Pokyny 1/2018 týkající se vydávání osvědčení a určování kritérií pro vydávání osvědčení podle článků 42 a 43 nařízení 2016/679

Verze 3.0

4. června 2019

Přijato

Historie verzí

Verze 3.0	4. června 2019	Doplnění přílohy 2 (verze 2.0 přílohy 2 přijatá dne 4. června 2019 po veřejné konzultaci)
Verze 2.1	9. dubna 2019	Přijetí opravy pokynů (bod 45)
Verze 2.0	23. ledna 2019	Přijetí pokynů po veřejné konzultaci – k témuž datu byla přijata příloha 2 (verze 1.0) k veřejné konzultaci
Verze 1.0	25. května 2018	Přijetí pokynů pro veřejnou konzultaci

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. e) nařízení Evropského parlamentu a Rady (EU) 2016/679 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 (dále jen „obecné nařízení o ochraně osobních údajů“),

s ohledem na Dohodu o EHP, a zejména na přílohu XI této dohody a protokol 37 k této dohodě, ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018,

s ohledem na článek 12 a článek 22 svého jednacího řádu ze dne 25. května 2018,

po zvážení výsledků veřejné konzultace o pokynech, která proběhla od 30. května 2018 do 12. července 2018, a o příloze 2, která proběhla od 15. února do 29. března 2019, podle čl. 70 odst. 4 obecného nařízení o ochraně osobních údajů,

PŘIJAL TYTO POKYNY:

1 ÚVOD

1. Obecné nařízení o ochraně osobních údajů (dále jen „nařízení 2016/679“, „obecné nařízení o ochraně osobních údajů“ nebo „nařízení“) poskytuje modernizovaný rámec odpovědnosti a dodržování základních práv pro ochranu osobních údajů v Evropě. Pro tento nový rámec má zásadní význam řada opatření, která mají usnadnit dodržování ustanovení obecného nařízení o ochraně osobních údajů. Ta zahrnují povinné požadavky za zvláštních 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. Před přijetím obecného nařízení o ochraně osobních údajů pracovní skupina zřízená podle článku 29 stanovila, že pro rámec odpovědnosti v oblasti ochrany osobních údajů by vydávání osvědčení mohlo hrát důležitou úlohu.[1] Aby vydávání osvědčení poskytovalo spolehlivé důkazy o dodržování ochrany osobních údajů, je zapotřebí zavést jasná pravidla stanovující požadavky na vydávání osvědčení.[2] Právní základ pro vypracování těchto pravidel poskytuje článek 42 obecného nařízení o ochraně osobních údajů.

3. V čl. 42 odst. 1 obecného nařízení o ochraně osobních údajů se stanoví:

   „Členské státy, dozorové úřady, [Evropský] sbor [pro ochranu osobních údajů] a [Evropská] Komise podpoří, zejména na úrovni Unie, zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání

[1] Pracovní skupina zřízená podle článku 29, stanovisko č. 3/2010 k zásadě odpovědnosti, WP173, 13. července 2010, body 69–71.
[2] Stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2010 k zásadě odpovědnosti (WP173), bod 69.

souladu s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli. Zohlední se specifické potřeby mikropodniků a malých a středních podniků.“

4. Mechanismy pro vydávání osvědčení[3] mohou zlepšit transparentnost nejen pro subjekty údajů, ale i ve vztazích mezi podniky, například mezi správci a zpracovateli. Obecné nařízení o ochraně osobních údajů ve 100. bodě odůvodnění 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.[4]

5. Obecné nařízení o ochraně osobních údajů nezavádí pro správce a zpracovatele právo nebo povinnost osvědčení získat; podle čl. 42 odst. 3 je vydání osvědčení dobrovolným postupem, který má napomoci k prokázání souladu s obecným nařízením o ochraně osobních údajů. Členské státy a dozorové úřady se vybízejí, aby podporovaly zavedení mechanismů pro vydávání osvědčení, a určí zapojení zúčastněných stran do procesu a životního cyklu vydávání osvědčení.

6. Kromě toho je dodržování schválených mechanismů pro vydávání osvědčení jedním z faktorů, které dozorové úřady musí považovat za přitěžující nebo polehčující okolnost při rozhodování o uložení správní pokuty a při rozhodování o výši pokuty (čl. 83 odst. 2 písm. j)).[5]

1.1 Oblast působnosti těchto pokynů

7. Tyto pokyny mají omezenou oblast působnosti; nejedná se o návod k vydávání osvědčení podle obecného nařízení o ochraně osobních údajů. Hlavním cílem těchto pokynů je určit zastřešující požadavky a kritéria, jež mohou být relevantní pro všechny druhy mechanismů pro vydávání osvědčení podle článků 42 a 43 obecného nařízení o ochraně osobních údajů. Za tímto účelem pokyny:

    - zkoumají důvody pro vydávání osvědčení jako nástroje odpovědnosti,
    - vysvětlují klíčové pojmy ustanovení o vydávání osvědčení v článcích 42 a 43 a
    - objasňují rozsah toho, co může být předmětem vydání osvědčení podle článků 42 a 43, a účel vydávání osvědčení,
    - napomáhají tomu, aby výsledky vydávání osvědčení byly smysluplné, jednoznačné, co možná nejvíce reprodukovatelné a porovnatelné bez ohledu na subjekt vydávající osvědčení (porovnatelnost).

8. Obecné nařízení o ochraně osobních údajů umožňuje členským státům a dozorovým úřadům provádět články 42 a 43 mnoha způsoby. Pokyny poskytují poradenství ohledně výkladu a provádění ustanovení článků 42 a 43 a mají pomoci členským státům, dozorovým úřadům

[3] Tyto pokyny budou odkazovat na mechanismy pro vydávání osvědčení a na pečeti a známky dokládající ochranu údajů společně jako na „mechanismy pro vydávání osvědčení“, viz oddíl 1.3.2.
[4] Ve 100. bodě odůvodnění se uvádí, že je třeba vybízet k zavedení mechanismů pro vydávání osvědčení s cílem „zvýšit transparentnost a lépe zajistit soulad s nařízením, aby subjekty údajů mohly u příslušných produktů a služeb rychle posoudit úroveň ochrany údajů“.
[5] Viz pracovní skupina zřízená podle článku 29, Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679 (WP 253).

a vnitrostátním akreditačním orgánům zavést jednotnější, harmonizovaný přístup k zavádění mechanismů pro vydávání osvědčení podle obecného nařízení o ochraně osobních údajů.

9. Doporučení obsažená v těchto pokynech budou relevantní pro:

    - příslušné dozorové úřady a Evropský sbor pro ochranu osobních údajů při schvalování kritérií pro vydávání osvědčení podle čl. 42 odst. 5, čl. 58 odst. 3 písm. f) a čl. 70 odst. 1 písm. o),
    - subjekty pro vydávání osvědčení při navrhování a revizi kritérií pro vydávání osvědčení předtím, než budou předložena příslušnému dozorovému úřadu ke schválení podle čl. 42 odst. 5,
    - Evropský sbor pro ochranu osobních údajů při schvalování evropské pečeti ochrany údajů podle čl. 42 odst. 5 a čl. 70 odst. 1 písm. o),
    - dozorové úřady při navrhování svých vlastních kritérií pro vydávání osvědčení,
    - Evropskou Komisi, které je svěřena pravomoc přijímat akty v přenesené pravomoci za účelem upřesnění požadavků, které je třeba zohlednit v souvislosti s mechanismy pro vydávání osvědčení podle čl. 43 odst. 8,
    - Evropský sbor pro ochranu osobních údajů v okamžiku, kdy Evropské Komisi poskytuje stanovisko k požadavkům na vydávání osvědčení podle čl. 70 odst. 1 písm. q) a čl. 43 odst. 8,
    - vnitrostátní akreditační orgány, které budou muset zohledňovat kritéria pro vydávání osvědčení pro účely akreditace subjektů pro vydávání osvědčení v souladu s normou EN-ISO/IEC 17065/2012 a s dodatečnými požadavky podle článku 43, a
    - správce a zpracovatele při vymezování jejich vlastní strategie pro dodržování obecného nařízení o ochraně osobních údajů a při posuzování osvědčení jako prostředku k prokázání souladu.

10. Evropský sbor pro ochranu osobních údajů v souladu s čl. 42 odst. 2 zveřejní samostatné pokyny zaměřené na určování kritérií pro schvalování mechanismů pro vydávání osvědčení jako nástrojů pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím.

1.2 Účel vydávání osvědčení podle obecného nařízení o ochraně osobních údajů

11. V čl. 42 odst. 1 se stanoví, že se zavedou mechanismy pro vydávání osvědčení „pro účely prokázání souladu s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli“.

12. Obecné nařízení o ochraně osobních údajů uvádí příklady situací, v nichž lze schválené mechanismy pro vydávání osvědčení použít jako prvek k prokázání souladu s povinnostmi správců a zpracovatelů, pokud jde o:

    - zavedení a prokázání vhodných technických a organizačních opatření uvedených v čl. 24 odst. 1 a 3, článku 25 a čl. 32 odst. 1 a 3,

- dostatečné záruky podle čl. 28 odst. 5 uvedené v čl. 28 odst. 1 (zpracovatel správci) a v čl. 28 odst. 4 (další zpracovatel zpracovateli).

13. Vzhledem k tomu, že osvědčení samo o sobě neprokazuje soulad, ale spíše představuje prvek, který lze použít k prokázání souladu, mělo by být vydáno transparentním způsobem. Prokázání souladu vyžaduje podpůrnou dokumentaci, zejména písemné zprávy, které nejen opakují, ale také popisují, jak jsou kritéria splněna, a pokud nejsou původně splněna, popisují opravy a nápravná opatření a jejich vhodnost, a tím poskytují důvody pro udělení a zachování osvědčení. To zahrnuje nástin konkrétního rozhodnutí o udělení, obnovení nebo odebrání osvědčení. Měly by být uvedeny důvody, argumenty a důkazy vyplývající z použití kritérií a závěry, úsudky nebo vývody vycházející ze skutečností nebo předpokladů shromážděných během vydávání osvědčení.

1.3 Klíčové pojmy

14. Následující oddíl se zabývá klíčovými pojmy uvedenými v článcích 42 a 43. Tato analýza má napomoci pochopení základních pojmů a rozsahu vydávání osvědčení podle obecného nařízení o ochraně osobních údajů.

1.3.1 Výklad pojmu „osvědčení“

15. Obecné nařízení o ochraně osobních údajů pojem „osvědčení“ nevymezuje. Mezinárodní organizace pro normalizaci (ISO) uvádí univerzální definici certifikace jako „poskytnutí písemného ujištění (certifikátu) nezávislým orgánem o tom, že produkt, služba nebo systém splňuje konkrétní požadavky“. Certifikace je také známa jako „posuzování shody třetí stranou“ a certifikační orgány lze také označovat jako „orgány posuzující shodu“. V normě EN-ISO/IEC 17000:2004 – Posuzování shody – Slovník a základní principy (na kterou odkazuje norma ISO17065) je certifikace definována takto: „potvrzení [...] vydané třetí stranou vztahující se k produktům, procesům nebo službám“.

16. „Potvrzení“ je „vydání výroku, které je založeno na rozhodnutí z přezkoumání, že splnění konkrétních požadavků je prokázáno“ (článek 5.2, ISO 17000:2004).

17. V souvislosti s vydáváním osvědčení podle článků 42 a 43 obecného nařízení o ochraně osobních údajů se vydávání osvědčení vztahuje k potvrzení vydanému třetí stranou vztahujícímu se k operacím zpracování prováděným správci a zpracovateli.

1.3.2 Mechanismy pro vydávání osvědčení, pečetě a známky

18. Obecné nařízení o ochraně osobních údajů nevymezuje „mechanismy pro vydávání osvědčení, pečetě nebo známky“ – a používá tyto pojmy pod společným názvem. Osvědčení je prohlášení o shodě. Pečeť nebo známka mohou být použity k potvrzení úspěšného dokončení postupu vydávání osvědčení. Pečeť nebo známka se obvykle vztahují k logu nebo symbolu, jehož přítomnost (kromě osvědčení) naznačuje, že předmět osvědčení byl nezávisle posouzen

v rámci postupu vydávání osvědčení a splňuje specifikované požadavky stanovené v normativních dokumentech, jako jsou předpisy, normy nebo technické specifikace. Tyto požadavky v souvislosti s vydáváním osvědčení podle obecného nařízení o ochraně osobních údajů jsou stanoveny v dodatečných požadavcích, které doplňují pravidla pro akreditaci subjektů pro vydávání osvědčení v normě EN-ISO/IEC 17065/2012 a kritéria pro vydávání osvědčení schválená dozorovým úřadem nebo sborem. Osvědčení, pečeť nebo známka podle obecného nařízení o ochraně osobních údajů mohou být vydány pouze na základě nezávislého posouzení podkladů akreditovaným subjektem pro vydávání osvědčení nebo příslušným dozorovým úřadem, v němž se uvádí, že kritéria pro vydávání osvědčení jsou splněna.

19. Tabulka uvádí obecný příklad procesu vydávání osvědčení.

Podání žádosti správcem nebo zpracovatelem	**Formální kontrola subjektem pro vydávání osvědčení**	**Posouzení Předběžné hodnocení**	**Posouzení Vyhodnocení cíle hodnocení**	**Posouzení Validace výsledků**	**Informace předávané příslušnému dozorovému úřadu**	**Osvědčení**	**Monitorování**	**Obnovení osvědčení**
Je popis cíle hodnocení jednoznačný a kompletní včetně rozhraní?	Lze popis cíle hodnocení přijmout?	Jaká jsou použitelná kritéria?	Splňuje cíl hodnocení kritéria?	Jsou stanovena všechna relevantní kritéria a zohledňují cíl hodnocení?	Jsou uvedeny důvody pro udělení nebo odebrání osvědčení?	Lze osvědčení udělit?	Splňuje cíl hodnocení i nadále daná kritéria?	Splňuje zpracování i nadále kritéria pro vydávání osvědčení?
Lze udělit přístup k činnostem zpracování cíle hodnocení?	Jsou všechny dokumenty kompletní a aktuální?	Jaké jsou použitelné metody hodnocení?	Je dokumentace cíle hodnocení správná?	Je hodnocení dostatečně doložené?		Jsou připraveny zprávy ke zveřejnění?	Používá se osvědčení/pečeť/značka důvěry správně?	Jsou uspokojivě řešeny oblasti vývoje?
Čl. 42 odst. 6	Čl. 43 odst. 4	Čl. 43 odst. 4	Čl. 42 odst. 5, čl. 43 odst. 4	Čl. 43 odst. 4	Čl. 43 odst. 1, čl. 43 odst. 5	Čl. 43 odst. 1, čl. 42 odst. 7	Čl. 42 odst. 7	Čl. 42 odst. 7

2 ÚLOHA DOZOROVÝCH ÚŘADŮ

20. V čl. 42 odst. 5 se stanoví, že osvědčení vydává akreditovaný subjekt pro vydávání osvědčení nebo příslušný dozorový úřad. Podle obecného nařízení o ochraně osobních údajů není vydávání osvědčení povinným úkolem dozorových úřadů. Obecné nařízení o ochraně osobních údajů namísto toho umožňuje řadu různých modelů. Dozorový úřad se může například rozhodnout pro jednu nebo více z těchto možností:

- vydávat osvědčení sám s ohledem na vlastní systém vydávání osvědčení,

- vydávat osvědčení sám s ohledem na vlastní systém vydávání osvědčení, avšak proces posuzování zcela nebo částečně delegovat na třetí strany,
- vytvořit vlastní systém vydávání osvědčení a postupem vydávání osvědčení pověřit subjekty pro vydávání osvědčení, které budou osvědčení vydávat, a
- podporovat trh v rozvoji mechanismů pro vydávání osvědčení.

21. Dozorový úřad bude muset rovněž zvážit svou úlohu s ohledem na rozhodnutí přijatá na vnitrostátní úrovni týkající se akreditačních mechanismů – zejména pokud je samotný dozorový úřad pověřen akreditací subjektů pro vydávání osvědčení podle čl. 43 odst. 1 obecného nařízení o ochraně osobních údajů. Každý dozorový úřad tedy určí, který přístup bude zvolen s cílem sledovat obecný záměr vydávání osvědčení podle obecného nařízení o ochraně osobních údajů. To bude určeno nejen v souvislosti s úkoly a pravomocemi uvedenými v článcích 57 a 58, ale také s ohledem na osvědčení jako faktor, který je třeba vzít v úvahu při určování správních pokut, a obecně jako prostředek k prokázání souladu.

2.1 Dozorový úřad jako subjekt pro vydávání osvědčení

22. Pokud se některý dozorový úřad rozhodne vydávat osvědčení, bude muset pečlivě posoudit svou úlohu, pokud jde o úkoly, které mu byly svěřeny podle obecného nařízení o ochraně osobních údajů. Jeho úloha by měla být při výkonu jeho funkcí transparentní. Bude muset věnovat zvláštní pozornost oddělení pravomocí týkajících se šetření a vymáhání práva, aby se předešlo případným střetům zájmů.

23. Pokud bude dozorový úřad vystupovat jako subjekt pro vydávání osvědčení, bude muset zajistit řádné vytvoření mechanismu pro vydávání osvědčení a vypracovat svá vlastní kritéria pro vydávání osvědčení nebo taková kritéria přijmout. Kromě toho každý dozorový úřad, který vydává osvědčení, má za úkol tato osvědčení pravidelně přezkoumávat (čl. 57 odst. 1 písm. o)) a má pravomoc osvědčení odebrat, pokud požadavky na osvědčení nejsou nebo přestaly být plněny (čl. 58 odst. 2 písm. h)). Ke splnění těchto požadavků je vhodné stanovit postup vydávání osvědčení a procedurální požadavky, a není-li stanoveno jinak, např. vnitrostátními právními předpisy, zavést právně vynutitelnou dohodu o provádění činností v oblasti vydávání osvědčení s konkrétní žadatelskou organizací. Je zapotřebí zajistit, aby tato dohoda o vydávání osvědčení vyžadovala, aby žadatel splňoval alespoň kritéria pro vydávání osvědčení, včetně opatření nezbytných k provádění hodnocení, monitorování dodržování kritérií a pravidelného přezkumu, což zahrnuje přístup k informacím a/nebo do prostor, dokumentaci a zveřejňování zpráv a výsledků a šetření stížností. Dále se očekává, že dozorový úřad bude kromě požadavků podle čl. 43 odst. 2 dodržovat požadavky pokynů pro akreditaci subjektů pro vydávání osvědčení.

2.2 Další úkoly dozorového úřadu týkající se vydávání osvědčení

24. V členských státech, v nichž subjekty pro vydávání osvědčení začnou vyvíjet činnost, má dozorový úřad bez ohledu na svou vlastní činnost pravomoc a úkol:

- posoudit kritéria systému vydávání osvědčení a předložit návrh rozhodnutí (čl. 42 odst. 5),

- oznámit sboru návrh rozhodnutí, hodlá-li schválit kritéria pro vydávání osvědčení (čl. 64 odst. 1 písm. c), čl. 64 odst. 7), a zvážit stanovisko sboru (čl. 64 odst. 1 písm. c) a čl. 70 odst. 1 písm. t)),
- schválit kritéria pro vydávání osvědčení (čl. 58 odst. 3 písm. f)) předtím, než může být provedena akreditace a vydáno osvědčení (čl. 42 odst. 5 a čl. 43 odst. 2 písm. b)),
- zveřejnit kritéria pro vydávání osvědčení (čl. 43 odst. 6),
- jednat jako příslušný orgán pro systémy vydávání osvědčení v celé EU, což může vést k vydání evropské pečeti ochrany údajů schválené Evropským sborem pro ochranu osobních údajů (čl. 42 odst. 5 a čl. 70 odst. 1 písm. o)), a
- nařídit subjektu pro vydávání osvědčení, aby a) osvědčení nevydal nebo b) osvědčení odebral, pokud požadavky na osvědčení (postupy nebo kritéria pro vydávání osvědčení) plněny nejsou nebo již přestaly být plněny (čl. 58 odst. 2 písm. h)).

25. Obecné nařízení o ochraně osobních údajů ukládá dozorovému úřadu, aby kritéria pro vydávání osvědčení schvaloval, nikoli aby je vytvářel. Za účelem schválení kritérií pro vydávání osvědčení podle čl. 42 odst. 5 by dozorový úřad měl mít jasnou představu o tom, co lze očekávat, zejména pokud jde o rozsah a obsah k prokázání souladu s obecným nařízením o ochraně osobních údajů a s ohledem na jeho úkol monitorovat a vymáhat uplatňování tohoto nařízení. V příloze jsou uvedeny pokyny pro zajištění harmonizovaného přístupu při posuzování kritérií pro účely schválení.

26. Ustanovení čl. 43 odst. 1 vyžaduje, aby subjekty pro vydávání osvědčení před vydáním nebo obnovením osvědčení informovaly svůj dozorový úřad s cílem umožnit mu výkon jeho nápravných pravomocí podle čl. 58 odst. 2 písm. h). Kromě toho čl. 43 odst. 5 také vyžaduje, aby subjekty pro vydávání osvědčení sdělily příslušnému dozorovému úřadu důvody pro vydání nebo odebrání požadovaného osvědčení. Ačkoli obecné nařízení o ochraně osobních údajů umožňuje dozorovým úřadům určit, jak budou tyto informace v praxi získávat, uznávat, přezkoumávat a nakládat s nimi (mohlo by to například zahrnovat technologická řešení umožňující podávání zpráv subjekty pro vydávání osvědčení), lze zavést postup a kritéria pro zpracovávání informací a zpráv poskytnutých ke každému úspěšnému projektu týkajícímu se vydávání osvědčení subjektem pro vydávání osvědčení podle čl. 43 odst. 1. Na základě těchto informací může dozorový úřad vykonávat svou pravomoc nařídit subjektu pro vydávání osvědčení, aby osvědčení odebral nebo je nevydal (čl. 58 odst. 2 písm. h)), a monitorovat a vymáhat uplatňování požadavků a kritérií pro vydávání osvědčení podle obecného nařízení o ochraně osobních údajů (čl. 57 odst. 1 písm. a) a čl. 58 odst. 2 písm. h)). To podpoří harmonizovaný přístup a porovnatelnost při vydávání osvědčení různými subjekty pro vydávání osvědčení a informovanost dozorových úřadů o stavu osvědčení určité organizace.

3 ÚLOHA SUBJEKTU PRO VYDÁVÁNÍ OSVĚDČENÍ

27. Úlohou subjektu pro vydávání osvědčení je vydávat, přezkoumávat, obnovovat a odebírat osvědčení (čl. 42 odst. 5 a 7) na základě mechanismu pro vydávání osvědčení a schválených kritérií (čl. 43 odst. 1). To vyžaduje, aby subjekt pro vydávání osvědčení nebo vlastník systému vydávání osvědčení určil a zavedl kritéria a postupy pro vydávání osvědčení, včetně postupů pro monitorování souladu, přezkum osvědčení, vyřizování stížností a odebírání osvědčení. Kritéria pro vydávání osvědčení se přezkoumávají v rámci akreditačního procesu, který posuzuje pravidla a postupy, na jejichž základě jsou osvědčení, pečetě nebo známky vydávány (čl. 43 odst. 2 písm. c)).

28. Pro získání akreditace podle článku 43 je nutná existence mechanismu pro vydávání osvědčení a kritérií pro vydávání osvědčení. Významný dopad na to, co subjekt pro vydávání osvědčení dělá, vyplývá z rozsahu a typu kritérií pro vydávání osvědčení, které mají dopad na postupy vydávání osvědčení, a naopak. Zvláštní kritéria mohou například vyžadovat zvláštní metody hodnocení, jako jsou kontroly na místě a přezkum kodexu. Tyto postupy jsou pro akreditaci povinné a jsou blíže vysvětleny v pokynech týkajících se akreditace.

29. Subjekt pro vydávání osvědčení je podle obecného nařízení o ochraně osobních údajů povinen poskytovat dozorovým úřadům informace, zejména pokud jde o jednotlivá osvědčení, které jsou nezbytné k monitorování uplatňování mechanismu pro vydávání osvědčení (čl. 42 odst. 7, čl. 43 odst. 5, čl. 58 odst. 2 písm. h)).

4 SCHVALOVÁNÍ KRITÉRIÍ PRO VYDÁVÁNÍ OSVĚDČENÍ

30. Kritéria pro vydávání osvědčení tvoří nedílnou součást jakéhokoli mechanismu pro vydávání osvědčení. Obecné nařízení o ochraně osobních údajů proto vyžaduje, aby kritéria pro vydávání osvědčení v rámci mechanismu pro vydávání osvědčení schválil příslušný dozorový úřad (čl. 42 odst. 5 a čl. 43 odst. 2 písm. b)). V případě evropské pečeti ochrany údajů schvaluje kritéria pro vydávání osvědčení Evropský sbor pro ochranu osobních údajů (čl. 42 odst. 5 a čl. 70 odst. 1 písm. o)). Oba způsoby schvalování kritérií pro vydávání osvědčení jsou vysvětleny níže.

31. Evropský sbor pro ochranu osobních údajů uznává následující účely pro schvalování kritérií pro vydávání osvědčení:

    - náležitě zohledňovat požadavky a zásady týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů stanovené v nařízení (EU) 2016/679 a
    - přispívat k jednotnému uplatňování obecného nařízení o ochraně osobních údajů.

32. Schválení se uděluje na základě toho, že v kritériích pro vydávání osvědčení je plně zohledněn požadavek obecného nařízení o ochraně osobních údajů, aby mechanismus pro vydávání osvědčení umožňoval správcům a zpracovatelům prokázat soulad s obecným nařízením o ochraně osobních údajů.

4.1 Schválení kritérií příslušným dozorovým úřadem

33. Kritéria pro vydávání osvědčení musí být schválena příslušným dozorovým úřadem před procesem akreditace subjektu pro vydávání osvědčení nebo během tohoto procesu. Schválení

se rovněž vyžaduje pro aktualizované nebo dodatečné systémy nebo soubory kritérií podle normy ISO 17065 týmž subjektem pro vydávání osvědčení, a to před použitím pozměněných mechanismů pro vydávání osvědčení (čl. 42 odst. 5 a čl. 43 odst. 2 písm. b)). Dozorové úřady nakládají se všemi žádostmi o schválení kritérií pro vydávání osvědčení spravedlivým a nediskriminačním způsobem, v souladu s veřejně dostupným postupem, v němž jsou uvedeny obecné podmínky, které musí být splněny, a popis procesu schvalování.

34. Subjekt pro vydávání osvědčení může vydávat osvědčení pouze v určitém členském státě v souladu s kritérii schválenými dozorovým úřadem v daném členském státě. Jinými slovy kritéria pro vydávání osvědčení musí být schválena příslušným dozorovým úřadem, pokud má subjekt pro vydávání osvědčení za cíl nabízet vydávání osvědčení a získá akreditaci. Pro celoevropské systémy vydávání osvědčení viz níže uvedený oddíl.

4.2 Schválení kritérií Evropským sborem pro ochranu osobních údajů v souvislosti s evropskou pečetí ochrany údajů

35. Subjekt pro vydávání osvědčení může rovněž vydávat osvědčení v souladu s kritérii schválenými Evropským sborem pro ochranu osobních údajů pro evropskou pečeť ochrany údajů. Kritéria pro vydávání osvědčení schválená Evropským sborem pro ochranu osobních údajů podle článku 63 mohou vést k evropské pečeti ochrany údajů (čl. 42 odst. 5). S ohledem na stávající úmluvy týkající se vydávání osvědčení a akreditace Evropský sbor pro ochranu osobních údajů uznává, že je žádoucí vyhnout se roztříštění trhu v oblasti vydávání osvědčení o ochraně osobních údajů. Konstatuje, že čl. 42 odst. 1 stanoví, že členské státy, dozorové úřady, sbor a Komise podpoří zavedení mechanismů pro vydávání osvědčení, zejména na úrovni Unie.

4.2.1 Žádost o schválení

36. Žádost o schválení kritérií podle čl. 42 odst. 5 a čl. 70 odst. 1 písm. o) Evropským sborem pro ochranu osobních údajů musí být předložena prostřednictvím příslušného dozorového úřadu a měla by uvádět záměr vlastníka systému, uchazeče nebo akreditovaného subjektu pro vydávání osvědčení nabízet kritéria v rámci mechanismu pro vydávání osvědčení správcům a zpracovatelům ve všech členských státech. Příslušný dozorový úřad předloží návrh Evropskému sboru pro ochranu osobních údajů, pokud má za to, že Evropský sbor pro ochranu osobních údajů by mohl kritéria schválit.

37. Výběr místa pro podání žádosti o schválení kritérií bude záležet na vlastnících systému vydávání osvědčení nebo na sídle subjektů pro vydávání osvědčení.

38. Pokud subjekt pro vydávání osvědčení podá žádost, obvykle má již podanou žádost o akreditaci nebo je již akreditován buď příslušným dozorovým úřadem, nebo vnitrostátním akreditačním orgánem svého členského státu. V případě, že subjekt pro vydávání osvědčení je již akreditován, pokud jde o mechanismus pro vydávání osvědčení podle obecného nařízení o ochraně osobních údajů, může to pomoci proces schvalování zjednodušit.

4.2.2 Kritéria pro evropskou pečeť ochrany údajů

39. Evropský sbor pro ochranu osobních údajů bude koordinovat proces posuzování žádostí a podle potřeby schválí kritéria pro evropskou pečeť ochrany údajů. Posouzení se zaměří na tyto oblasti: rozsah kritérií a schopnost sloužit jako společné osvědčení. Pokud Evropský sbor pro ochranu osobních údajů kritéria schválí, očekává se, že příslušný dozorový úřad podle sídla subjektu pro vydávání osvědčení v EU bude vyřizovat stížnosti týkající se samotného mechanismu a informovat ostatní dozorové úřady. Tento dozorový úřad má rovněž pravomoc přijímat opatření proti subjektu pro vydávání osvědčení. Příslušný dozorový úřad případně informuje ostatní dozorové úřady a Evropský sbor pro ochranu osobních údajů.

40. Kritéria pro vydávání osvědčení týkající se společného osvědčení podléhají požadavkům v rámci celé EU a pro zvládnutí těchto požadavků by měla poskytovat specifický mechanismus. Evropské mechanismy pro vydávání osvědčení musí být určeny k použití ve všech členských státech. Na základě čl. 42 odst. 5 je zapotřebí, aby mechanismus pro evropskou pečeť ochrany údajů, jakož i jeho kritéria byly přizpůsobitelné tak, aby bylo možné případně zohlednit vnitrostátní odvětvové předpisy, např. v případě zpracování údajů ve školách, a aby počítaly s celoevropským uplatněním.

41. Například: Mezinárodní škola nabízející školní vzdělávání subjektům údajů v Unii má sídlo v členském státě „A“. Škola chce získat osvědčení pro svůj proces podávání přihlášek on-line prostřednictvím celounijního systému vydávání osvědčení k dosažení evropské pečeti ochrany údajů. Na základě této evropské pečeti hodlá škola požádat o vydání osvědčení pro operace zpracování nabízeného subjektem pro vydávání osvědčení usazeným v členském státě „B“. Kritéria pro pečeti navržená a zdokumentovaná v příslušném mechanismu musí být schopna zohlednit předpisy pro školy použitelné v členském státě „A“. Kritéria by rovněž měla vyžadovat, aby proces podávání přihlášek on-line dané školy poskytoval informace a zohledňoval příslušné požadavky členského státu na ochranu údajů, které se mohou v jiných členských státech lišit. Příkladem jsou soubory osobních údajů, které mají být předloženy pro účely přihlášky, např. hodnocení z mateřské školy nebo výsledky zkoušek, různá doba uchovávání, sběr nebo zpracování finančních nebo biometrických údajů, další omezení zpracování.

    - Mezi kritéria na vysoké úrovni pro schválení mechanismu pro evropskou pečeť ochrany údajů patří:
        - kritéria schválená sborem,
        - uplatnění napříč jurisdikcemi, při zohlednění případných vnitrostátních právních požadavků a odvětvových předpisů,
        -
    - harmonizovaná kritéria, která jsou přizpůsobitelná tak, aby odrážela vnitrostátní požadavky,
        - popis mechanismu pro vydávání osvědčení,
        - dohody o vydávání osvědčení respektující celoevropské požadavky,

- postupy k zajištění a poskytnutí řešení pro vnitrostátní odchylky a zajištění toho, aby pečeť pomohla prokázat soulad s obecným nařízením o ochraně osobních údajů, a
- jazyk zpráv určených všem dotčeným dozorovým úřadům.

42. Příloha rovněž obsahuje doporučení ohledně kritérií pro evropskou pečeť ochrany údajů.

4.2.3 Úloha akreditace

43. Jak je uvedeno v bodě 4.2.1, pokud jsou kritéria určena jako vhodná pro vydání společného osvědčení a byla jako taková schválena sborem podle čl. 42 odst. 5, mohou být subjekty pro vydávání osvědčení akreditovány k vydávání osvědčení na základě těchto kritérií na úrovni Unie.

44. Systémy, které mají být nabízeny pouze v určitých členských státech, se nebudou ucházet o pečeti na úrovni EU. Akreditace v rozsahu evropské pečeti ochrany údajů bude vyžadovat akreditaci v členském státě sídla subjektu pro vydávání osvědčení, který hodlá daný systém provozovat, tj. odpovědného za vydávání osvědčení a řízení činností vydávání osvědčení svých subjektů a dceřiných společností v jiných členských státech. Pokud některé provozovny nebo kanceláře řídí a vydávají osvědčení nezávisle, každá z těchto provozoven nebo kanceláří bude muset mít samostatnou akreditaci v členském státě, v němž sídlí. Jinými slovy akreditace je nezbytná pouze v členském státě sídla subjektu pro vydávání osvědčení v případě, že osvědčení vydává pouze ústředí. Naopak, pokud osvědčení vydávají i jiné provozovny subjektu pro vydávání osvědčení, musí být tyto provozovny rovněž akreditovány.

45. Pokud tedy subjekt pro vydávání osvědčení není akreditován pro vydávání osvědčení v rámci evropské pečeti ochrany údajů, pak nelze kritéria schválená Evropským sborem pro ochranu osobních údajů použít a pečeť nemůže být nabízena.

5 VYPRACOVÁNÍ KRITÉRIÍ PRO VYDÁVÁNÍ OSVĚDČENÍ

46. Obecné nařízení o ochraně osobních údajů stanovilo rámec pro vypracování kritérií pro vydávání osvědčení. Vzhledem k tomu, že základní požadavky týkající se postupu vydávání osvědčení řeší články 42 a 43, které zároveň stanoví základní kritéria pro postupy vydávání osvědčení, základ kritérií pro vydávání osvědčení musí vycházet ze zásad a pravidel obecného nařízení o ochraně osobních údajů a musí pomoci poskytnout ujištění o naplnění těchto zásad a pravidel.

47. Vypracování kritérií pro vydávání osvědčení by se mělo zaměřit na ověřitelnost, významnost a vhodnost kritérií pro vydávání osvědčení k prokázání souladu s nařízením. Kritéria pro vydávání osvědčení by měla být formulována tak, aby byla jasná a srozumitelná a umožnila uplatňování v praxi.

48. Při navrhování kritérií pro vydávání osvědčení se případně přihlédne mimo jiné k níže uvedeným aspektům souladu na podporu posouzení operace zpracování:

    - zákonnost zpracovávání podle článku 6,
    - zásady zpracování údajů podle článku 5,
    - práva subjektů údajů podle článků 12–23,
    - povinnost ohlašovat případy porušení zabezpečení údajů podle článku 33,
    - povinnost záměrné a standardní ochrany údajů podle článku 25,
    - zda bylo případně provedeno posouzení vlivu na ochranu osobních údajů podle čl. 35 odst. 7 písm. d) a
    - technická a organizační opatření zavedená podle článku 32.

49. Rozsah, v jakém se tyto úvahy odrážejí v kritériích, se může lišit v závislosti na rozsahu osvědčení, který může zahrnovat typ operace (operací) zpracování a oblast (např. zdravotnictví), které se osvědčení týká.

5.1 Na co lze vydat osvědčení podle obecného nařízení o ochraně osobních údajů?

50. Evropský sbor pro ochranu osobních údajů má za to, že obecné nařízení o ochraně osobních údajů nabízí široký rozsah toho, co může být předmětem vydání osvědčení podle obecného nařízení o ochraně osobních údajů, pokud je smyslem pomoci prokázat soulad s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli (čl. 42 odst. 1).

51. Při posuzování operace zpracování musí být případně zváženy tyto tři základní složky:

    1. osobní údaje (věcná působnost obecného nařízení o ochraně osobních údajů);
    2. technické systémy – infrastruktura, např. hardware a software, používané ke zpracování osobních údajů a
    3. procesy a postupy související s operací (operacemi) zpracování.

52. Každá složka použitá při operacích zpracování musí být posouzena na základě stanovených kritérií. Vliv mohou mít přinejmenším čtyři různé významné faktory: 1) organizační a právní struktura správce nebo zpracovatele; 2) oddělení, prostředí a osoby zapojené do operace (operací) zpracování; 3) technický popis prvků, které mají být posouzeny, a v neposlední řadě 4) infrastruktura IT na podporu operace zpracování včetně provozních systémů, virtuálních systémů, databází, systémů ověřování a schvalování, routerů a firewallů, systémů ukládání, komunikační infrastruktury nebo přístupu k internetu a souvisejících technických opatření.

53. Všechny tři hlavní složky jsou důležité pro návrh postupů vydávání osvědčení a kritérií pro vydávání osvědčení. V závislosti na předmětu osvědčení se může lišit rozsah, v jakém budou zohledněny. V některých případech například nemusí být určité složky vzaty v úvahu, pokud jsou z hlediska předmětu osvědčení považovány za nevýznamné.

54. Pro další zpřesnění toho, co může podle obecného nařízení o ochraně osobních údajů získat osvědčení, obsahuje uvedené nařízení další pokyny. Z čl. 42 odst. 7 vyplývá, že osvědčení podle obecného nařízení o ochraně osobních údajů se vydávají pouze správcům údajů a zpracovatelům údajů, což například vylučuje vydávání osvědčení pověřencům pro ochranu osobních údajů. V čl. 43 odst. 1 písm. b) se odkazuje na normu ISO 17065, která stanoví akreditaci certifikačních orgánů posuzujících soulad produktů, služeb a procesů. Operace nebo soubor operací zpracování se podle terminologie normy ISO 17065 mohou stát produktem nebo službou a jako takové mohou být předmětem certifikace. Například zpracování údajů o zaměstnancích za účelem výplaty mezd nebo řízení pracovního volna je ve smyslu obecného nařízení o ochraně osobních údajů souborem operací a v terminologii ISO může být produktem, procesem nebo službou.

55. Na základě těchto úvah má Evropský sbor pro ochranu osobních údajů za to, že z hlediska rozsahu je vydávání osvědčení podle obecného nařízení o ochraně osobních údajů zaměřeno na operace nebo soubory operací zpracování. Ty mohou zahrnovat procesy správy ve smyslu organizačních opatření, a tudíž jako nedílné součásti operace zpracování (např. proces správy zřízený pro vyřizování stížností v rámci zpracování údajů o zaměstnancích za účelem výplaty mezd).

56. Aby bylo možné posoudit soulad operace zpracování s kritérii pro vydávání osvědčení, musí být uvedena konkrétní situace. Například soulad použití technické infrastruktury nasazené při operaci zpracování závisí na kategoriích údajů, které jsou určeny ke zpracování. Organizační opatření závisí na kategoriích a množství údajů a na technické infrastruktuře využívané ke zpracování, s přihlédnutím k povaze, rozsahu, obsahu a účelům zpracování, jakož i k rizikům pro práva a svobody subjektů údajů.

57. Kromě toho je třeba mít na paměti, že aplikace IT se mohou značně lišit, i když slouží stejným účelům zpracování. Proto je třeba k této skutečnosti přihlédnout při vymezování rozsahu mechanismů pro vydávání osvědčení a při navrhování kritérií pro vydávání osvědčení, tj. rozsah vydávání osvědčení a kritérií by neměl být tak úzký, aby vyloučil aplikace IT, které jsou pojaty odlišně.

5.2 Stanovení předmětu osvědčení

58. Rozsah mechanismu pro vydávání osvědčení je třeba odlišovat od předmětu – nazývaného také cíl hodnocení – v jednotlivých projektech vydávání osvědčení v rámci mechanismu pro vydávání osvědčení. Mechanismus pro vydávání osvědčení může vymezit svůj rozsah buď obecně, nebo ve vztahu ke konkrétnímu typu nebo oblasti operací zpracování, a může již tedy určit předměty osvědčení, které spadají do rozsahu mechanismu pro vydávání osvědčení (např. bezpečné uchovávání a ochrana osobních údajů uložených v digitálním trezoru). Spolehlivé a smysluplné posouzení souladu může být provedeno pouze v případě, že je konkrétní předmět projektu osvědčení přesně popsán. Musí být jasně popsáno, které operace zpracování jsou zahrnuty do předmětu osvědčení a poté hlavní složky, tj. které údaje, procesy a technická infrastruktura budou posouzeny a které posouzeny nebudou. Přitom musí být vždy zohledněna a popsána rozhraní pro jiné procesy. Samozřejmě, co není známo, nemůže být součástí posouzení, a nemůže tedy získat osvědčení. Konkrétní předmět osvědčení musí být

v každém případě smysluplný, pokud jde o sdělení nebo prohlášení poskytovaná ohledně osvědčení nebo v osvědčení, a neměl by uživatele, zákazníka ani spotřebitele uvádět v omyl.

59. [Příklad 1]

Banka nabízí svým zákazníkům internetové stránky pro účely internetového bankovnictví. V rámci této služby existuje možnost provádět převody, nakupovat akcie, vytvářet trvalé příkazy a spravovat účet. Banka chce získat osvědčení v rámci mechanismu pro vydávání osvědčení o ochraně údajů s obecným rozsahem na základě obecných kritérií pro tyto oblasti:

a) Zabezpečené přihlašování

Zabezpečené přihlašování je operace zpracování, která je pro koncového uživatele srozumitelná a která je relevantní z hlediska ochrany údajů, neboť hraje důležitou úlohu při zajišťování zabezpečení dotčených osobních údajů. Proto je tato operace zpracování nezbytná pro zabezpečené přihlašování, a může tedy představovat smysluplný cíl hodnocení, pokud osvědčení jasně uvádí, že osvědčení se vztahuje pouze na operaci zpracování při přihlašování.

b) Webový front-end

I když může být webový front-end z hlediska ochrany údajů relevantní, není pro koncového uživatele srozumitelný, a proto nemůže být smysluplným cílem hodnocení. Kromě toho není uživateli jasné, které služby na webových stránkách, a tedy které operace zpracování, jsou do osvědčení zahrnuty.

c) Internetové bankovnictví

Webový front-end spolu s back-endem jsou operace zpracování prováděné v rámci služby internetového bankovnictví, které mohou být pro uživatele smysluplné. V této souvislosti musí být obě zahrnuty do cíle hodnocení. Zatímco operace zpracování, které nejsou přímo spojeny s poskytováním služby internetového bankovnictví, jako jsou operace zpracování pro účely předcházení praní peněz, mohou být z cíle hodnocení vyloučeny.

Služby internetového bankovnictví, které banka nabízí prostřednictvím svých internetových stránek, však mohou zahrnovat i jiné služby, které zase vyžadují vlastní operace zpracování. V této souvislosti mohou ostatní služby zahrnovat například nabízení pojistného produktu. Vzhledem k tomu, že tato doplňková služba není přímo spojena s účelem poskytování služeb internetového bankovnictví, může být z cíle hodnocení vyloučena. Pokud je tato doplňková služba (pojištění) vyloučena z cíle hodnocení, jsou rozhraní pro tuto službu integrovanou na internetových stránkách součástí cíle hodnocení, a musí být proto popsána, aby bylo možné mezi těmito službami jasně rozlišovat. Tento popis je nezbytný pro určení a vyhodnocení možných toků údajů mezi těmito dvěma službami.

60. [Příklad 2]

Banka svým zákazníkům nabízí službu, která jim umožňuje sloučit informace týkající se různých účtů a platebních karet od několika bank (agregace účtů). Banka si přeje získat pro tuto službu osvědčení podle obecného nařízení o ochraně osobních údajů. Příslušný dozorový úřad schválil

zvláštní soubor kritérií pro vydávání osvědčení, která se zaměřují na tento druh činnosti. Rozsah mechanismu pro vydávání osvědčení se týká pouze těchto aspektů souladu:

- ověření totožnosti uživatele a
- přijatelné způsoby, jak získat údaje, které je třeba agregovat, z jiných bank/služeb.

Vzhledem k tomu, že rozsah tohoto mechanismu pro vydávání osvědčení sám vymezuje cíl hodnocení, nelze v rámci navrhovaného rozsahu smysluplně zúžit cíl hodnocení a vydat osvědčení pouze pro konkrétní prvky nebo jednu činnost zpracování. V tomto scénáři musí cíl hodnocení odpovídat konkrétnímu rozsahu.

5.3 Metody hodnocení a metodika posuzování

61. Posouzení shody s cílem prokázat soulad operací zpracování vyžaduje určení a stanovení metod hodnocení a metodiky posuzování. Je důležité, zda jsou informace pro posouzení shromažďovány pouze z dokumentace (což by nebylo samo o sobě dostatečné), nebo zda se informace aktivně shromažďují na místě a prostřednictvím přímého nebo nepřímého přístupu. Způsob, jakým jsou informace shromažďovány, má dopad na význam osvědčení, a proto by měl být definován a popsán.

    Postupy pro vydávání a pravidelný přezkum osvědčení by měly zahrnovat specifikace pro určení vhodné úrovně hodnocení (hloubky a detailnosti) s cílem splnit kritéria pro vydávání osvědčení a měly by zahrnovat tyto položky:

    - poskytnutí informací o použitých metodách posuzování a zjištěních shromážděných např. při auditech na místě nebo v dokumentaci, a jejich specifikaci,
    - poskytnutí metod hodnocení se zaměřením na operace zpracování (údaje, systémy, procesy) a účel zpracování,
    - určení kategorií údajů, potřeb ochrany a zda jsou zahrnuti zpracovatelé nebo třetí strany,
    - určení úlohy a existence mechanismu kontroly přístupu vymezeného v souvislosti s úlohami a povinnostmi.

62. Hloubka hodnocení má dopad na význam a hodnotu osvědčení. Omezením hloubky hodnocení z praktických důvodů nebo za účelem snížení nákladů se sníží jeho význam. Rozhodnutí o detailnosti hodnocení může na druhou stranu překročit finanční možnosti žadatele a často i způsobilost hodnotitelů a auditorů. Pro účely prokázání souladu nemusí být vždy zásadní dosáhnout vysoce podrobné analýzy použitých IT systémů, aby zůstala smysluplná.

5.4 Dokumentace posouzení

63. Dokumentace týkající se vydávání osvědčení by měla být podrobná a komplexní. Nedostatek dokumentace znamená nemožnost řádného posouzení. Základní funkcí dokumentace týkající se vydávání osvědčení je zajištění transparentnosti procesu hodnocení v rámci mechanismu pro vydávání osvědčení. Dokumentace přináší odpovědi na otázky týkající se požadavků stanovených zákonem. Mechanismy pro vydávání osvědčení by měly stanovit

standardizovanou metodiku dokumentace. Poté bude možné porovnat dokumentaci týkající se vydávání osvědčení se skutečným stavem na místě a s kritérii pro vydávání osvědčení.

64. Komplexní dokumentace toho, co je předmětem osvědčení, a použitá metodika slouží transparentnosti. Podle čl. 43 odst. 2 písm. c) by měly mechanismy pro vydávání osvědčení stanovit postupy, které umožní přezkum osvědčení. Aby mohl dozorový úřad posoudit, zda a do jaké míry může být osvědčení uznáno v rámci formálního šetření, může být podrobná dokumentace tím nejvhodnějším způsobem komunikace. Dokumentace vypracovaná během hodnocení by se proto měla zaměřit na tři hlavní aspekty:

    - soulad a soudržnost použitých metod hodnocení,
    - metody hodnocení zaměřené na prokázání souladu předmětu osvědčení s kritérii pro vydávání osvědčení, a tedy s nařízením, a
    - zda byly výsledky hodnocení schváleny nezávislým a nestranným subjektem pro vydávání osvědčení.

5.5 Dokumentace výsledků

65. Ve 100. bodě odůvodnění jsou uvedeny informace o tom, jaké cíle se zavedením vydávání osvědčení sledují.

„S cílem zvýšit transparentnost a lépe zajistit soulad s tímto nařízením je třeba vybízet k zavedení mechanismů pro vydávání osvědčení, jakož i pečetí a známek dokládajících ochranu údajů, aby subjekty údajů mohly u příslušných produktů a služeb rychle posoudit úroveň ochrany údajů.“

66. Pro zvýšení transparentnosti hraje doložení výsledků a jejich sdělování důležitou roli. Subjekty pro vydávání osvědčení, které používají mechanismy pro vydávání osvědčení, pečetě nebo známky zaměřené na subjekty údajů (v jejich postavení spotřebitelů nebo zákazníků), by měly poskytovat snadno dostupné, srozumitelné a smysluplné informace o operaci (operacích) zpracování, které získaly osvědčení. Tyto veřejné informace by měly obsahovat alespoň

    - popis cíle hodnocení,
    - odkaz na schválená kritéria použitá na konkrétní cíl hodnocení,
    - metodiku pro hodnocení kritérií (hodnocení na místě, dokumentace atd.) a
    - dobu platnosti osvědčení a
    - možnost porovnatelnosti výsledků dozorovými úřady a veřejností.

6 POKYNY PRO VYMEZENÍ KRITÉRIÍ PRO VYDÁVÁNÍ OSVĚDČENÍ

67. Kritéria pro vydávání osvědčení jsou nedílnou součástí mechanismu pro vydávání osvědčení. Postup vydávání osvědčení zahrnuje požadavky na to, jakým způsobem, kým a v jakém rozsahu, a na podrobnost posouzení, které se provádí v jednotlivých projektech vydávání osvědčení týkajících se konkrétního předmětu nebo cíle hodnocení. Kritéria pro vydávání osvědčení stanoví jmenovité požadavky, na jejichž základě se samotná operace zpracování vymezená v rámci cíle hodnocení posuzuje. Tyto pokyny pro vymezení kritérií pro vydávání osvědčení poskytují obecné rady, které usnadní posuzování kritérií pro vydávání osvědčení pro účely schválení.

    - Při schvalování nebo vymezování kritérií pro vydávání osvědčení je třeba přihlédnout k níže uvedeným obecným úvahám. Kritéria pro vydávání osvědčení by měla:
    - být jednotná a ověřitelná,
    - být přezkoumatelná s cílem usnadnit hodnocení operací zpracování podle obecného nařízení o ochraně osobních údajů, zejména stanovením cílů a prováděcích pokynů k dosažení těchto cílů,
    - být relevantní s ohledem na cílové skupiny, např. vztahy mezi podniky (B2B) a mezi podniky a zákazníky (B2C),
    - zohledňovat jiné normy (jako jsou normy ISO, vnitrostátní normy) a v případě potřeby s nimi být interoperabilní a
    - být flexibilní a odstupňovatelná pro uplatnění na různé typy a velikosti organizací včetně mikropodniků a malých a středních podniků v souladu s čl. 42 odst. 1 a přístupem založeným na posouzení rizik podle 77. bodu odůvodnění.

68. Malá místní společnost, jako je maloobchodník, bude obvykle provádět méně složité operace zpracování než velký nadnárodní prodejce. I když jsou požadavky na zákonnost operací zpracování stejné, je nutné vzít v úvahu rozsah zpracování údajů a jeho složitost; z toho vyplývá, že je třeba, aby byly mechanismy pro vydávání osvědčení a jejich kritéria přizpůsobitelné v závislosti na konkrétní činnosti zpracování.

6.1 Stávající normy

69. Subjekty pro vydávání osvědčení budou muset vzít v úvahu, jak konkrétní kritéria zohledňují stávající příslušné nástroje, jako například kodexy chování, technické normy nebo vnitrostátní regulační a právní iniciativy. V ideálním případě budou kritéria interoperabilní se stávajícími normami, které mohou správci či zpracovateli pomoci při plnění jejich povinností podle obecného nařízení o ochraně osobních údajů. Avšak zatímco odvětvové normy se často zaměřují na ochranu a zabezpečení organizace proti hrozbám, obecné nařízení o ochraně osobních údajů je zaměřeno na ochranu základních práv fyzických osob. Tato rozdílná perspektiva musí být zohledněna při koncipování kritérií nebo schvalování kritérií či mechanismů pro vydávání osvědčení založených na odvětvových normách.

6.2 Vymezení kritérií

70. Kritéria pro vydávání osvědčení musí odpovídat prohlášení o osvědčení (sdělení nebo prohlášení) mechanismu pro vydávání osvědčení nebo systému vydávání osvědčení a odpovídat očekáváním, která vyvolává. Již samotný název mechanismu pro vydávání osvědčení může určit rozsah použití a bude mít dopad na určení kritérií.

71. [Příklad 3]

    Rozsah mechanismu nazvaného „HealthPrivacyMark“ by měl být omezen na odvětví zdravotnictví. Název pečeti vyvolává očekávání, že byly přezkoumány požadavky na ochranu údajů v souvislosti se zdravotními údaji. Kritéria tohoto mechanismu proto musí být vhodná pro posouzení požadavků na ochranu údajů v tomto odvětví.

72. [Příklad 4]

    Mechanismus, který se týká vydávání osvědčení pro operace zpracování, jež zahrnují systémy správy při zpracování údajů, by měl určit kritéria, která umožní uznávání a posuzování postupů správy a podpůrných technických a organizačních opatření.

73. [Příklad 5]

    Kritéria pro mechanismus, který se týká cloud computingu, musí zohledňovat zvláštní technické požadavky nezbytné pro využívání cloudových služeb. Pokud jsou například použity servery mimo EU, musí kritéria zohledňovat podmínky stanovené v kapitole V obecného nařízení o ochraně osobních údajů, pokud jde o předávání údajů do třetích zemí.

74. Kritéria koncipovaná tak, aby vyhovovala různým cílům hodnocení v různých odvětvích a /nebo členských státech by měla: umožňovat použití různých scénářů; umožňovat určení vhodných opatření, která budou vyhovovat malým, středním nebo velkým operacím zpracování a zohledňovat rizika různé pravděpodobnosti a závažnosti pro práva a svobody fyzických osob v souladu s obecným nařízením o ochraně osobních údajů. V důsledku toho musí postupy vydávání osvědčení (např. pro metodu a hloubku dokumentování, testování nebo hodnocení), které tato kritéria doplňují, odpovídat uvedeným potřebám a umožňovat a mít zavedená pravidla, například pro uplatňování příslušných kritérií v jednotlivých projektech vydávání osvědčení. Kritéria musí usnadnit posouzení toho, zda byly poskytnuty dostatečné záruky pro provedení vhodných technických a organizačních opatření.

6.3 Doba platnosti kritérií pro vydávání osvědčení

75. Ačkoli kritéria pro vydávání osvědčení musí být v průběhu času spolehlivá, neměla by být neměnná. Měla by být předmětem revize například v těchto situacích:

    - mění se právní rámec,
    - pojmy a ustanovení jsou vykládány v rozsudcích Evropského soudního dvora nebo
    - nastal vývoj v nejnovějších technických poznatcích.

předsedkyně

(Andrea Jelinek)

Přijato

PŘÍLOHA 1: ÚKOLY A PRAVOMOCI DOZOROVÝCH ÚŘADŮ V SOUVISLOSTI S VYDÁVÁNÍM OSVĚDČENÍ V SOULADU S OBECNÝM NAŘÍZENÍM O OCHRANĚ OSOBNÍCH ÚDAJŮ

	Ustanovení	Požadavky
Úkoly	Čl. 43 odst. 6	Vyžaduje, aby dozorový úřad zveřejnil kritéria uvedená v čl. 42 odst. 5 ve snadno přístupné formě a předal je sboru.
	Čl. 57 odst. 1 písm. n)	Vyžaduje, aby dozorový úřad schválil kritéria pro vydávání osvědčení podle čl. 42 odst. 5.
	Čl. 57 odst. 1 písm. o)	Stanoví, že v případě potřeby (tj. pokud vydá osvědčení) provádí pravidelný přezkum osvědčení vydaného v souladu s čl. 42 odst. 7.
	Čl. 64 odst. 1 písm. c)	Vyžaduje, aby dozorový úřad oznámil sboru návrh rozhodnutí, pokud má za cíl schválit kritéria pro vydávání osvědčení uvedená v čl. 42 odst. 5.
Pravomoci	Čl. 58 odst. 1 písm. c)	Stanoví, že dozorový úřad má pravomoc provádět přezkumy osvědčení v souladu s čl. 42 odst. 7.
	Čl. 58 odst. 2 písm. h)	Stanoví, že dozorový úřad má pravomoc odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení nebo osvědčení nevydal.
	Čl. 58 odst. 3 písm. e)	Stanoví, že dozorový úřad má pravomoc akreditovat subjekty pro vydávání osvědčení.
	Čl. 58 odst. 3 písm. f)	Stanoví, že dozorový úřad má pravomoc vydávat osvědčení a schvalovat kritéria pro vydávání osvědčení.

PŘÍLOHA 2

1 ÚVOD

Příloha 2 stanoví pokyny pro přezkum a posuzování kritérií pro vydávání osvědčení podle čl. 42 odst. 5. Určuje témata, která dozorový úřad pro ochranu údajů a Evropský sbor pro ochranu osobních údajů posoudí a použijí pro účely schvalování kritérií pro vydávání osvědčení v rámci mechanismu pro vydávání osvědčení. Dané otázky by měli zohlednit subjekty pro vydávání osvědčení a vlastníci systémů, jež chtějí vypracovat a předložit kritéria ke schválení. Seznam není vyčerpávající, ale obsahuje minimální množinu témat, jež mají být zohledněna. Ne všechny otázky budou použitelné; měly by však být zohledněny při navrhování kritérií a může být nutné odůvodnění s cílem vysvětlit, proč se kritéria na určité aspekty nevztahují. Některé otázky se opakují, neboť se týkají různých úhlů pohledu. Tyto pokyny by měly být zohledněny v souladu s právními požadavky stanovenými obecným nařízením o ochraně osobních údajů, a případně vnitrostátními právními předpisy.

2 ROZSAH MECHANISMU PRO VYDÁVÁNÍ OSVĚDČENÍ A CÍL HODNOCENÍ

a. Je rozsah mechanismu pro vydávání osvědčení (pro který mají být kritéria ochrany osobních údajů použita) jasně popsán?

b. Je rozsah mechanismu pro vydávání osvědčení smysluplný pro příslušnou cílovou skupinu a není zavádějící?

- *Příklad: Pečeť důvěryhodné společnosti (Trusted Company Seal) naznačuje, že činnosti zpracování celé společnosti byly podrobeny auditu, ačkoli předmětem osvědčení jsou ve skutečnosti pouze určené operace zpracování, např. on-line platební proces. Rozsah je tedy zavádějící.*

c. Odráží rozsah mechanismu pro vydávání osvědčení všechny příslušné aspekty operací zpracování?

- *Příklad: Aby známka ochrany soukromí ve zdravotnictví (Privacy Health Mark) splňovala požadavky podle článku 9, musí zahrnovat veškeré údaje z hodnocení týkající se zdraví.*

d. Umožňuje rozsah mechanismu pro vydávání osvědčení smysluplné vydávání osvědčení o ochraně údajů s přihlédnutím k povaze, obsahu a riziku souvisejících operací zpracování?

- *Příklad: Pokud se rozsah mechanismu pro vydávání osvědčení zaměřuje pouze na konkrétní aspekty operací zpracování, například shromažďování údajů, ale nikoli na operace dalšího zpracování, například zpracování za účelem vytvoření reklamních profilů nebo správy práv subjektu údajů, nebylo by to pro subjekty údajů smysluplné.*

e. Zahrnuje rozsah mechanismu pro vydávání osvědčení zpracování osobních údajů v příslušné zemi, kde je žádost podána, nebo řeší přeshraniční zpracování a/nebo předávání?

f. Popisují kritéria pro vydávání osvědčení dostatečně, jak by měl být cíl hodnocení vymezen?

- *Příklad: Pečeť ochrany soukromí (Privacy Seal) nabízející obecný rozsah vyžadující pouze „specifikaci zpracování, které podléhá vydání osvědčení“, by neposkytla dostatečně jasné pokyny, jak stanovit a popsat cíl hodnocení.*

- *Příklad: (Konkrétní) rozsah pečeti potvrzující bezpečné uložení osobních údajů v digitálním trezoru (The Privacy Vault Seal) by měl ve svých kritériích podrobně popisovat požadavky pro splnění tohoto rozsahu, např. definici trezoru, systémové požadavky, povinná technická a organizační opatření. V takovém případě může rozsah jasně vymezit cíl hodnocení.*

    (1) Vyžadují kritéria, aby cíl hodnocení zahrnoval určení všech příslušných operací zpracování, znázornění toku údajů a stanovení oblasti použití cíle hodnocení?

    - *Příklad: Mechanismus pro vydávání osvědčení nabízí vydávání osvědčení pro operace zpracování správců podle obecného nařízení o ochraně osobních údajů bez dalšího upřesnění oblasti použití (obecný rozsah). Kritéria používaná mechanismem vyžadují, aby žádající správce určil cílenou operaci zpracování (cíl hodnocení) z hlediska typů údajů, použitých systémů a procesů.*

    (2) Vyžadují kritéria, aby žadatel objasnil, kde zpracování, které je předmětem hodnocení, začíná a končí? Vyžadují kritéria, aby cíl hodnocení zahrnoval rozhraní, pokud vzájemně závislé operace zpracování nejsou do cíle hodnocení zahrnuty? A je to uspokojivě zdůvodněno?

    - *Příklad: Cíl hodnocení dostatečně podrobně popisující operaci zpracování internetové služby, například zahrnutí registrace uživatelů, poskytování služby, fakturace, protokolování IP adres, rozhraní s uživateli a třetími stranami a vyloučení hostování na serveru (avšak zahrnutí dohod o zpracování a o technických a organizačních opatřeních).*

g. Zaručují kritéria, že (jednotlivé) cíle hodnocení jsou srozumitelné pro příslušnou cílovou skupinu, případně i pro subjekty údajů?

3 OBECNÉ POŽADAVKY

a. Jsou všechny příslušné pojmy používané v katalogu kritérií (tj. kompletní soubor kritérií pro vydávání osvědčení) určeny, vysvětleny a popsány?

b. Jsou určeny všechny normativní odkazy?

c. Zahrnují kritéria definici odpovědnosti, postupů a zpracování v oblasti ochrany osobních údajů, na něž se vztahuje mechanismus pro vydávání osvědčení?

4 OPERACE ZPRACOVÁNÍ, ČL. 42 ODST. 1

Pokud jde o rozsah mechanismu pro vydávání osvědčení (obecný nebo konkrétní), zohledňují kritéria všechny příslušné složky operací zpracování (data, systémy a procesy)?

a. Vyžadují kritéria určení platného právního základu zpracování, pokud jde o cíl hodnocení?

b. Pokud jde o cíl hodnocení, uznávají kritéria příslušné fáze zpracování a celý životní cyklus údajů, včetně výmazu anebo anonymizace?

c. Pokud jde o cíl hodnocení, vyžadují kritéria přenositelnost údajů?

d. Pokud jde o cíl hodnocení, umožňují kritéria určení a zohlednění zvláštních druhů operací zpracování, např. automatizované rozhodování, profilování?

e. Pokud jde o cíl hodnocení, umožňují kritéria určení zvláštních kategorií údajů?

f. Umožňují a vyžadují kritéria posouzení rizika jednotlivých operací zpracování a potřeb ochrany pro práva a svobody subjektů údajů?

g. Umožňují a vyžadují kritéria náležité zohlednění rizika pro práva a svobody fyzických osob?

…

5 ZÁKONNOST ZPRACOVÁNÍ

a. Vyžadují kritéria kontrolu zákonnosti zpracování pro jednotlivé operace zpracování, pokud jde o účel a nezbytnost zpracování?

b. Vyžadují kritéria kontrolu všech požadavků právního základu pro jednotlivé operace zpracování?

6 ZÁSADY, ČLÁNEK 5

a. Zohledňují kritéria náležitě všechny zásady ochrany údajů podle článku 5?

b. Vyžadují kritéria prokázání minimalizace údajů pro jednotlivé cíle hodnocení?

…

7 OBECNÉ POVINNOSTI SPRÁVCŮ A ZPRACOVATELŮ

a. Vyžadují kritéria prokázání smluvních dohod mezi zpracovateli a správci?

b. Jsou dohody mezi správci a zpracovateli předmětem hodnocení?

c. Odrážejí kritéria povinnosti správce podle kapitoly IV?

d. Vyžadují kritéria důkaz o přezkoumání a aktualizaci technických a organizačních opatření zavedených správcem podle čl. 24 odst. 1?

e. Zahrnují kritéria kontrolu, jestli organizace posoudila, zda by měl být jmenován pověřenec pro ochranu osobních údajů, jak vyžaduje článek 37? Splňuje pověřenec pro ochranu osobních údajů, je-li to relevantní, požadavky podle článků 37 až 39?

f. Zahrnují kritéria kontrolu, zda jsou vyžadovány záznamy o činnostech zpracování v souladu s čl. 30 odst. 5, a zohledňují náležitě požadavky podle článku 30?

8 PRÁVA SUBJEKTŮ ÚDAJŮ

a. Zohledňují kritéria náležitě právo subjektu údajů na informace a vyžadují zavedení příslušných opatření?

b. Vyžadují kritéria, aby subjekty údajů měly přiměřený, nebo dokonce větší přístup ke svým údajům a kontrolu nad nimi, včetně přenositelnosti údajů?

c. Vyžadují kritéria, aby byla zavedena opatření, která umožní zásah do operace zpracování, aby byla zaručena práva subjektů údajů a umožněny opravy, výmaz nebo omezení?

…

9 RIZIKA PRO PRÁVA A SVOBODY FYZICKÝCH OSOB

a. Umožňují a vyžadují kritéria posouzení rizik pro práva a svobody fyzických osob?

b. Stanoví nebo vyžadují kritéria uznávanou metodiku posuzování rizik? Pokud ano, je přiměřená?

c. Umožňují a vyžadují kritéria posouzení vlivu zamýšlených operací zpracování na práva a svobody fyzických osob?

d. Vyžadují kritéria předchozí konzultaci týkající se zbývajících rizik, která nemohla být zmírněna, na základě výsledků posouzení vlivu na ochranu osobních údajů?

10 TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ ZARUČUJÍCÍ OCHRANU

a. Vyžadují kritéria použití technických a organizačních opatření zajišťujících důvěrnost operací zpracování?

b. Vyžadují kritéria použití technických a organizačních opatření zajišťujících integritu operací zpracování?

c. Vyžadují kritéria použití technických a organizačních opatření zajišťujících dostupnost operací zpracování?

d. Vyžadují kritéria použití opatření zajišťujících transparentnost operací zpracování, jde-li o

e. odpovědnost?

f. práva subjektů údajů?

g. posouzení jednotlivých operací zpracování, např. pro algoritmickou transparentnost?

h. Vyžadují kritéria použití technických a organizačních opatření zaručujících práva subjektů údajů, např. schopnost poskytovat informace nebo přenositelnost údajů?

i. Vyžadují kritéria použití technických a organizačních opatření umožňujících zasáhnout do operace zpracování, aby byla zaručena práva subjektů údajů a umožněny opravy, výmaz nebo omezení?

j. Vyžadují kritéria použití opatření umožňujících zasáhnout do operace zpracování za účelem opravy nebo kontroly systému nebo procesu?

k. Vyžadují kritéria použití technických a organizačních opatření s cílem zajistit minimalizaci údajů, například zrušení propojení údajů a subjektu údajů nebo jejich oddělení, anonymizace nebo pseudonymizace nebo izolace datových systémů?

l. Vyžadují kritéria technická opatření k zavedení standardní ochrany údajů?

m. Vyžadují kritéria technická a organizační opatření zavádějící záměrnou ochranu údajů, např. systém řízení ochrany údajů k prokazování, sdělování, řízení a prosazování požadavků na ochranu údajů?

n. Vyžadují kritéria technická a organizační opatření zavádějící náležitou pravidelnou odbornou přípravu a vzdělávání pracovníků, kteří mají trvalý nebo pravidelný přístup k osobním údajům?

o. Vyžadují kritéria přezkum opatření?

p. Vyžadují kritéria sebehodnocení / interní audit?

q. Vyžadují kritéria opatření, které zajistí, že povinnosti týkající se ohlašování případů porušení zabezpečení osobních údajů jsou plněny v přiměřené době a v přiměřeném rozsahu?

r. Vyžadují kritéria zavedení a ověřování postupů pro řízení incidentů?

s. Vyžadují kritéria monitorování vývoje v oblasti ochrany soukromí a technologií a aktualizaci systému v souladu s požadavky?

…

11 JINÉ ZVLÁŠTNÍ PRVKY VSTŘÍCNÉ OCHRANĚ OSOBNÍCH ÚDAJŮ

a. Vyžadují kritéria zavedení technik zvyšujících ochranu údajů? Sem mohou patřit kritéria, která vyžadují zvýšenou ochranu dat odstraněním nebo snížením rizika v oblasti osobních údajů a/nebo ochrany údajů.

- *Příklad: Kritéria, která vyžadují zvýšenou nepropojitelnost s využitím řízení identity uživatele zaměřeného na uživatele, například přihlašovací údaje založené na atributech, namísto řízení identity zaměřeného na organizaci, by odrážela techniku zvyšující ochranu údajů.*

b. Vyžadují kritéria zavedení rozšířené kontroly ze strany subjektů údajů k usnadnění sebeurčení a volby?

…

12 KRITÉRIA PRO ÚČELY PROKÁZÁNÍ EXISTENCE VHODNÝCH ZÁRUK PRO PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ

Kritéria budou zohledněna v připravovaných pokynech na základě čl. 42 odst. 2.

13 DALŠÍ KRITÉRIA PRO EVROPSKOU PEČEŤ OCHRANY ÚDAJŮ

a. Mají kritéria pokrýt všechny členské státy?

b. <u>možňují</u> kritéria zohlednit právní předpisy a situace v oblasti ochrany osobních údajů v členských státech?

c. Vyžadují kritéria hodnocení jednotlivých cílů hodnocení, pokud jde o právní předpisy členských států v oblasti ochrany údajů v daném odvětví?

d. Vyžadují kritéria, aby správce nebo zpracovatel poskytl subjektům údajů a zúčastněným stranám v jazycích členských států

e. informace týkající se zpracování / cíle hodnocení?

f. dokumentaci zpracování / cíle hodnocení?

g. výsledky hodnocení?

…

14 CELKOVÉ HODNOCENÍ KRITÉRIÍ

a. Pokrývají kritéria plně rozsah mechanismu pro vydávání osvědčení (tj. komplexní kritéria) s cílem poskytnout dostatečné záruky tak, aby bylo vydané osvědčení důvěryhodné?

- *Příklad: Pokud se rozsah mechanismu pro vydávání osvědčení zaměřuje na operace zpracování údajů o zdravotním stavu, měla by být zaručena vysoká úroveň ochrany údajů tím, že budou vymezena kritéria, která zajistí například podrobné posouzení a uplatňování zásad záměrné a standardní ochrany údajů.*

b. Jsou kritéria úměrná velikosti operace zpracování, která je zohledňována v rozsahu mechanismu pro vydávání osvědčení, citlivosti informací a riziku zpracování?

c. Je pravděpodobné, že kritéria zlepší dodržování ochrany osobních údajů ze strany správců a zpracovatelů?

d. Bude to pro subjekty údajů znamenat přínos z hlediska jejich práva na informace, včetně vysvětlení požadovaných výsledků subjektům údajů?