PRACOVNÍ SKUPINA PODLE ČLÁNKU 29

WP261

Návrh vodítek pro akreditaci subjektů vydávajících osvědčení podle Nařízení (EU) 2016/679

Schváleno dne 6. února 2018

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na články 29 a 30 uvedené směrnice

a s ohledem na svůj jednací řád,

PŘIJALA TATO VODÍTKA:

Obsah

Vodítka pro akreditaci subjektů vydávajících osvědčení podle článku 43 obecného nařízení o ochraně osobních údajů (2016/679)

1 Úvod

Obecné nařízení o ochraně osobních údajů (Nařízení (EU) 2016/679, dále jen „obecné nařízení"), které nabude účinnosti 25. května 2018, stanovuje modernizovaný, na odpovědnost a základní práva orientovaný právní rámec ochrany osobních údajů v Evropě. Středobodem této nové úpravy jsou opatření usnadňující dosáhnout souladu s ustanoveními obecného nařízení. Patří sem požadavky mandatorní za určitých okolností (včetně jmenování pověřence pro ochranu osobních údajů a provádění posouzení vlivu na ochranu osobních údajů), jakož i opatření dobrovolná, např. etické kodexy a certifikační mechanismy.

V rámci zavedení certifikačních mechanismů, pečetí a známek dokládajících ochranu osobních údajů, musí členské státy podle článku 43 odst. 1 obecného nařízení zajistit, aby subjekty pro vydávání osvědčení podle článku 42 odst. 1 byly akreditovány jedním nebo oběma orgány, tedy příslušným dozorovým úřadem nebo vnitrostátním akreditačním orgánem. Pokud akreditaci provádí vnitrostátní akreditační orgán v souladu s normou EN-ISO/IEC 17065/2012, musí být uplatněny i dodatečné požadavky ze strany příslušného dozorového úřadu.

Smysluplné certifikační mechanismy mohou zkvalitnit soulad s obecným nařízením i transparentnost vůči subjektům údajů i v oblasti obchodních vztahů B2B, například mezi správci a zpracovateli. Správci a zpracovatelé budou těžit z atestace nezávislou třetí stranou za účelem prokázání souladu svých operací zpracování.[1]

Pracovní skupina podle článku 29 (WP29) je toho názoru, že ohledně akreditace je potřeba poskytnout pokyny. Mimořádná hodnota a cíl akreditace spočívá ve skutečnosti, že jde o autoritativní vyjádření způsobilosti subjektů pro vydávání osvědčení, jež přispívá k vytváření důvěry v certifikační mechanismus.

Cílem těchto vodítek je poskytnout návod, jak vykládat a uplatňovat ustanovení článku 43 obecného nařízení. Zvláště pak mají pomoci členským státům, dozorovým úřadům a vnitrostátním akreditačním orgánům zavést sourodou a harmonizovanou základnu pro akreditaci subjektů pro vydávání osvědčení, které vydávají certifikáty v souladu s obecným nařízením.

[1] Recitál 100 obecného nařízení říká, že zavedení mechanismů pro vydávání osvědčení může zvýšit transparentnost a lépe zajistit soulad s nařízením, a umožnit subjektům údajů posoudit úroveň ochrany údajů u příslušných produktů a služeb.

2 Rozsah

Tato vodítka:

- Vysvětlují účel akreditace v kontextu obecného nařízení;
- Vysvětlují dostupné způsoby akreditace subjektů pro vydávání osvědčení podle článku 43 odst. 1 a vyzdvihují hlavní otázky, které je třeba vzít v potaz;
- Poskytují rámec pro zavedení dodatečných akreditačních požadavků v případě, kdy akreditaci vykonává vnitrostátní akreditační orgán;
- Poskytují rámec pro zavedení akreditačních požadavků v případě, kdy akreditaci vykonává dozorový úřad.

Tato vodítka nejsou příručkou postupů pro akreditaci subjektů pro vydávání osvědčení souladnou s obecným nařízením. Nevytváří nový technický standard pro akreditaci subjektů pro vydávání osvědčení pro účely obecného nařízení.

Tato vodítka jsou určena:

- Členským státům, které musí zajistit, aby subjekty pro vydávání osvědčení byly akreditovány dozorovým úřadem a/nebo vnitrostátním akreditačním orgánem;

- Vnitrostátním akreditačním orgánům, které akreditují subjekty pro vydávání osvědčení podle článku 43 odst. 1 písm. b);

- Příslušnému dozorovému úřadu (a v relevantních případech Evropskému sboru pro ochranu osobních údajů - EDPB), který stanovuje „dodatečné požadavky“ k těm, jež jsou uvedeni v normě EN-ISO/IEC 17065/2012[2], když akreditaci provádí vnitrostátní akreditační orgán podle článku 43 odst. 1 písm. b);

- Příslušnému dozorovému úřadu (a v relevantních případech EDPB), který stanovuje akreditační požadavky pro situaci, kdy akreditaci provádí dozorový úřad podle článku 43 odst. 1 písm. a);

- Dalším zainteresovaným stranám, jako jsou budoucí subjekty pro vydávání osvědčení nebo vlastníci certifikačních schémat stanovující certifikační kritéria a postupy[3].

[2] Mezinárodní organizace pro normalizaci: Posuzování shody - Požadavky na orgány certifikující produkty, procesy a služby.
[3] Vlastníkem schématu je identifikovatelná organizace, která sestavila certifikační kritéria a požadavky, vůči kterým má být shoda posuzována. Akreditace je na organizaci, která posouzení provádí (článek 43 odst. 4) vůči požadavkům podle certifikačního schématu a vydává certifikáty (tj. subjekt pro vydávání osvědčení, nazývaný také subjekt posuzování shody). Organizace provádějící posouzení může být tou samou organizací, která vyvinula a vlastní schéma, mohou však existovat situace, kdy je jedna organizace vlastníkem schématu a druhá (nebo více jiných) posudky provádí.

Definice

Následující definice mají posílit všeobecné chápání základních prvků akreditačního procesu. Měly by být brány jako reference bez nároku na neotřesitelnou správnost. Tyto definice vycházejí ze stávajících regulatorních rámců a standardů, především z příslušných ustanovení obecného nařízení a normy ISO 17065. Pro potřeby těchto vodítek platí následující definice:

„akreditace“ subjektů pro vydávání viz oddíl 3 o výkladu akreditace pro účely článku 43 obecného nařízení;

„dodatečné požadavky“ znamenají požadavky stanovené příslušným dozorovým úřadem a vůči kterým je akreditace prováděna[4];

„certifikace“ znamená posouzení a nestranné potvrzení třetí stranou[5] udávající, že plnění certifikačních kritérií bylo prokázáno;

„subjekt pro vydávání osvědčení“ znamená shodu posuzující[6] orgán[7] používající certifikační mechanismy[8];

„certifikační schéma“ znamená certifikační systém vztahující se ke konkrétním výrobkům, procesům a službám, na které se vztahují stejné konkrétní požadavky, pravidla a postupy;[9]

„kritéria“ nebo certifikační kritéria znamenají kritéria, vůči kterým je certifikace (posuzování shody) prováděna;[10]

„vnitrostátní akreditační orgán“ znamená jediný orgán v členském státě jmenovaný v souladu s Nařízením Evropského parlamentu a Rady (ES) č. 765/2008, který na základě státem delegované pravomoci provádí akreditaci[11].

[4] Článek 43 odst. 1 písm. b), odst. 3, odst. 6.

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

[6] Posudek shody třetí stranou je prováděn organizací nezávislou na osobě nebo organizaci, poskytující předmět a na uživatelském zájmu na tomto předmětu, srov. ISO 17000, 2.4.

[7] Viz ISO 17000, 2.5: „orgán, který vykonává služby v oblasti posuzování shody“; ISO 17011: „orgány vykonávající posuzování shody a mohou být předmětem akreditace“; ISO 17065, 3.12.

[8] Článek 42 odst. 1 a 42 odst. 5 obecného nařízení.

[9] Viz 3.9 v kombinaci s přílohou B normy ISO 17065.

[10] Viz článek 42 odst. 5.

[11] Viz článek 2 odst. 11 nařízení 765/2008/ES.

3 Výklad pojmu „akreditace“ pro potřeby článku 43 obecného nařízení

Obecné nařízení nedefinuje pojem „akreditace“. Článek 2 odst. 10 nařízení (ES) č. 765/2008, který stanovuje obecné požadavky na akreditaci, ji definuje jako:

> *„osvědčování vnitrostátním akreditačním orgánem toho, že subjekt posuzování shody splňuje požadavky pro provádění konkrétních činností posuzování shody, které stanoví harmonizované normy, a pokud je to relevantní, také veškeré další požadavky, včetně těch, které jsou stanoveny v příslušných odvětvových předpisech*“

Podle ISO 17011

> *„se akreditace týká atestace ohledně orgánu pro posuzování shody, která formálně vyjadřuje jeho kompetenci k provádění konkrétních úkonů posuzování shody*“

Článek 43 odst. 1 stanoví:

> *„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 (1), v souladu s normou EN-ISO/IEC 17065/2012 a s dodatečnými požadavky stanovenými dozorovým úřadem, který je příslušný podle článku 55 nebo 56.“*

Při respektování obecného nařízení se budou akreditační požadavky řídit také:

- Normou EN-ISO/IEC 17065/2012 a „dodatečnými požadavky“ stanovenými dozorovým úřadem příslušným podle článku 43 odst. 1 písm. b), je-li akreditace prováděna vnitrostátním akreditačním orgánem;
- Požadavky definovanými dozorovým úřadem, pokud akreditaci sám provádí.

V obou případech musí konsolidované požadavky zahrnovat požadavky zmíněné v článku 43 odst. 2.

WP29 bere na vědomí, že účelem akreditace je poskytnout autoritativní stanovisko k způsobilosti daného orgánu k provádění certifikace (činnosti posuzování shody)[12]. Ve smyslu obecného nařízení je akreditaci třeba chápat jako:

[12] Srov. recitál 15 765/2008/ES.

osvědčování[13] vnitrostátním akreditačním orgánem toho, že subjekt posuzování shody[14] splňuje požadavky pro provádění konkrétních činností posuzování shody podle článků 42 a 43 obecného nařízení s přihlédnutím k normě EN-ISO/IEC 17065/2012 a dodatečným požadavkům stanoveným dozorovým úřadem nebo sborem (EDPB).

4 Akreditace podle článku 43 odst. 1 obecného nařízení

Článek 43 odst. 1 konstatuje, že existuje několik možností, jak akreditovat subjekty pro vydávání osvědčení. Obecné nařízení vyžaduje, aby dozorové úřady a členské státy definovaly proces akreditace subjektů pro vydávání osvědčení. V tomto oddílu jsou vysvětleny způsoby akreditace stanovené článkem 43.

4.1 Role členských států

Článek 43 odst. 1 vyžaduje, aby členské státy *zajistily*, že tyto subjekty pro vydávání osvědčení budou akreditovány, umožňuje však každému členskému státu určit, kdo bude odpovědný za provádění posudku vedoucího k akreditaci. Článek 43 odst. 1 uvádí tři možnosti, jak akreditaci provádět:

(1) Výhradně dozorovým úřadem na podkladě jeho vlastních požadavků;

(2) Výhradně vnitrostátním akreditačním orgánem určeným v souladu s nařízením (ES) 765/2008 a v souladu s normou EN-ISO/IEC 17065/2012 a s dodatečnými požadavky stanovenými příslušným dozorovým úřadem; nebo

(3) Kombinovaně jak dozorovým úřadem, tak vnitrostátním akreditačním orgánem (a v souladu se všemi požadavky vyjmenovanými shora v odstavci 2).

Je na členském státu rozhodnout, zda akreditaci budou provádět jen jedna nebo obě ze jmenovaných institucí, tj. dozorový úřad a vnitrostátní akreditační orgán, v každém případě by však mělo dojít k zajištění odpovídajících zdrojů[15].

4.2 Provázanost s Nařízením (ES) 765/2008

Pracovní skupina poznamenává, že článek 2 odst. 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“.

Článek 2 odst. 11 by mohl být vnímán jako nesourodý s článkem 43 odst. 1 písm. a) a písm. b) obecného nařízení, umožňující akreditaci jiným subjektem než vnitrostátním akreditačním orgánem členského státu. WP29 se domnívá, že záměrem legislativy EU bylo odchýlit se od obecné zásady, že

[13] Srov. článek 2 odst. 10 Nařízení (ES) 765/2008 Evropského parlamentu a Rady ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh.
[14] Srov. s definicí pojmu „akreditace“ v normě ISO 17011.
[15] Viz článek 4 odst. 9 nařízení (EC) 765/2008.

akreditace má být prováděna výlučně vnitrostátním akreditačním orgánem a dát tak v oblasti akreditace subjektů pro vydávání osvědčení stejnou pravomoc. Článek 43 odst. 1 je tedy zvláštním zákonem (lex specialis) vůči článku 2 odst. 11 v nařízení 765/2008.

4.3 Role vnitrostátního akreditačního orgánu

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

WP29 v zájmu vyjasnění dodává, že specifickou zmínkou „podle odst. 1 písm. b)“ článek 43 odst. 3 implikuje, že formulací „tyto požadavky“ se myslí „dodatečné požadavky“ stanovené příslušným dozorovým úřadem podle článku 43 odst. 1 písm. b) a požadavky vyložené v článku 43 odst. 2.

Vnitrostátní akreditační orgány mají při akreditaci uplatňovat dodatečné požadavky, jak je stanoví dozorové úřady.

Subjekt pro vydávání osvědčení se stávající akreditací podle normy ISO 17065 pro certifikační schémata nesouvisející s obecným nařízením, který si přeje rozšířit rozsah své akreditace na certifikaci podle obecného nařízení, bude muset splnit dodatečné požadavky stanovené dozorovým úřadem, pokud je proces akreditace prováděn vnitrostátním akreditačním orgánem. Je-li akreditace nabízena příslušným dozorovým úřadem, pak subjekt pro vydávání osvědčení žádající o akreditaci bude muset splnit požadavky tohoto příslušného dozorového úřadu.

4.4 Role dozorového úřadu

WP29 poznamenává, že článek 57 odst. 1 písm. q) stanoví, že dozorový úřad *provádí* schvalování subjektu pro vydávání osvědčení podle článku 43 jakožto svůj úkol podle článku 57. Článek 58 odst. 3 písm. e) stanoví, že dozorový úřad má povolovací a poradní pravomoc akreditovat subjekty pro vydávání osvědčení podle článku 43. Znění článku 43 odst. 1 dává prostor pro určitou flexibilitu, přičemž akreditační pravomoc dozorového úřadu by měla být chápána jako úkol jen, pokud je to vhodné. Tento bod lze vyjasnit právem členského státu. I tak musí podle článku 43 odst. 2 písm. a) subjekt pro vydávání osvědčení během procesu akreditace vnitrostátním akreditačním orgánem prokázat ke spokojenosti příslušného dozorového úřadu svoji nezávislost a odborné znalosti ohledně předmětu osvědčení.

Stanoví-li členský stát, že subjekty pro vydávání osvědčení musí být akreditovány dozorovým úřadem, pak by dozorový úřad měl stanovit akreditační kritéria, která by měla zahrnovat, avšak ne jenom, požadavky uvedené v článku 43 odst. 2. Ve srovnání s povinnostmi ohledně akreditace subjektů pro vydávání osvědčení vnitrostátními akreditačními orgány, stanoví článek 43 méně pokynů ohledně akreditačních požadavků/kritérií pro případ, kdy akreditaci provádí dozorový úřad sám. V zájmu podpory harmonizovaného přístupu k akreditaci, by se certifikační kritéria používaná dozorovým

úřadem měla řídit normou ISO 17065 a měla by být doplněna o dodatečné požadavky, jež dozorový úřad stanoví podle článku 43 odst. 1 písm. b). Pracovní skupina WP29 upozorňuje, že článek 43 odst. 2 písm. a) – písm. e) zohledňuje a konkretizuje požadavky ISO 17065, jež přispějí ke konzistentnosti.

Stanoví-li členské státy, že subjekty pro vydávání osvědčení budou akreditovány vnitrostátními akreditačními orgány, pak by dozorový úřad měl stanovit dodatečné požadavky doplňující stávající pravidla pro akreditaci obsažená v nařízení (ES) 765/2008 (jehož články 3-14 se týkají organizace a provádění akreditace subjektů posuzování shody) a technická pravidla popisující metody a postupy subjektů pro vydávání osvědčení. V tomto ohledu poskytuje nařízení (ES) 765/2008 další návod: Článek 2 odst. 10 definuje akreditaci a zmiňuje „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 se měly soustředit na usnadnění posuzování, mimo jiné, nezávislosti a úrovně odborné znalosti subjektů pro vydávání osvědčení, například jejich schopnosti hodnotit a certifikovat operace zpracování osobních údajů správci a zpracovateli podle článku 42 odst. 1. To zahrnuje i způsobilost vyžadovanou pro odvětvová schémata a s ohledem na ochranu základních práv a svobod fyzických osob. Příloha těchto vodítek nabízí pomůcku pro informování příslušných dozorových úřadů při stanovování „dodatečných požadavků" v souladu s článkem 43 odst. 1 písm. b) a článkem 43 odst. 3.

Článek 43 odst. 6 stanoví, že „požadavky podle odstavce 3 tohoto článku [.....] zveřejní dozorový úřad ve snadno přístupné formě". Proto, pro zajištění transparentnosti, by veškerá kritéria nebo požadavky schválené dozorovým úřadem měly být zveřejněny. Z hlediska kvality a důvěry v subjekty pro vydávání osvědčení by bylo žádoucí, aby všechny požadavky na akreditaci byly snadno dostupné veřejnosti.

4.5 Dozorový úřad jako subjekt pro vydávání osvědčení

Článek 42 odst. 5 stanoví, že dozorový úřad může vydávat osvědčení, obecné nařízení však nevyžaduje, aby byl akreditován na splnění požadavků podle nařízení (ES) 765/2008. Pracovní skupina WP29 poukazuje na to, že článek 43 odst. 1 písm. a) a zejména článek 58 odst. 2 písm. h) a odst. 3 písm. a), e)-f) zmocňují dozorové úřady k provádění jak akreditace, tak certifikace a současně poskytovat rady a, v příslušných případech, odebírat certifikace nebo nařizovat subjektům pro vydávání osvědčení certifikaci nevydat.

Může dojít k situacím, kdy bude oddělení akreditační a certifikační role a povinnosti vhodné nebo požadované, například, pokud v členském státě jsou vedle dozorového úřadu i další subjekty pro vydávání osvědčení a všichni vydávají certifikace stejného rozsahu. Dozorové úřady by proto měly učinit dostatečná organizační opatření k oddělení úkolů podle obecného nařízení zakotvit a usnadnit certifikační mechanismy a současně přijmout preventivní opatření k vyloučení střetu zájmů, který může z těchto úkolů vyplynout. Navíc by členské státy a dozorové úřady při formulování vnitrostátních zákonů a postupů týkajících se akreditace a vydávání osvědčení (certifikace) podle obecného nařízení měly pamatovat na harmonizovanou evropskou úroveň.

4.6 Akreditační kritéria

Příloha těchto vodítek poskytuje návod, jak určit dodatečná akreditační kritéria. Identifikuje příslušná ustanovení v obecném nařízení a navrhuje požadavky a kritéria, jež by dozorové úřady a vnitrostátní akreditační orgány měly zvážit pro zajištění souladu s obecným nařízením.

Jak je uvedeno výše, pokud jsou subjekty pro vydávání osvědčení akreditovány vnitrostátním akreditačním orgánem, pak norma EN-ISO/IEC 17065/2012 bude příslušným akreditačním standardem doplněným ještě dalšími požadavky stanovenými dozorovým úřadem. Článek 43 odst. 2 zrcadlí obecně použitelná ustanovení normy EN-ISO/IEC 17065/2012 ve světle ochrany základních práv podle obecného nařízení. V dalším textu uvedený rámec používá článek 43 odst. 2 a normu EN-ISO/IEC 17065/2012 jako východisko pro určení požadavků a dalších kritérií pro posuzování odborné znalosti o ochraně dat na straně subjektů pro vydávání osvědčení a jejich schopnosti zohlednit práva a svobody fyzických osob v souvislosti se zpracováním osobních údajů, jak upravuje obecné nařízení. WP29 poznamenává, že se především soustředí na zajištění, aby v souladu s článkem 43 odst. 1 měly subjekty pro vydávání osvědčení náležitou úroveň odborných znalostí v ochraně osobních údajů.

Dodatečné akreditační požadavky a kritéria stanovená dozorovým úřadem budou platné pro všechny subjekty pro vydávání osvědčení požadujících akreditaci. Akreditační orgán vyhodnotí, zda je subjekt pro vydávání osvědčení způsobilý k výkonu certifikační činnosti v souladu s dodatečnými požadavky a předmětem certifikace. V akreditačních kritériích může být zmínka o výchozích certifikačních schématech s ohledem na konkrétní obory nebo oblasti certifikace.

WP29 dále poznamenává, že budou požadovány zvláštní odborné znalosti na poli ochrany dat jako doplněk požadavků ISO, pokud jiné, externí instituce, jako laboratoře nebo auditoři, provádějí části nebo ucelené fáze certifikačních činností jménem akreditovaného subjektu pro vydávání osvědčení. V takových případech není akreditace těchto externích institucí podle samotného obecného nařízení možná. Pro zajištění vhodnosti těchto institucí pro činnost jménem akreditovaného subjektu pro vydávání osvědčení je však nutné zabezpečit, aby stejné znalosti v oblasti ochrany dat, jaké jsou vyžadovány od akreditovaného subjektu, měla a doložila i externí instituce ve vztahu k dané prováděné činnosti.

Rámec pro určení akreditačních kritérií v příloze těchto vodítek nepředstavuje manuál postupu akreditačního procesu vykonávaného vnitrostátním akreditačním orgánem nebo dozorovým úřadem. Poskytuje návod ohledně struktury a metodiky a tím soubor nástrojů pro dozorový úřad pro určování dodatečných požadavků na akreditaci.

[Poznámka vydavatele: PŘÍLOHA k těmto vodítkům bude doplněna později]