

# Stanovisko sboru (podle článku 64)



**Stanovisko 19/2004 ke kritériím EuroPrise pro vydávání  
osvědčení, pokud jde o jejich schválení EDPB jako evropské  
pečeti ochrany údajů podle čl. 42 odst. 5 (obecného nařízení  
o ochraně osobních údajů)**

**Přijato dne 16. července 2024**

## Obsah

1. SHRNU TÍ SKUTEČNOSTÍ .....	4
2. POSOUZENÍ .....	5
2.1 Oblast působnosti mechanismu pro vydávání osvědčení a cíl hodnocení.....	5
2.2 Zpracování .....	5
2.3 Zákonnost a zásady zpracování údajů .....	6
2.4 Obecné povinnosti správců a zpracovatelů .....	6
2.5 Práva subjektů údajů .....	6
2.6 Rizika pro práva a svobody .....	6
2.7 Technická a organizační opatření zaručující ochranu .....	6
2.8 Kritéria pro účely prokázání existence vhodných záruk pro předávání osobních údajů...	7
3. DALŠÍ KRITÉRIA PRO EVROPSKOU PEČEŤ OCHRANY ÚDAJŮ .....	7
ZÁVĚRY/DOPORUČENÍ .....	7
ZÁVĚREČNÉ PŘIPOMÍNKY .....	7

## Evropský sbor pro ochranu osobních údajů

s ohledem na článek 63, čl. 64 odst. 2 a článek 42 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 Evropském hospodářském prostoru (EHP), a zejména na přílohu XI a protokol 37 k této dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018<sup>1</sup>,

s ohledem na články 10 a 22 svého jednacího řádu,

- (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 zavedení pečeti a známek dokládajících ochranu osobních údajů pro účely prokázání souladu operací zpracování prováděných správci a zpracovateli s obecným nařízením o ochraně osobních údajů, přičemž zohlední specifické potřeby mikropodniků a malých a středních podniků.<sup>2</sup> Zavedení mechanismů pro vydávání osvědčení může navíc zvýšit transparentnost a umožnit subjektům údajů posoudit úroveň ochrany osobních údajů u příslušných produktů a služeb.<sup>3</sup>
- (2) Kritéria pro vydávání osvědčení jsou nedílnou součástí mechanismu pro vydávání osvědčení. Obecné nařízení o ochraně osobních údajů proto vyžaduje, aby kritéria vnitrostátního mechanismu pro vydávání osvědčení schválil příslušný dozorový úřad (čl. 42 odst. 5 a čl. 43 odst. 2 písm. b) obecného nařízení o ochraně osobních údajů) a aby evropskou pečeť ochrany údajů schválil EDPB (čl. 42 odst. 5 a čl. 70 odst. 1 písm. o) obecného nařízení o ochraně osobních údajů).
- (3) Pokud dozorový úřad hodlá navrhnout schválení evropské pečeti ochrany údajů ze strany EDPB podle čl. 42 odst. 5 obecného nařízení o ochraně osobních údajů, měl by uvést záměr vlastníka systému nabízet mechanismus pro vydávání osvědčení ve všech členských státech. V tomto případě je hlavní úlohou EDPB zajistit jednotné uplatňování obecného nařízení o ochraně osobních údajů prostřednictvím mechanismu jednotnosti podle článků 63, 64 a 65 obecného nařízení o ochraně osobních údajů. V tomto rámci podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů schvaluje kritéria pro vydávání osvědčení EDPB.
- (4) Cílem tohoto stanoviska je zajistit jednotné uplatňování obecného nařízení o ochraně osobních údajů, a to i ze strany dozorových úřadů, správců a zpracovatelů s ohledem na základní prvky, které musí mechanismy pro vydávání osvědčení rozpracovávat. Posouzení 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, který obsahuje „pokyny k posuzování kritérií pro vydávání osvědčení“ (dále jen „dodatek“), v souvislosti s nímž dne 26. května 2021 skončilo období veřejné konzultace.

<sup>1</sup> Pokud se v tomto stanovisku hovoří o „členských státech“, rozumějí se tím „členské státy EHP“.

<sup>2</sup> Čl. 42 odst. 1 obecného nařízení o ochraně osobních údajů.

<sup>3</sup> 100. bod odůvodnění obecného nařízení o ochraně osobních údajů.

- (5) V souladu s tím EDPB bere na vědomí, že ke každému mechanismu pro vydávání osvědčení by se mělo přistupovat 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 obecným nařízením o ochraně osobních údajů. Jejich kritéria by proto měla řádně splňovat požadavky a zásady týkající se ochrany osobních údajů stanovené v obecném nařízení o ochraně osobních údajů a přispívat k jeho jednotnému 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.
- (8) V důsledku toho by vydávání těchto osvědčení mělo přinášet přidanou hodnotu správcům a zpracovatelům tím, že pomůže zavést standardizovaná a stanovená organizační a technická opatření, která prokazatelně usnadní a posílí soulad operací zpracování s obecným nařízením o ochraně osobních údajů, a to s přihlédnutím k požadavkům specifickým pro dané odvětví.
- (9) EDPB vítá úsilí vlastníků systémů o vypracování mechanismů pro vydávání osvědčení, které představují praktický a potenciálně nákladově efektivní nástroj k zajištění většího souladu s obecným nařízením o ochraně osobních údajů a podpoře práva na soukromí a ochranu údajů subjektů údajů prostřednictvím zvýšení transparentnosti.
- (10) EDPB připomíná, že vydávání osvědčení představuje dobrovolný nástroj odpovědnosti a že dodržování mechanismu pro vydávání osvědčení nijak neomezuje odpovědnost správců nebo zpracovatelů za dodržování obecného nařízení o ochraně osobních údajů ani nebrání dozorovým úřadům ve výkonu jejich úkolů a pravomocí podle obecného nařízení o ochraně osobních údajů a příslušných vnitrostátních právních předpisů.
- (11) V tomto stanovisku se EDPB zabývá otázkami, jako jsou oblast působnosti kritérií a jejich použitelnost a význam ve všech členských státech.
- (12) Toto stanovisko se zaměřuje na kritéria pro vydávání osvědčení. Požaduje-li EDPB informace na vysoké úrovni o metodách hodnocení, aby mohl důkladně posoudit přezkoumatelnost kritérií v souvislosti se svým stanoviskem, neznamená to, že je toto stanovisko zároveň i schválením těchto metod hodnocení.
- (13) Stanovisko EDPB bude podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů ve spojení s čl. 10 odst. 2 jednacího řádu EDPB přijato do osmi týdnů od prvního pracovního dne poté, co předsedkyně a příslušný dozorový úřad rozhodnou, že předložený spis je úplný. Z rozhodnutí předsedkyně 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 vyřeší námítky vyjádřené v původním stanovisku EDPB,

## **PŘIJAL TOTO STANOVISKO:**

### **1. SHRnutí SKUTEČNOSTÍ**

1. V souladu s čl. 42 odst. 5 obecného nařízení o ochraně osobních údajů a s pokyny vypracovala společnost EuroPrise Cert GmbH (dále jen „vlastník systému“), což je německý právní subjekt, návrh „katalogu kritérií EuroPrise pro vydávání osvědčení vztahujících se na operace zpracování prováděné zpracovateli (oblast působnosti: EU), v1.5“ (dále jen „návrh kritérií pro vydávání osvědčení“, „kritéria pro vydávání osvědčení“ nebo „kritéria“) a předložila jej Landesbeauftragte für Datenschutz und

Informationsfreiheit Nordrhein-Westfalen, což je příslušný německý dozorový úřad v Severním Porýní-Vestfálsku.

2. Německý dozorový úřad předložil dne 29. dubna 2024 EDPB ke schválení návrh kritérií pro vydávání osvědčení podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů. Rozhodnutí o úplnosti spisu bylo přijato dne 29. května 2024.
3. Mechanismus EuroPrise pro vydávání osvědčení není mechanismem pro vydávání osvědčení podle čl. 46 odst. 2 písm. f) obecného nařízení o ochraně osobních údajů určeným pro mezinárodní předávání osobních údajů, a neposkytuje tudíž vhodné záruky v rámci předávání osobních údajů do třetích zemí nebo mezinárodním organizacím za podmínek uvedených v čl. 46 odst. 2 písm. f). K předání osobních údajů do třetí země nebo mezinárodní organizaci může dojít pouze v případě, že jsou dodržena ustanovení kapitoly V obecného nařízení o ochraně osobních údajů.

## 2. POSOUZENÍ

4. EDPB provedl posouzení kritérií pro vydávání osvědčení v rámci jejich schvalování podle čl. 42 odst. 5 obecného nařízení o ochraně osobních údajů v souladu se strukturou stanovenou v příloze 2 pokynů (dále jen „příloha“) a jejím dodatku.

### 2.1 Oblast působnosti mechanismu pro vydávání osvědčení a cíl hodnocení

5. Mechanismus EuroPrise pro vydávání osvědčení je založen na kritériích pro vydávání osvědčení v rámci celoevropského systému pro vydávání osvědčení vztahujících se na zpracování prováděná zpracovateli. Osvědčení, na která se vztahuje katalog kritérií, se týkají operací zpracování, které jsou prováděny v souvislosti s produkty, postupy a službami nebo s pomocí (i několika) produktů a služeb a u nichž žadatel o vydání osvědčení vystupuje jako zpracovatel. Hlavní kritéria tohoto mechanismu pro vydávání osvědčení jsou rozdělena do tří souborů požadavků, a to: právní požadavky (soubor 1), technická a organizační opatření (soubor 2) a práva subjektů údajů (soubor 3).
6. Žadatelé o vydání osvědčení musí být v rámci tohoto systému zpracovatelé. To zahrnuje zpracovatele, kteří jsou přímo pověřeni zpracováním osobních údajů správcem ve smyslu čl. 4 odst. 7 obecného nařízení o ochraně osobních údajů. Žadateli o vydání osvědčení však mohou být také zpracovatelé ve smyslu čl. 28 odst. 2 a 4 obecného nařízení o ochraně osobních údajů (další zpracovatelé).
7. Pokud zpracovatel, který je certifikován v rámci systému vydávání osvědčení EuroPrise, využívá dalšího zpracovatele, nemůže další zpracovatel tvrdit, že byl certifikován v rámci systému vydávání osvědčení EuroPrise. V takovém případě se osvědčení vztahuje pouze na operace zpracování prováděné původním, certifikovaným zpracovatelem. Další zpracovatelé však také mohou požádat o vydání osvědčení, což by vedlo k samostatnému a nezávislému postupu hodnocení.
8. EDPB konstatuje, že podle dokumentace týkající se oblasti působnosti mechanismu pro vydávání osvědčení, kterou předložil německý dozorový úřad, se systém EuroPrise vztahuje na zpracovatele se sídlem v Evropské unii (EU) nebo v Evropském hospodářském prostoru (EHP).

### 2.2 Zpracování

9. Oblast působnosti těchto kritérií není omezena na určité druhy operací zpracování. Jedná se spíše o metodiku, která je základem hodnocení EuroPrise a která umožňuje vydávání osvědčení pro jakékoli

operace zpracování prováděné zpracovateli. Jde tudíž o univerzální metodický přístup, na jehož základě lze vydávat osvědčení pro velké množství velmi odlišných operací zpracování. Je proto velmi důležité, aby byly dodrženy požadavky na metodiku, neboť jedině tak lze zajistit jednotné uplatňování kritérií pro vydávání osvědčení a srovnatelnou úroveň testování v rámci různých postupů vydávání osvědčení. Cílem je zajistit srovnatelnost a reprodukovatelnost vydaných osvědčení a jejich závěrů.

### 2.3 Zákonnost a zásady zpracování údajů

10. Podle kritérií je nutné přezkoumat, zda jsou operace zpracování, které mají být certifikovány, v souladu se zásadami záměrné a standardní ochrany osobních údajů (oddíl 1.5 kritérií), což zahrnuje účast žadatele na pomoci správci při provádění těchto zásad. To umožňuje posoudit soulad s článkem 25 obecného nařízení o ochraně osobních údajů ve spojení s článkem 5 tohoto nařízení. Ačkoli neexistují žádná kritéria přímo zaměřená na soulad s článkem 6 obecného nařízení o ochraně osobních údajů (vzhledem k tomu, že za zákonnost zpracování odpovídá správce), cílem těchto kritérií je zajistit, aby žadatelé z řad zpracovatelů navrhovali operace zpracování, které mají být certifikovány způsobem, jenž správcům pomůže dodržovat zásady ochrany osobních údajů podle článku 5 obecného nařízení o ochraně osobních údajů, včetně zásady zákonnosti zpracování.

### 2.4 Obecné povinnosti správců a zpracovatelů

11. Kritéria odrážejí vztah mezi zpracovatelem a správcem. Podle kritérií je zpracovatel zejména povinen mít vzor dohody o zpracování údajů se správcem, který zohledňuje všechny požadavky stanovené v článku 28 obecného nařízení o ochraně osobních údajů (oddíl 1.2 kritérií).
12. Podle kritérií musí žadatelé jmenovat pověřence pro ochranu osobních údajů podle článku 37 obecného nařízení o ochraně osobních údajů a předložit doklad o jeho jmenování (např. osvědčení o jmenování). Účelem je ověřit, zda pověřenec pro ochranu osobních údajů splňuje požadavky stanovené v článcích 37 až 39 (soubor 1, oddíl 1.1 kritérií).
13. Na základě kritérií se kontroluje obsah záznamů o činnostech zpracování v souladu s článkem 30 obecného nařízení o ochraně osobních údajů (soubor 1, oddíl 1.1 kritérií).

### 2.5 Práva subjektů údajů

14. Kritéria se dostatečně zabývají právem subjektu údajů na informace v souladu s kapitolou III obecného nařízení o ochraně osobních údajů a vyžadují zavedení příslušných opatření. Kritéria rovněž vyžadují zavedení opatření umožňujících zasáhnout do operace zpracování s cílem zaručit práva subjektů údajů a umožnit opravy, výmaz nebo omezení zpracování (soubor 3 kritérií).

### 2.6 Rizika pro práva a svobody

15. Podle kritérií si zpracovatel musí být vědom možných rizik pro práva a svobody fyzických osob v souvislosti se zpracováním údajů, které je cílem hodnocení. Pokud je pravděpodobné, že zpracování osobních údajů povede k vysokému riziku pro práva a svobody fyzických osob, několik kritérií zajišťuje, že žadatel musí prokázat splnění požadavků stanovených v článku 35 obecného nařízení o ochraně osobních údajů (oddíl 1.2.2 kritérií, požadavek č. 6 a oddíly 1.3.2, 1.3.3, 2.1.5.1 a 2.1.5.9 kritérií).

### 2.7 Technická a organizační opatření zaručující ochranu

16. Podle kritérií musí být uplatněna technická a organizační opatření zajišťující důvěrnost, integritu a dostupnost operací zpracování. Kritéria rovněž vyžadují uplatnění technických opatření k provedení

záměrné a standardní ochrany osobních údajů v souladu s články 25 a 32 obecného nařízení o ochraně osobních údajů (oddíly 1.5 a 2.1 kritérií / další dokumenty).

17. Podle kritérií musí být uplatněna opatření k zajištění toho, aby byla včas a v řádném rozsahu splněna povinnost ohlásit porušení zabezpečení osobních údajů v souladu s článkem 33 obecného nařízení o ochraně osobních údajů (oddíl 1.2.2 kritérií, požadavek č. 6).

### 2.8 Kritéria pro účely prokázání existence vhodných záruk pro předávání osobních údajů

18. Podle kritérií musí být identifikována všechna předání osobních údajů do třetích zemí a mezinárodním organizacím zainteresovaným na daném cíli hodnocení a zdůvodněno, proč byl zvolen daný mechanismus pro předávání údajů s ohledem na vhodné záruky podle kapitoly V obecného nařízení o ochraně osobních údajů (oddíl 1.4 kritérií).

## 3. DALŠÍ KRITÉRIA PRO EVROPSKOU PEČEŤ OCHRANY ÚDAJŮ

19. Podle pokynů musí být součástí posouzení i otázka, „zda lze na základě kritérií zohlednit právní předpisy nebo scénáře v oblasti ochrany osobních údajů v členských státech“. Oddíl 4 kritérií vyžaduje, aby žadatel dodržoval platné vnitrostátní a příslušné odvětvové právní předpisy o ochraně osobních údajů. EDPB má navíc za to, že „zprávu o dodržování vnitrostátních právních předpisů“, která posuzuje zejména to, jak cíl hodnocení splňuje platné požadavky vnitrostátních právních předpisů o ochraně údajů, vypracují právníci za předpokladu, že prokázali nezbytnou úroveň odborných znalostí, pokud jde o platné vnitrostátní právní předpisy.

## ZÁVĚRY/DOPORUČENÍ

20. EDPB dospěl k závěru, že návrh kritérií pro vydávání osvědčení je v souladu s obecným nařízením o ochraně osobních údajů, a v rámci svého úkolu stanoveného v čl. 70 odst. 1 písm. o) obecného nařízení o ochraně osobních údajů je schvaluje, což vede k vydávání společných osvědčení (evropské pečeti ochrany údajů).
21. EDPB zaregistruje mechanismus pro vydávání osvědčení s názvem „katalog kritérií EuroPrise pro vydávání osvědčení vztahujících se na operace zpracování prováděné zpracovateli“ ve veřejném registru mechanismů pro vydávání osvědčení a pečeti a známek dokládajících ochranu osobních údajů podle čl. 42 odst. 8.

## ZÁVĚREČNÉ PŘIPOMÍNKY

22. Toto stanovisko je určeno německému dozorovému úřadu v Severním Porýní-Vestfálsku a bude zveřejněno podle čl. 64 odst. 5 písm. b) obecného nařízení o ochraně osobních údajů.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně  
Anu Talus