruky;
2. v žádosti bylo uvedeno, zda jsou využíváni zpracovatelé, a pokud jsou zpracovatelé žadatelem, musí být popsány jejich povinnosti a úkoly a žádost musí obsahovat příslušnou smlouvu (smlouvy) se správcem/zpracovatelem.

7.3 Přezkum žádosti

Navíc k bodu 7.3 normy ISO/IEC 17065/2012 by se mělo požadovat, aby

1. v dohodě o vydávání osvědčení byly stanoveny závazné metody hodnocení, pokud jde o cíl hodnocení;
2. posouzení dostatečnosti odborných znalostí uvedené v bodě 7.3 písm. e) zohledňovalo v přiměřeném rozsahu jak technickou, tak právní odbornost v oblasti ochrany údajů.

7.4 Hodnocení

Navíc k bodu 7.4 normy ISO/IEC 17065/2012 musí mechanismy pro vydávání osvědčení popisovat dostatečné metody hodnocení pro posouzení souladu operace (operací) zpracování s kritérii pro vydávání osvědčení, což v odpovídajících případech zahrnuje například:

1. metodu posuzování nezbytnosti a přiměřenosti operací zpracování ve vztahu k jejich účelu a k dotčeným subjektům údajů;

2. metodu hodnocení rozsahu, skladby a posouzení všech rizik, která správce a zpracovatel vezme v úvahu s ohledem na právní důsledky podle článků 30, 32, 35 a 36 nařízení GDPR, jakož i s ohledem na vymezení technických a organizačních opatření podle článků 24, 25 a 32 nařízení GDPR, pokud se výše uvedené články vztahují na předmět osvědčení, a
3. metodu posuzování nápravných opatření a rovněž záruk a postupů, jež mají zajistit ochranu osobních údajů v souvislosti s jejich zpracováním, které se má vztahovat na předmět osvědčení, a prokázat, že jsou splněny právní požadavky stanovené v těchto kritériích, a
4. dokumentaci metod a zjištění.

Subjekt pro vydávání osvědčení by měl mít povinnost zajistit, aby tyto metody hodnocení byly standardizované a obecně použitelné. To znamená, že srovnatelné metody hodnocení se používají pro srovnatelné cíle hodnocení. Veškeré odchylky od tohoto postupu musí subjekt pro vydávání osvědčení odůvodnit.

Navíc k bodu 7.4.2 normy ISO/IEC 17065/2012 by mělo být povoleno, aby hodnocení prováděli externí odborníci, kteří byli uznáni subjektem pro vydávání osvědčení.

Navíc k bodu 7.4.5 normy ISO/IEC 17065/2012 by se mělo požadovat, aby vydávání osvědčení o ochraně údajů v souladu s články 42 a 43 nařízení GDPR, které se již vztahuje na část předmětu osvědčení, mohlo být zahrnuto do stávajícího procesu vydávání osvědčení. Nestačí však zcela nahradit (částečná) hodnocení. Subjekt pro vydávání osvědčení je povinen ověřit splnění kritérií. Pro účely uznání je v každém případě nutné, aby byla k dispozici úplná hodnotící zpráva nebo informace, které umožní vyhodnotit předchozí činnost v oblasti vydávání osvědčení a její výsledky. Prohlášení o osvědčení nebo podobné potvrzení o osvědčení by nemělo být považováno za dostatečné k nahrazení zprávy.

Navíc k bodu 7.4.6 normy ISO/IEC 17065/2012 by se mělo požadovat, aby subjekt pro vydávání osvědčení ve svém mechanismu pro vydávání osvědčení podrobně uvedl, jakým způsobem informace požadované v bodě 7.4.6 informují klienta (žadatele o osvědčení) o neshodách v rámci mechanismu pro vydávání osvědčení. V dané souvislosti by měla být vymezena alespoň povaha a načasování těchto informací.

Navíc k bodu 7.4.9 normy ISO/IEC 17065/2012 by se mělo požadovat, aby dokumentace byla na požádání plně přístupná dozorovému úřadu pro ochranu údajů.

7.5 Přezkum

Navíc k bodu 7.5 normy ISO/IEC 17065/2012 jsou vyžadovány postupy pro vydávání, pravidelný přezkum a odebírání příslušných osvědčení podle čl. 43 odst. 2 a čl. 43 odst. 3.

7.6 Rozhodnutí o vydání osvědčení

Navíc k bodu 7.6.1 normy ISO/IEC 17065/2012 by měl mít subjekt pro vydávání osvědčení povinnost ve svých postupech podrobně stanovit, jakým způsobem je zajištěna jeho nezávislost a odpovědnost, co se týče jednotlivých rozhodnutí o vydání osvědčení.

7.7 Dokumentace týkající se vydávání osvědčení

Navíc k bodu 7.7.1 písm. e) normy ISO/IEC 17065/2012 a v souladu s čl. 42 odst. 7 nařízení GDPR by se mělo požadovat, aby doba platnosti osvědčení nepřekročila tři roky.

Navíc k bodu 7.7.1 písm. e) normy ISO/IEC 17065/2012 by se mělo požadovat, aby období zamýšleného monitorování ve smyslu bodu 7.9 bylo rovněž zdokumentováno.

Navíc k bodu 7.7.1 písm. f) normy ISO/IEC 17065/2012 by subjekt pro vydávání osvědčení měl být povinen v dokumentaci týkající se vydávání osvědčení uvést předmět osvědčení (v příslušném případě uvést status, pokud jde o verzi, nebo podobné charakteristiky).

7.8 Rejstřík produktů, které získaly osvědčení

Navíc k bodu 7.8 normy ISO/IEC 17065/2012 by subjekt pro vydávání osvědčení měl mít povinnost uchovávat informace o produktech, procesech a službách, které získaly osvědčení, dostupné interně i pro veřejnost. Subjekt pro vydávání osvědčení zveřejní shrnutí hodnotící zprávy. Cílem tohoto shrnutí je zajistit transparentnost v souvislosti s tím, co bylo předmětem osvědčení a jakým způsobem proběhlo posouzení. Vysvětlí se v něm například:

(a) rozsah osvědčení a jasný popis předmětu osvědčení;

(b) příslušná kritéria pro vydávání osvědčení (včetně statusu, pokud jde o verzi nebo funkce);

(c) metody hodnocení a provedené zkoušky a

(d) výsledek (výsledky).

Navíc k bodu 7.8 normy ISO/IEC 17065/2012 a podle čl. 43 odst. 5 nařízení GDPR informuje subjekt pro vydávání osvědčení příslušné dozorové úřady o důvodech udělení nebo zrušení požadovaného osvědčení.

7.9 Dozor

Navíc k bodům 7.9.1, 7.9.2 a 7.9.3 normy ISO/IEC 17065/2012 a podle čl. 43 odst. 2 písm. c) nařízení GDPR by měla být povinná pravidelná monitorovací opatření k zachování osvědčení během sledovacího období.

7.10 Změny ovlivňující osvědčení

Navíc k bodům 7.10.1 a 7.10.2 normy EN ISO/IEC 17065/2012 se mezi změny ovlivňující osvědčení, které má posoudit subjekt pro vydávání osvědčení, zahrnují: změny právních předpisů o ochraně údajů, přijímání aktů Evropské komise v přenesené pravomoci v souladu s čl. 43 odst. 8 a čl. 43 odst. 9, rozhodnutí Evropského sboru pro ochranu osobních údajů a soudní rozhodnutí týkající se ochrany údajů. Postupy týkající se těchto změn, které je třeba dohodnout, by mohly zahrnovat například: přechodná období, postup schvalování příslušným dozorovým úřadem, opětovné posouzení příslušného předmětu osvědčení a vhodná opatření pro zrušení osvědčení, jestliže operace zpracování, která získala osvědčení, již není v souladu s aktualizovanými kritérii.

7.11 Ukončení, omezení, pozastavení nebo odebrání osvědčení

Navíc k bodu 7.11.1 normy ISO/IEC 17065/2012 by od subjektu pro vydávání osvědčení mělo být požadováno, aby v příslušných případech o přijatých opatřeních a o trvání, omezení, pozastavení nebo odebrání osvědčení neprodleně písemně informoval příslušný dozorový úřad a vnitrostátní akreditační orgán.

Podle čl. 58 odst. 2 písm. h) je subjekt pro vydávání osvědčení povinen přijímat rozhodnutí a pokyny od příslušného dozorového úřadu ohledně odebrání nebo nevydání osvědčení klientovi (žadateli), jestliže požadavek na osvědčení (již) není splněn.

7.12 Záznamy

Subjekt pro vydávání osvědčení by měl mít povinnost uchovávat veškerou dokumentaci tak, aby byla kompletní, srozumitelná, aktualizovaná a bylo možné ji podrobit auditu.

7.13 Stížnosti a odvolání, čl. 43 odst. 2 písm. d)

Navíc k bodu 7.13.1 normy ISO/IEC 17065/2012 by subjekt pro vydávání osvědčení měl být povinen definovat:

(a) kdo může podat stížnost nebo vznést námitku;

(b) kdo ji zpracuje na straně subjektu pro vydávání osvědčení;

(c) která ověřování se v této souvislosti uskuteční a

(d) možnosti konzultací zúčastněných stran.

Navíc k bodu 7.13.2 normy ISO/IEC 17065/2012 by subjekt pro vydávání osvědčení měl být povinen definovat:

(a) jak a komu musí být takové potvrzení poskytnuto;

(b) příslušné lhůty a

(c) jaké procesy je třeba zahájit později.

Navíc k bodu 7.13.1 normy ISO/IEC 17065/2012 musí subjekt pro vydávání osvědčení definovat, jak je zajištěno oddělení mezi činnostmi vydávání osvědčení a vyřizováním odvolání a stížností.

8 POŽADAVKY NA SYSTÉM ŘÍZENÍ

Všeobecným požadavkem systému řízení podle bodu 8 normy ISO/IEC 17065/2012 je, aby provádění všech požadavků uvedených v předchozích bodech v rámci rozsahu mechanismu pro vydávání osvědčení akreditovaným subjektem pro vydávání osvědčení bylo dokumentováno, hodnoceno, kontrolováno a monitorováno nezávisle.

Hlavní zásadou řízení je definovat takový systém, který umožní, aby cíle řízení byly stanovovány účinně a efektivně, a to zejména provádění služeb vydávání osvědčení prostřednictvím vhodných specifikací. To vyžaduje transparentnost a ověřitelnost provádění požadavků na akreditaci subjektem pro vydávání osvědčení a jejich trvalé dodržování.

Za tímto účelem musí systém řízení stanovit metodiku jednak pro dosažení a kontrolu těchto požadavků v souladu s předpisy o ochraně údajů, jednak pro jejich průběžnou kontrolu ze strany samotného akreditovaného subjektu.

Tyto zásady řízení a jejich zdokumentované provádění musí být transparentní a musí být zpřístupněny akreditovaným subjektem pro vydávání osvědčení podle akreditačního postupu na základě článku 58 a poté na žádost dozorového úřadu pro ochranu údajů kdykoli během šetření, a to v podobě přezkumu ochrany údajů podle čl. 58 odst. 1 písm. b) nebo přezkumu osvědčení, která byla vydána v souladu s čl. 42 odst. 7, podle čl. 58 odst. 1 písm. c).

Akreditovaný subjekt pro vydávání osvědčení musí trvale a nepřetržitě zveřejňovat, jaká osvědčování byla provedena a na jakém základě (resp. mechanismy či systémy vydávání osvědčení), jak dlouho jsou osvědčení platná a podle jakého rámce a podmínek (100. bod odůvodnění).

8.1 Všeobecné požadavky na systém řízení

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

8.2 Dokumentace systému řízení

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

8.3 Kontrola dokumentů

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

8.4 Kontrola záznamů

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

8.5 Přezkoumání řízení

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

8.6 Interní audity

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

8.7 Nápravná opatření

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

8.8 Preventivní opatření

Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

9 DOPLŇKOVÉ POŽADAVKY[21]

9.1 Aktualizace metod hodnocení

Subjekt pro vydávání osvědčení zavede postupy pro aktualizaci metod hodnocení k použití v rámci hodnocení podle bodu 7.4. Aktualizace se musí uskutečnit v závislosti na změnách právního rámce, příslušných rizicích a stavu techniky a nákladech na provádění technických a organizačních opatření.

9.2 Udržování odborných znalostí

Subjekty pro vydávání osvědčení stanoví postupy k zajištění odborné přípravy svých zaměstnanců, která jim umožní aktualizovat si dovednosti s ohledem na vývoj uvedený v bodě 9.1.

9.3 Odpovědnosti a pravomoci

9.3.1 Komunikace mezi subjektem pro vydávání osvědčení a jeho klienty

Musí být zavedeny metody pro provádění vhodných postupů a komunikačních struktur mezi subjektem pro vydávání osvědčení a jeho klientem. To zahrnuje:

1. vedení dokumentace úkolů a odpovědností akreditovaným subjektem pro vydávání osvědčení pro účely:
    a. žádostí o informace nebo
    b. umožnění kontaktu v případě stížnosti týkající se osvědčení;
2. zachování postupu podávání žádostí pro účely:
    a. informací o stavu žádosti;
    b. hodnocení provedených příslušným dozorovým úřadem, pokud jde o
        i. zpětnou vazbu;
        ii. rozhodnutí učiněná příslušným dozorovým úřadem.

9.3.2 Dokumentace hodnotících činností

Dodatečné požadavky může stanovit dozorový úřad.

[21] Příslušný dozorový úřad může v souladu s vnitrostátním právem stanovit a doplnit další požadavky.

9.3.3 Vyřizování stížností

Vyřizování stížností bude zavedeno jako nedílná součást systému řízení, který zejména provádí požadavky uvedené v bodě 4.1.2.2 písm. c), bodě 4.1.2.2 písm. j), bodě 4.6 písm. d) a bodě 7.13 normy ISO/IEC 17065/2012.

Relevantní stížnosti a námitky by měly být sděleny příslušnému dozorovému úřadu.

9.3.4 Řízení postupů odebrání akreditace

Postupy v případě pozastavení nebo odebrání akreditace musí být začleněny do systému řízení subjektu pro vydávání osvědčení, včetně oznámení tohoto kroku klientům.