



Stanovisko 14/2026 ke kritériím pro vydávání osvědčení Europrivacy, pokud jde o jejich schválení sborem jako evropské pečeti ochrany údajů podle čl. 42 odst. 5 GDPR

Přijato dne 15. dubna 2026

Obsah

1 Shrnutí skutečností.....	3
2 Posouzení.....	4
2.1 Rozsah mechanismu pro vydávání osvědčení a cíl hodnocení	5
2.2 Operace zpracování.....	6
2.3 Zákonnost zpracování.....	6
2.4 Zásady zpracování údajů	7
2.5 Obecné povinnosti správců a zpracovatelů	7
2.6 Práva subjektů údajů.....	8
2.7 Rizika pro práva a svobodu.....	8
2.8 Technická a organizační opatření zaručující ochranu.....	8
2.9 Kritéria pro účely prokázání existence vhodných záruk pro předávání osobních údajů	9
3 Další kritéria pro evropskou pečeť ochrany údajů	9
4 Závěry a doporučení	10
5 Závěrečné poznámky.....	10

Evropský sbor pro ochranu osobních údajů,

s ohledem na články 42 a 63 a čl. 64 odst. 2 [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 „GDPR“),

s ohledem na Dohodu o Evropském hospodářském prostoru (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 2018¹,

s ohledem na články 10 a 22 svého jednacího řádu,

vzhledem k těmto důvodům:

1. Členské státy, dozorové úřady, Evropský sbor pro ochranu osobních údajů (dále jen „EDPB“ nebo „sbor“) a Evropská komise podpoří zejména na úrovni Unie zavedení mechanismů pro vydávání osvědčení o ochraně údajů (dále jen „mechanismy pro vydávání osvědčení“) a pečeti a značek dokládajících ochranu údajů za účelem prokázání souladu operací zpracování prováděných správci a zpracovateli s GDPR, a to s přihlédnutím ke zvláštním potřebám mikropodniků a malých a středních podniků. Zavedení mechanismů pro vydávání osvědčení může navíc zvýšit transparentnost a umožnit subjektům údajů posoudit úroveň ochrany údajů v případě příslušných produktů a služeb.
2. Kritéria pro vydávání osvědčení tvoří nedílnou součást mechanismu pro vydávání osvědčení. GDPR proto vyžaduje, aby kritéria vnitrostátního mechanismu pro vydávání osvědčení schválil příslušný dozorový úřad (čl. 42 odst. 5 a čl. 43 odst. 2 písm. b) GDPR) a aby evropskou pečeť ochrany údajů schválil EDPB (čl. 42 odst. 5 a čl. 70 odst. 1 písm. o) GDPR).
3. Pokud dozorový úřad hodlá navrhnout EDPB schválení evropské pečeti ochrany údajů podle čl. 42 odst. 5 GDPR, měl by dozorový úřad uvést záměr vlastníka systému nabízet mechanismus pro vydávání osvědčení ve všech členských státech. V tomto případě je hlavní úlohou EDPB zajistit důsledné uplatňování GDPR prostřednictvím mechanismu jednotnosti uvedeného v člancích 63, 64 a 65 GDPR. V tomto rámci schvaluje podle čl. 64 odst. 2 GDPR kritéria pro vydávání osvědčení EDPB.
4. Cílem tohoto stanoviska je zajistit důsledné uplatňování nařízení GDPR, a to i ze strany dozorových úřadů, správců a zpracovatelů s ohledem na základní prvky, které musí mechanismy pro vydávání osvědčení stanovit. Posuzování ze strany EDPB se provádí zejména na základě „Pokynů 1/2018 týkajících se vydávání osvědčení a určování kritérií pro vydávání osvědčení podle článků 42 a 43 nařízení“ (dále jen „pokyny“) a jejich dodatku obsahujícího „pokyny k posuzování kritérií pro vydávání osvědčení“ (dále jen „dodatek“), u něhož dne 26. května 2021 skončilo období veřejné konzultace.
5. V souladu s tím EDPB uznává, že každý mechanismus pro vydávání osvědčení by měl být řešen individuálně a že jím není dotčeno posouzení jakéhokoli jiného mechanismu pro vydávání osvědčení.
6. Mechanismy pro vydávání osvědčení by měly správcům a zpracovatelům umožnit prokázat soulad s GDPR. Jejich kritéria by proto měla řádně odrážet požadavky a zásady týkající se ochrany osobních údajů stanovené v GDPR a přispívat k jeho důslednému uplatňování.
7. Vlastník systému by měl zároveň zajistit soulad a shodu mechanismu pro vydávání osvědčení se všemi zahrnutými nebo využitými normami ISO a postupy pro vydávání osvědčení.

¹ Odkazy na „členské státy“ v celém tomto dokumentu je třeba chápat jako odkazy na „členské státy EHP“.

8. V důsledku toho by osvědčení měla správcům a zpracovatelům přinášet přidanou hodnotu tím, že pomohou zavést standardizovaná a specifikovaná organizační a technická opatření, která prokazatelně usnadní a zvýší soulad operací zpracování s GDPR, a to s přihlédnutím k požadavkům specifickým pro dané odvětví.
9. EDPB vítá úsilí vlastníků systémů o vypracování mechanismů pro vydávání osvědčení, které jsou praktickým a potenciálně nákladově efektivním nástrojem k zajištění většího souladu s GDPR a podpoře práva na soukromí a ochranu údajů subjektů údajů prostřednictvím zvýšení transparentnosti.
10. Sbor připomíná, že osvědčení jsou dobrovolnými nástroji odpovědnosti a že dodržování mechanismu pro vydávání osvědčení nesnižuje odpovědnost správců nebo zpracovatelů za dodržování nařízení GDPR ani nebrání dozorovým úřadům ve výkonu jejich úkolů a pravomocí podle nařízení GDPR a příslušných vnitrostátních právních předpisů.
11. V tomto stanovisku se EDPB zabývá otázkami, jako jsou rozsah kritérií a jejich použitelnost a význam ve všech členských státech.
12. Toto stanovisko EDPB se zaměřuje pouze na kritéria pro vydávání osvědčení. EDPB může požadovat informace na vysoké úrovni o metodách hodnocení, aby mohl důkladně posoudit přezkoumatelnost kritérií v souvislosti se svým stanoviskem. To však neznamená, že je toto stanovisko zároveň schválením těchto metod hodnocení.
13. Stanovisko EDPB se přijímá postupem podle čl. 64 odst. 2 nařízení GDPR ve spojení s čl. 10 odst. 2 jednacího řádu EDPB, a to do osmi týdnů od prvního pracovního dne poté, co předseda a příslušný dozorový úřad rozhodli, že spis je úplný. Z rozhodnutí předsedy může být tato lhůta s přihlédnutím k náročnosti dané věci prodloužena o dalších šest týdnů. Dospěje-li EDPB ve svém stanovisku k závěru, že kritéria nelze v daném okamžiku schválit, může je dozorový úřad znovu předložit ke schválení, jakmile budou vyřešeny námítky vyjádřené v původním stanovisku EDPB,

přijal toto stanovisko:

1 Shrnutí skutečností

14. V souladu s čl. 42 odst. 5 nařízení GDPR a pokyny vypracovalo Evropské středisko pro vydávání osvědčení a ochranu soukromí (dále jen „vlastník systému“) kritéria pro vydávání osvědčení Europrivacy (verze 82) (dále jen „kritéria pro vydávání osvědčení“).
15. Lucemburský dozorový úřad předložil dne 29. ledna 2026 sboru EDPB ke schválení kritéria pro vydávání osvědčení Europrivacy (verze 82) podle čl. 64 odst. 2 GDPR.
16. Rozhodnutí o úplnosti spisu bylo přijato dne 31. března 2026.
17. EDPB připomíná, že dne 10. října 2022 vydáním stanoviska EDPB 28/2022 schválil kritéria pro vydávání osvědčení Europrivacy (verze 60) jako evropskou pečeť ochrany údajů podle čl. 42 odst. 5 GDPR (dále jen „předchozí stanovisko EDPB“).
18. Toto stanovisko se zabývá pozměněnou verzí kritérií pro vydávání osvědčení Europrivacy (verze 82). Sbor především konstatuje, že v této verzi kritérií pro vydávání osvědčení, která je v současné době předložena EDPB, byla oblast působnosti rozšířena na žadatele, na které se vztahuje čl. 3 odst. 2 GDPR, a v této souvislosti bylo zavedeno kritérium týkající se možného střetu s právními předpisy třetích zemí. Sbor dále konstatuje, že některá kritéria pro

vydávání osvědčení schválená EDPB v roce 2022 byla v pozměněné verzi kritérií pro vydávání osvědčení Europrivacy (verze 82) upravena, upřesněna a/nebo vyjasněna. Tyto změny se týkají zejména: jmenování zástupce v EHP a spolupráce na žádostech příslušných orgánů pro ochranu údajů v EHP; zprávy o posouzení plnění vnitrostátních povinností (dále jen „NOCAR“), dalšího zpracování, záruk doprovázejících zpracování zvláštních kategorií osobních údajů, práv subjektu údajů, zapojení dílčích zpracovatelů, řešení případů porušení zabezpečení údajů, posouzení rizik pro zpracování údajů a bezpečnostní politiky a požadavků.

19. EDPB zdůrazňuje, že změna kritérií pro vydávání osvědčení, která již byla schválena v roce 2022, ovlivní dosud vydaná osvědčení i probíhající procesy vydávání osvědčení. Proto by mělo být přechodné období mezi evropskými pečeti ochrany údajů vydávanými podle kritérií pro vydávání osvědčení schválených předchozím stanoviskem EDPB (verze 60) a pečeti vydávanými podle kritérií pro vydávání osvědčení (verze 82) posuzovaných v tomto stanovisku řízeno vhodným a transparentním způsobem. V tomto ohledu sbor na základě dokumentace poskytnuté vlastníkem systému chápe, že všechny probíhající procesy vydávání osvědčení musí být dokončeny do konce roku 2026 a po tomto okamžiku se kritéria pro vydávání osvědčení schválená předchozím stanoviskem EDPB (verze 60) již nebudou používat pro vydávání nových osvědčení. Dosud vydaná osvědčení zůstanou platná až do konce tříletého období platnosti a budou obnovena podle kritérií pro vydávání osvědčení (verze 82). Po konci roku 2029 budou proto kritéria pro vydávání osvědčení schválená předchozím stanoviskem EDPB (verze 60) plně nahrazena kritérii pro vydávání osvědčení (verze 82). Kromě toho vlastník systému zveřejní informace o tomto plánu přechodu. Je možné, že bude třeba provést určité úpravy v akreditaci subjektů pro vydávání osvědčení, ale toto stanovisko se touto otázkou nezabývá, protože se netýká působnosti EDPB.
20. Obecný systém pro vydávání osvědčení Europrivacy není určen jako nástroj pro předávání údajů podle čl. 42 odst. 2 a čl. 46 písm. f) GDPR. Dne 29. ledna 2026 předložil lucemburský dozorový úřad sboru EDPB ke schválení podle čl. 64 odst. 2 GDPR také dodatečný soubor kritérií pro vydávání osvědčení („Rozšíření systému pro vydávání osvědčení Europrivacy pro účely vydávání osvědčení dovozcům údajů podle článku 46“), jehož působnost se vztahuje na správce a zpracovatele se sídlem mimo EHP, kteří nepodléhají přímo nařízení GDPR podle čl. 3 odst. 2 GDPR, ale zpracovávají osobní údaje získané od jiného správce nebo zpracovatele údajů, na kterého se nařízení GDPR vztahuje. K tomuto souboru kritérií pro vydávání osvědčení, která mají být použita jako nástroj pro předávání údajů podle čl. 46 odst. 2 písm. f) GDPR, přijal EDPB stanovisko č. 15/2026.

2 Posouzení

21. EDPB provedl posouzení kritérií pro vydávání osvědčení za účelem jejich schválení podle čl. 42 odst. 5 GDPR v souladu se strukturou stanovenou v příloze 2 pokynů (dále jen „příloha“) a jejím dodatku.
22. V souvislosti s tímto stanoviskem a za účelem schválení kritérií pro vydávání osvědčení posoudil EDPB oddíly Předběžné kontroly žádostí a cíle hodnocení (A); Základní kritéria osvědčení Europrivacy podle GDPR (G) a Kontroly technologických a organizačních opatření (T), které jsou uvedeny spolu s kritérii pro vydávání osvědčení.

23. Dále sbor v této souvislosti konstatuje, že „doplňkové kontextové kontroly“², které jsou poskytovány spolu s kritérii pro vydávání osvědčení schválenými v předchozím stanovisku EDPB (verze 60) a jejichž cílem bylo zajistit, aby zpracování údajů zapojených do cíle hodnocení bylo v souladu s požadavky specifickými pro danou oblast a technologii³, nebyly v předchozím stanovisku EDPB schváleny a že tyto „doplňkové kontextové kontroly“ se již v aktualizované dokumentaci poskytnuté v souvislosti s tímto stanoviskem nevyskytují.
24. Sbor bere na vědomí, jak je objasněno v definicích systému, že odkazy na „příslušné úřady pro ochranu údajů“ v celém systému se myslí úřady pro ochranu údajů v EHP⁴.
25. S ohledem na definice právních předpisů třetí země má sbor za to, že se jedná o právní předpisy, které se vztahují na žadatele a/nebo na osobní údaje zpracovávané v cíli hodnocení, a to v rozsahu, v němž takové právní předpisy neukládají omezení práv na ochranu údajů, která jdou nad rámec toho, co je v demokratické společnosti nezbytné a přiměřené k zajištění jednoho z cílů uvedených v čl. 23 odst. 1 GDPR, jsou přiměřené sledovanému cíli, respektují podstatu práva na ochranu údajů, stanoví konkrétní opatření na ochranu základních práv a zájmů subjektů údajů.

2.1 Rozsah mechanismu pro vydávání osvědčení a cíl hodnocení

26. EDPB připomíná⁵, že systém pro vydávání osvědčení Europrivacy je obecný systém, neboť se zaměřuje na širokou škálu různých operací zpracování prováděných správci a zpracovateli z různých odvětví činnosti.
27. Sbor vítá, že v dokumentaci týkající se rozsahu tohoto systému pro vydávání osvědčení, kterou poskytl lucemburský dozorový úřad, se pozměněný systém osvědčení Europrivacy vztahuje na: i) správce a zpracovatele usazené v Evropské unii (EU) nebo v Evropském hospodářském prostoru (EHP); ii) správce a zpracovatele usazené mimo EHP, kteří podléhají GDPR podle čl. 3 odst. 2 GDPR buď proto, že nabízejí zboží nebo služby subjektům údajů v EHP, nebo proto, že monitorují chování subjektů údajů v EHP⁶. Použitelnost kritérií je definována v závislosti na roli a odpovědnosti žadatele.
28. Pokud jde o žadatele podle čl. 3 odst. 2 GDPR nacházející se ve třetí zemi, na které se nevztahuje rozhodnutí o přiměřenosti zahrnující cíl hodnocení, kritérium podle bodu A.2.1.6 definuje podmínky, které je třeba splnit při vymezení cíle hodnocení během přezkumu jejich žádosti o vydání osvědčení. Zejména před zvážením auditu vydávání osvědčení požaduje, aby subjekt pro vydávání osvědčení zkontroloval, zda je žadatel schopen prokázat, že vnitrostátní právní předpisy a praxe třetí země nebrání žadateli v plnění požadavků pro vydávání osvědčení. Pokud tomu tak není, proces vydávání osvědčení se ve fázi žádosti zastaví.
29. Sbor bere na vědomí, že správce údajů může procesu vydávání osvědčení Europrivacy podrobit cíl hodnocení, který podléhá společné správě (kritérium podle bodu A.2.1.5). V případě, že cíl hodnocení podléhá společné správě, chce sbor zdůraznit, že akreditovaný

² EDPB ve svém předchozím stanovisku „doplňkové kontextové kontroly“ neschválil.

³ Předchozí stanovisko EDPB, body 7 a 8.

⁴ Viz definici „příslušného dozorového úřadu“ stanovenou v kritériích osvědčení Europrivacy: „*Pojem „Příslušný úřad pro ochranu osobních údajů“ se vztahuje na úřady pro ochranu osobních údajů v EHP. Celkově se týká vnitrostátních úřadů pro ochranu osobních údajů, které mají pravomoc prosazovat soulad osobních údajů zpracovávaných cílem hodnocení. V případě osvědčení podle GDPR vydaného dovozci údajů podle článku 46 GDPR je příslušným úřadem pro ochranu osobních údajů úřad příslušný pro vývozce údajů v EHP, s výjimkou podání stížnosti, kdy je příslušný kterýkoli úřad v EHP.*“

⁵ Předchozí stanovisko EDPB, bod 6.

⁶ Viz Pokyny EDPB k místní působnosti GDPR (článek 3), verze 2.1, přijaté dne 12. listopadu 2019, oddíl 2.

subjekt pro vydávání osvědčení bude muset pečlivě provést proces žádosti, aby se ujistil, že je cíl hodnocení smysluplný a že žadatel je plně odpovědný za soulad cíle hodnocení se všemi povinnostmi podle GDPR, které má systém pro vydávání osvědčení prokázat. V důsledku toho by ujednání uzavřené mezi žadatelem a ostatními společnými správci zainteresovanými na cíli hodnocení, pokud jde o jejich příslušnou odpovědnost za dodržování povinností podle GDPR, mohlo v závislosti na okolnostech činností zpracování daného cíle hodnocení bránit žadateli ve splnění kritérií pro vydávání osvědčení.

2.2 Operace zpracování

30. Jak EDPB uvedl ve svém předchozím stanovisku, kritéria pro vydávání osvědčení se zabývají příslušnými složkami operací zpracování (údaje, systémy a zpracování) s ohledem na obecný rozsah působnosti systému vydávání osvědčení. Kritéria pro vydávání osvědčení umožňují zejména určit zvláštní kategorie údajů definované v článku 9 GDPR (oddíl G.2 kritérií – Zpracování zvláštních kategorií údajů).

2.3 Zákonnost zpracování

31. Jak EDPB uvedl ve svém předchozím stanovisku k již schváleným kritériím pro vydávání osvědčení (verze 60), kritéria pro vydávání osvědčení vyžadují kontrolu zákonnosti zpracování údajů v případě každé jednotlivé operace zpracování v rámci daného cíle hodnocení a vyžadují kontrolu požadavků na právní základ podle článku 6 nařízení GDPR (oddíl G.1 kritérií – Zákonnost zpracování údajů). Sbor zejména vítá, že aktualizovaná kritéria pro vydávání osvědčení vyžadují, aby se souhlas subjektů údajů vztahoval na každý účel, pro který je zpracování prováděno, a aby odvolání souhlasu nemělo za následek újmu subjektu údajů.
32. Jak bylo uvedeno v předchozím stanovisku EDPB, kritéria pro vydávání osvědčení navíc vyžadují kontrolu konkrétních požadavků na podmínky, za nichž je podle čl. 9 odst. 2 GDPR povoleno zpracování zvláštních kategorií osobních údajů (oddíl G.2.1 kritérií – Zpracování zvláštních kategorií údajů), a uvedení dalších omezení a záruk pro práva a svobody subjektu údajů. Kritéria pro vydávání osvědčení rovněž vyžadují ověření požadavků na podmínky definovaných v článku 10 GDPR pro zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů (oddíl G.2.2 kritérií), je-li to relevantní. V tomto ohledu sbor rovněž vítá, že aktualizovaná kritéria pro vydávání osvědčení (kritérium podle bodu G.2.1.3 – Dodatečné záruky pro zpracování zvláštních kategorií osobních údajů) rovněž vyžadují, aby žadatel zavedl dodatečná omezení a záruky přizpůsobené zvláštní povaze údajů a odpovídajícím rizikům, pokud se zpracování týká zvláštních kategorií osobních údajů.
33. Pokud jde o žadatele podle čl. 3 odst. 2 GDPR, kteří se nacházejí ve třetí zemi, na niž se nevztahuje rozhodnutí o odpovídající ochraně zahrnující cíl hodnocení, aktualizovaná kritéria pro vydání osvědčení navíc vyžadují, aby žadatel předložil zprávu vypracovanou právním odborníkem, v níž se posuzuje, zda vnitrostátní právní předpisy a praxe třetí země nebrání plnění povinností v oblasti ochrany údajů podle GDPR. Stejně tak musí být posouzeno, zda vnitrostátní právní předpisy třetí země neukládají omezení práv na ochranu údajů nad rámec toho, co je v demokratické společnosti nezbytné a přiměřené k zajištění jednoho z cílů uvedených v čl. 23 odst. 1 GDPR, zda jsou přiměřené sledovanému cíli, zda respektují podstatu práva na ochranu údajů a zda stanoví zvláštní opatření na ochranu základních práv a zájmů subjektů údajů. Musí být také přezkoumáno, zda mohou regulační nebo organizační změny bránit plnění kritérií nebo ovlivnit cíl hodnocení či práva subjektů údajů, a subjekt pro vydávání osvědčení by o tom měl být informován (kritérium podle bodu G.1.1.5).

34. V této souvislosti aktualizovaná kritéria pro vydávání osvědčení v pokynech objasňují, že „pokud je žadatel usazen mimo EHP a využívá rozhodnutí o odpovídající ochraně, které se týká zpracování prováděného v rámci cíle hodnocení, lze splnění tohoto požadavku prokázat prostřednictvím zjednodušené zprávy“. Podle těchto kritérií by tato zpráva měla posoudit, zda je rozhodnutí o odpovídající ochraně platné, a zdokumentovat důvody, proč cíl hodnocení spadá do oblasti působnosti rozhodnutí o odpovídající ochraně“ (kritérium podle bodu G.1.1.5, písmena F).

2.4 Zásady zpracování údajů

35. EDPB připomíná, že kritéria pro vydávání osvědčení přiměřeně zohledňují zásady ochrany údajů podle článku 5 GDPR. Aktualizovaná kritéria pro vydávání osvědčení zejména rozšiřují a dále rozvádějí zásadu účelového omezení tím, že zahrnují zvláštní kritérium, které vyžaduje prokázání toho, že osobní údaje nejsou dále zpracovávány způsobem, který je s těmito účely neslučitelný, a že každé další zpracování by mělo být zvlášť posouzeno jako zákonné a že posouzení slučitelnosti účelu je provedeno a řádně zdokumentováno pro další zpracování údajů (kritérium podle bodu G.1.1.6).

2.5 Obecné povinnosti správců a zpracovatelů

36. Sbor EDPB připomíná, že kritéria pro vydávání osvědčení⁷ odrážejí povinnosti správce podle článku 24 GDPR (oddíl G.4 – Odpovědnost správce údajů) a vyžadují posouzení smluvních ujednání mezi zpracovatelem a správcem podle článku 28 nařízení GDPR (oddíl G.5 kritérií – Zpracovatelé nebo dílčí zpracovatelé údajů).
37. Sbor dále vítá doplnění toho, že kritéria pro vydávání osvědčení vyžadují, aby žadatel podle čl. 3 odst. 2 GDPR určil kancelář nebo zástupce v EHP podle článku 27 nařízení GDPR, jehož kontaktní údaje jsou k dispozici na internetových stránkách žadatele (kritérium G.4.1.4). Sbor bere tato kritéria pro vydávání osvědčení na vědomí a připomíná, že se nejedná vždy o povinnost správců a zpracovatelů podle GDPR, a proto je třeba mít na paměti podmínky stanovené v článku 27 GDPR.
38. Kromě toho EDPB podotýká, jak uvedl ve svém předchozím stanovisku, že kritéria pro vydání osvědčení vyžadují, aby všichni žadatelé jmenovali pověřence pro ochranu osobních údajů, a to i v případě, že žadatel není povinen jmenovat pověřence pro ochranu osobních údajů podle článku 37 GDPR. Kritéria ověřují, zda pověřenec pro ochranu osobních údajů splňuje požadavky podle článků 37 až 39 (oddíl G.9 kritérií – Pověřenec pro ochranu osobních údajů).
39. Stejně tak kritéria pro vydávání osvědčení vyžadují kontrolu obsahu záznamů o činnostech zpracování v souladu s článkem 30 GDPR (oddíl G.5.3 kritérií – Záznamy o činnostech zpracování). V tomto ohledu sbor vítá, že aktualizovaná kritéria pro vydávání osvědčení v případě žadatelů podle čl. 3 odst. 2 GDPR vyžadují, aby spolupracovali při žádostech příslušných orgánů pro ochranu údajů v EHP a na požádání jim zpřístupnili záznamy o činnostech zpracování (kritérium G.5.3.5).
40. Stejně tak EDPB podotýká, že byla zahrnuta některá další kritéria pro vydávání osvědčení týkající se zapojení dílčích zpracovatelů pro žadatele, kteří působí jako správci nebo zpracovatelé (oddíl G.5.1.2 – Zapojení dílčích zpracovatelů). Toto rozlišení umožňuje lépe zohlednit rozdělení rolí a odpovědnosti mezi účastníky zpracovatelského řetězce.

⁷ Předchozí stanovisko EDPB, bod 15.

2.6 Práva subjektů údajů

41. Stejně jako ve svém předchozím stanovisku EDPB připomíná, že kritéria pro vydávání osvědčení se dostatečně zabývají právem subjektu údajů na informace v souladu s kapitolou III GDPR a vyžadují zavedení příslušných opatření⁸. Kritéria pro vydávání osvědčení rovněž vyžadují zavedení opatření umožňujících zasáhnout do operace zpracování s cílem zaručit práva subjektů údajů a umožnit opravy, výmaz nebo omezení zpracování (oddíl G.3 kritérií – Práva subjektů údajů).
42. Kromě toho EDPB vítá zlepšení, k nimž došlo v kritériích pro vydávání osvědčení, pokud jde o informace, které mají být poskytnuty subjektům údajů (oddíl G 3.2 – Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů, a oddíl G.3.3 – Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů), o způsoby komunikace se subjekty údajů⁹ a pro účely výkonu práv subjektů údajů¹⁰ (oddíl G 3.1 – Transparentní informace, sdělení a postupy pro výkon práv subjektů údajů), jakož i o právo na přístup (oddíl G 3.4 – Právo subjektu údajů na přístup k osobním údajům), na výmaz (oddíl G.3.6 – Právo na výmaz („právo být zapomenut“)), na omezení zpracování (kritérium G 3.7.1 – Právo na omezení zpracování), o oznamovací povinnost týkající se opravy nebo výmazu osobních údajů nebo omezení zpracování (kritérium G.3.8.2 – Povinnost informovat subjekty údajů o příjemcích, pokud o to požádají), o právo vznést námitku (kritérium G.3.10 – Právo vznést námitku) a o právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování (kritérium G.3.11 – Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování).

2.7 Rizika pro práva a svobodu

43. EDPB již ve svém předchozím stanovisku uvedl, že kritéria pro vydávání osvědčení vyžadují posouzení rizika pro práva a svobody fyzických osob při zpracování údajů v rámci daného cíle hodnocení v souladu s článkem 35 GDPR (oddíl G.8 kritérií – Povinnost posoudit, zda je vyžadováno posouzení vlivu na ochranu osobních údajů)¹¹.
44. EDPB vítá změny provedené v kritériích pro vydávání osvědčení s cílem stanovit, že „žadatel měl opakovatelnou metodikou posoudit rizika, která zpracování představuje a která mohou mít dopad na práva a svobody fyzických osob“ (oddíl G.6.2.4 – Posouzení rizik pro zpracování údajů).
45. Kromě toho EDPB vítá další doplnění a podrobnosti, které zavedla kritéria pro vydávání osvědčení. EDPB například bere na vědomí doplnění procesu posouzení vlivu na ochranu osobních údajů týkající se situací, kdy žadatel není povinen toto posouzení provést (oddíl G.8.2.1 – Požadavky na proces posouzení vlivu na ochranu osobních údajů).

2.8 Technická a organizační opatření zaručující ochranu

⁸ Předchozí stanovisko EDPB, bod 19.

⁹ Například kritérium G.3.1.1 – Povinnosti informovat ve srozumitelném jazyce – dále rozvádí informace o zpracování údajů poskytované žadatelem subjektu údajů, které nyní zahrnují, že by i) měly být poskytnuty písemně nebo jinými prostředky, ii) měly být k dispozici v úředním jazyce (úředních jazycích) žadatele a iii) měly být dostupné v jazyce cílových subjektů údajů.

¹⁰ Například kritérium G.3.1.3 – Zajištění řádné správy a evidence práv subjektu údajů – nyní vyžaduje, aby žadatel měl zaveden postup nebo mechanismus, který by subjektu údajů potvrdil přijetí žádosti a vedl záznamy i o žádostech subjektu údajů s datem přijetí.

¹¹ Předchozí stanovisko EDPB, bod 20.

46. Jak je uvedeno v předchozím stanovisku EDPB, kritéria pro vydávání osvědčení vyžadují uplatnění technických a organizačních opatření zajišťujících důvěrnost, integritu a dostupnost operací zpracování. Kritéria rovněž vyžadují uplatnění technických opatření k provedení záměrné a standardní ochrany údajů v souladu s články 25 a 32 GDPR (oddíl G.6 kritérií – Záměrná a standardní ochrana údajů a zabezpečení zpracování, oddíl G.6.2 kritérií – Zabezpečení zpracování a oddíl T kritérií)¹². V tomto ohledu sbor vítá, že pozměněná kritéria pro vydávání osvědčení dále podrobněji popisují (oddíl G.6.1.2 – Standardní minimalizace údajů) pravidla a postupy, které musí žadatel použít, aby tato kritéria splnil.
47. Jak bylo zdůrazněno v předchozím stanovisku EDPB, kritéria pro vydávání osvědčení vyžadují uplatnění opatření, která zajistí, že povinnosti týkající se oznamování porušení zabezpečení osobních údajů budou plněny včas a v rozsahu podle článků 33 a 34 GDPR (oddíl G.7 kritérií – Řízení případů porušení zabezpečení osobních údajů).
48. V této souvislosti sbor konstatuje, že kritéria pro vydávání osvědčení byla dále zdokonalena a rozpracována. Konkrétně kritéria pro vydávání osvědčení nyní obsahují podrobnější seznam (oddíl G.7.1.1. – Povinnost dokumentovat porušení zabezpečení údajů), pokud jde o informace, které musí žadatel dokumentovat, pokud dojde k porušení zabezpečení údajů (např. kategorie osobních údajů, které jsou nebo mohou být dotčeny, přibližný počet subjektů údajů, které jsou nebo mohou být dotčeny; kategorie a přibližný počet záznamů osobních údajů, kterých se týká nebo může týkat, pravděpodobné důsledky porušení zabezpečení osobních údajů).

2.9 Kritéria pro účely prokázání existence vhodných záruk pro předávání osobních údajů

49. Jak sbor potvrdil ve svém předchozím stanovisku, kritéria pro vydávání osvědčení vyžadují identifikaci všech předání osobních údajů do třetích zemí a mezinárodním organizacím zainteresovaných na daném cíle hodnocení a zdůvodnění volby mechanismu pro předání údajů, který poskytuje vhodné záruky, podle kapitoly V GDPR (oddíl G.10 – Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím).
50. EDPB bere na vědomí, že pro žadatele podle čl. 3 odst. 2 GDPR se tato kritéria pro vydávání osvědčení použijí jak v případě předávání osobních údajů zahrnutých do cíle hodnocení subjektům nacházejícím se ve stejné třetí zemi, v níž se nachází žadatel, tak v případě, že se uvedené subjekty nacházejí v jiné třetí zemi.
51. Kromě toho sbor vítá, že kritéria pro vydávání osvědčení týkající se předávání osobních údajů byla nyní dále rozpracována a jasněji stanoví povinnosti žadatele v této oblasti (oddíl G.10.1 – Obecné povinnosti při mezinárodním předávání osobních údajů do třetích zemí nebo mezinárodním organizacím).

3 Další kritéria pro evropskou pečeť ochrany údajů

¹² Předchozí stanovisko EDPB, bod 21.

52. Podle pokynů musí posouzení zahrnovat otázku, „zda jsou kritéria schopna zohlednit právní předpisy nebo scénáře ochrany údajů v členských státech“. Jak bylo potvrzeno v předchozím stanovisku EDPB, oddíl G.1.1.3 kritérií pro vydávání osvědčení vyžaduje, aby žadatel předložil takové posouzení ve zprávě o posouzení dodržování vnitrostátních povinností (NOCAR). Tato zpráva musí obsahovat posouzení vnitrostátních povinností vztahujících se na cíl hodnocení a bude dokumentovat opatření přijatá žadatelem za účelem dodržení platných pravidel a případně i probíhající nápravná opatření. Žadatel nesmí používat seznam klíčových doplňkových vnitrostátních požadavků, který mu pro každou zemi poskytl vlastník systému, jako vyčerpávající seznam vnitrostátních povinností relevantních pro cíl hodnocení. Orientační seznam minimálních doplňkových kontrol a požadavků na kontroly poskytnutý vlastníkem systému není kritériem pro vydávání osvědčení v oblasti působnosti tohoto stanoviska.
53. Sbor vítá úpravy provedené v NOCAR v aktualizovaných kritériích (oddíl G.1.1.3 – Posouzení dodržování vnitrostátních povinností). Zejména je nyní vyjasněno, že žadatel by měl ve zprávě o posouzení dodržování vnitrostátních povinností (NOCAR) doložit posouzení souladu zpracování údajů „s doplňkovými vnitrostátními povinnostmi v EHP týkajícími se ochrany osobních údajů, které se na žadatele vztahují“. Zpráva NOCAR by měla mimo jiné obsahovat zejména jasnou identifikaci posuzovaného cíle hodnocení, seznam identifikovaných doplňkových vnitrostátních povinností na ochranu údajů v EHP, které se na cíl hodnocení vztahuje, jakož i hodnocení souladu cíle hodnocení s identifikovanými doplňkovými vnitrostátními povinnostmi na ochranu údajů v EHP. Sbor se domnívá, že v případě, že je žadatel usazen mimo EHP a vztahuje se na něj čl. 3 odst. 2 GDPR, je třeba povinnosti týkající se ochrany údajů na úrovni EHP, které se vztahují na cíl hodnocení, určit na základě místa, kde se nacházejí subjekty údajů, kterým žadatel nabízí zboží nebo služby nebo jejichž chování je sledováno.

4 Závěry a doporučení

54. Závěrem se EDPB domnívá, že kritéria pro vydávání osvědčení Europrivacy jsou v souladu s GDPR, a schvaluje je v souladu s úkolem sboru definovaným v čl. 70 odst. 1 písm. o) GDPR, což vede ke společnému vydávání osvědčení (evropská pečeť ochrany údajů).
55. EDPB považuje kritéria pro vydávání osvědčení za nedílnou součást systému pro vydávání osvědčení a zapíše systém pro vydávání osvědčení Europrivacy do veřejného rejstříku mechanismů pro vydávání osvědčení a pečeti a známek ochrany údajů a kritéria zveřejní v souladu s čl. 42 odst. 8 nařízení GDPR.

5 Závěrečné poznámky

56. Toto stanovisko je určeno lucemburskému dozorovému úřadu a bude zveřejněno podle čl. 64 odst. 5 písm. b) GDPR.

Za Evropský sbor pro ochranu osobních údajů

Předsedkyně

Anu Talus

