Stanovisko 28/2022 ke kritériím vydávání osvědčení Europrivacy, pokud jde o jejich schválení sborem jako evropské pečeti ochrany údajů podle čl. 42 odst. 5 (obecného nařízení o ochraně osobních údajů)

Přijato dne 10. října 2022

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[1],

s ohledem na články 10 a 22 svého jednacího řádu,

(1) Členské státy, dozorové úřady, Evropský sbor pro ochranu osobních údajů (dále jen „sbor“) a Evropská komise podpoří zejména na úrovni Unie zavedení mechanismů pro vydávání osvědčení o ochraně údajů (dále jen „mechanismy pro vydávání osvědčení“) a pečetí a značek dokládajících ochranu údajů za účelem prokázání souladu operací zpracování správci a zpracovateli s obecným nařízením o ochraně osobních údajů s přihlédnutím ke zvláštním potřebám mikropodniků a malých a středních podniků.[2] Zavedení mechanismů pro vydávání osvědčení může nadto zvýšit transparentnost a umožnit subjektům údajů posoudit úroveň ochrany údajů v případě příslušných výrobků a služeb.[3]

(2) Kritéria vydávání osvědčení tvoří nedílnou součást 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 sbor (čl. 42 odst. 5 a čl. 70 odst. 1 písm. o) obecného nařízení o ochraně osobních údajů).

(3) Pokud dozorový úřad (dále jen „DÚ“) hodlá navrhnout schválení evropské pečeti ochrany údajů ze strany sboru podle čl. 42 odst. 5 obecného nařízení o ochraně osobních údajů, měl by DÚ uvést záměr vlastníka systému nabízet mechanismus pro vydávání osvědčení ve všech členských státech. V tomto případě je hlavní úlohou sboru 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 vydávání osvědčení sbor.

(4) Cílem tohoto stanoviska je zajistit důsledné uplatňování obecného nařízení o ochraně osobních údajů, a to i ze strany příslušných DÚ, správců a zpracovatelů s ohledem na základní prvky, které musí mechanismy pro vydávání osvědčení rozpracovávat. Posouzení ze strany sboru 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“), u něhož dne 26. května 2021 skončilo období veřejné konzultace.

(5) V souladu s tím sbor bere na vědomí, že každý mechanismus pro vydávání osvědčení by měl být řešen individuálně a že jím není dotčeno posouzení jakéhokoli jiného mechanismu pro vydávání osvědčení.

[1] Pokud se v tomto stanovisku hovoří o „členských státech“, rozumějí se tím „členské státy EHP“.
[2] Čl. 42 odst. 1 obecného nařízení o ochraně osobních údajů.
[3] 100. bod odůvodnění obecného nařízení o ochraně osobních údajů.

(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 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.

(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) Sbor 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) Sbor 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 sbor zabývá otázkami, jako jsou rozsah kritérií a jejich použitelnost a význam ve všech členských státech.

(12) Toto stanovisko se zaměřuje na kritéria pro vydávání osvědčení. Požaduje-li sbor informace na vysoké úrovni o metodách hodnocení s cílem důkladně posoudit přezkoumatelnost kritérií v souvislosti se svým stanoviskem, neznamená, že je toto stanovisko zároveň i schválením těchto metod hodnocení.

(13) Stanovisko sboru bude podle čl. 64 odst. 3 obecného nařízení o ochraně osobních údajů ve spojení s čl. 10 odst. 2 jednacího řádu sboru přijato do osmi týdnů od prvního pracovního dne poté, co předseda a příslušný dozorový úřad rozhodnou, že předložený spis je úplný. Z rozhodnutí předsedy může být tato lhůta s přihlédnutím k náročnosti dané věci prodloužena o dalších šest týdnů. Dospěje-li sbor ve svém stanovisku k závěru, že kritéria nelze v daném okamžiku schválit, může je DÚ znovu předložit ke schválení, jakmile se vypořádá s námitkami vyjádřenými v původním stanovisku sboru.

PŘIJAL TOTO STANOVISKO:

SHRNUTÍ SKUTEČNOSTÍ

1. V souladu s čl. 42 odst. 5 nařízení a pokynů vypracovalo Evropské středisko pro vydávání osvědčení a ochranu soukromí (dále jen „vlastník systému“) návrh kritérií Europrivacy v.60 (dále jen „návrh kritérií pro vydávání osvědčení“, „kritéria pro vydávání osvědčení“ nebo „kritéria“).

2. Lucemburský dozorový úřad (dále jen „lucemburský DÚ“) předložil dne 28. září 2022 sboru ke schválení kritéria pro vydávání osvědčení podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů. Rozhodnutí o úplnosti spisu bylo přijato dne 28. září 2022.

3. Mechanismus pro vydávání osvědčení Europrivacy není certifikací podle čl. 46 odst. 2 písm. f) obecného nařízení o ochraně osobních údajů určenou pro mezinárodní předávání osobních údajů, a

proto neskýtá 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. Sbor 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.

5. Sbor poznamenává, že prováděcí pokyny a navrhované způsoby ověřování mechanismu pro vydávání osvědčení poskytnuté vlastníkem systému nejsou v celém spektru kritérií zcela jednotné. Například v oddílu T.2.3.2 se vyžaduje, aby byla zavedena pravidla, zásady, postupy nebo mechanismy pro odhalování a hlášení narušení (např. systém detekce narušení, který kontroluje provoz sítě kvůli podezřelým aktivitám a upozorňuje na případy, kdy je taková aktivita zjištěna), zatímco v rámci navrhovaných způsobů ověření se mluví o kontrole a penetračním testu (podle požadavků v oddíle T.2.3.1). Ačkoli tyto nesrovnalosti nespadají do oblasti jeho posuzování, sbor podotýká, že pokud je vlastník systému neodstraní, mohou se stát překážkou akreditace subjektu pro vydávání osvědčení.

2.1 Rozsah mechanismu pro vydávání osvědčení a cíl hodnocení

6. Mechanismus pro vydávání osvědčení Europrivacy je obecným systémem, protože se zaměřuje na širokou škálu různých operací zpracování prováděných správci a zpracovateli působícími v různých odvětvích činností. Hlavní kritéria tohoto mechanismu pro vydávání osvědčení tvoří „základní kritéria“ a „kontroly technických a organizačních opatření“ týkající se technologických a organizačních opatření zavedených k zabezpečení zpracovávaných osobních údajů. Soubor kritérií pro „kontroly technických a organizačních opatření“ se použije pouze v případě, že cíl hodnocení zpracovává zvláštní kategorie údajů, údaje související s trestnými činy nebo osobní údaje dítěte.

7. Kromě toho tato kritéria zahrnují také „doplňkové kontextové kontroly“, jejichž cílem je zajistit, aby zpracování údajů v rámci cíle hodnocení bylo v souladu s požadavky specifickými pro danou oblast a technologii. Informativní matice poskytnutá vlastníkem systému popisuje, na které kategorie operací zpracování údajů se vztahují jednotlivé sady kritérií „doplňkových kontextuálních kontrol“.

8. Sbor vítá obecné systémy, které obsahují specifická kritéria, díky čemuž jsou odstupňovatelné a použitelné pro konkrétní operace zpracování nebo odvětví činnosti. Sbor si však rovněž přeje objasnit, že v souvislosti s obecným systémem se nevyžaduje úplnost kritérií týkajících se konkrétních operací zpracování, a tato úplnost tedy nebyla v rámci tohoto stanoviska posuzována. Kromě toho sbor připomíná, že pokud zveřejní dokumenty týkající se konkrétních činností zpracování, vlastník systému a akreditované certifikační orgány musí tyto dokumenty zohlednit.

9. Kritéria použitelná při stanovení cíle jsou definována v požadavcích uvedených v bodu A.2.1.1. Konkrétní pravidla použitelná v případě procesu, který musí žadatel a subjekt pro vydávání osvědčení dodržet při definování cíle hodnocení, jsou uvedena v systému Europrivacy (10.2 - Činnosti před vydáním osvědčení).

10. Sbor v dokumentaci týkající se rozsahu mechanismu pro vydávání osvědčení, kterou poskytl lucemburský DÚ, uvádí, že systém Europrivacy se vztahuje na správce a zpracovatele usazené v Evropské unii (EU) nebo v Evropském hospodářském prostoru (EHP). Použitelnost kritérií je definována v závislosti na roli a odpovědnosti žadatele.

11. Sbor bere na vědomí, že správce údajů může procesu pro vydávání osvědčení podle Europrivacy podrobit cíl hodnocení, který podléhá společné správě (kritéria podle bodu A.2.7.1). V případech, kdy cíl hodnocení podléhá společné správě, sbor zdůrazňuje, že akreditovaný 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 obecného nařízení o ochraně osobních údajů, které má mechanismus pro vydávání osvědčení prokázat. V důsledku toho by ujednání uzavřené mezi žadatelem a ostatními společnými správci zainteresovanými na cíli hodnocení, pokud jde o jejich příslušné podíly na odpovědnosti za dodržování povinností podle obecného nařízení o ochraně osobních údajů[4], mohlo v závislosti na okolnostech činností zpracování daného cíle hodnocení zamezit žadateli ve splnění kritérií pro vydávání osvědčení.

12. Sbor bere na vědomí, že zpracování genetických údajů je z oblasti působnosti mechanismu pro vydávání osvědčení Europrivacy vyloučeno. V důsledku toho se posouzení kritérií prováděné sborem nevztahuje na vhodnost kritérií pro cíl hodnocení, u něhož by docházelo ke zpracování takových údajů.

2.2 Operace zpracování

13. Kritéria se zabývají příslušnými složkami operací zpracování (údaje, systémy a zpracování) s ohledem na obecný rozsah působnosti mechanismu pro vydávání osvědčení. Kritéria zejména umožňují určit zvláštní kategorie údajů definované v článku 9 obecného nařízení o ochraně osobních údajů (oddíl G.2 kritérií - Zpracování zvláštních kategorií osobních údajů).

2.3 Zákonnost zpracování

14. Kritéria 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 obecného nařízení o ochraně osobních údajů (oddíl G.1 kritérií - Zákonnost zpracování údajů).

2.4 Zásady zpracování údajů

15. Kritéria dostatečně zohledňují zásady ochrany údajů podle článku 5 obecného nařízení o ochraně osobních údajů. Podle kritérií je zejména nutné, aby žadatel prokázal, že dané osobní údaje jsou přiměřené, relevantní a jejich rozsah je omezen na to, co je nezbytné vzhledem k účelům, pro které jsou zpracovávány (minimalizace údajů).

2.5 Obecné povinnosti správců a zpracovatelů

16. Kritéria odrážejí povinnosti správce podle článku 24 obecného nařízení o ochraně osobních údajů (oddíl G.4 - Odpovědnost správce údajů) a vyžadují posouzení smluvních ujednání mezi zpracovatelem

[4] *Vymezení jejich podílů na odpovědnosti se musí týkat zejména výkonu práv subjektů údajů a povinností poskytovat informace. Kromě toho by rozdělení odpovědnosti mělo zahrnovat další povinnosti správce, například pokud jde o obecné zásady ochrany osobních údajů, právní základ, bezpečnostní opatření, povinnost oznámit porušení zabezpečení osobních údajů, posouzení dopadů na ochranu osobních údajů, využívání zpracovatelů, předávání osobních údajů do třetích zemí a kontakty se subjekty údajů a dozorovými úřady* (pokyny 07/2020 k pojmům správce a zpracovatele v obecném nařízení o ochraně osobních údajů)

a správcem podle článku 28 obecného nařízení o ochraně osobních údajů (oddíl G.5 kritérií - Zpracovatelé údajů nebo dílčí zpracovatelé).

17. Kritéria vyžadují, aby všichni žadatelé jmenovali pověřence pro ochranu osobních údajů (dále jen „pověřenec"), a to i v případech, kdy žadatel není povinen jmenovat tohoto pověřence podle článku 37 obecného nařízení o ochraně osobních údajů. Tato kritéria mají ověřit, zda pověřenec splňuje požadavky podle článků 37 až 39 (oddíl G.9 kritérií - Pověřenec pro ochranu osobních údajů).

18. Podle těchto kritérií se kontroluje obsah záznamů o činnostech zpracování v souladu s článkem 30 obecného nařízení o ochraně osobních údajů (oddíl G.5.3 kritérií - Záznamy o činnostech zpracování).

2.6 Práva subjektů údajů

19. 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 (oddíl G.3 kritérií - Práva subjektů údajů).

2.7 Rizika pro práva a svobody

20. Kritéria vyžadují posouzení rizika pro práva a svobody fyzických osob v souvislosti se zpracováním údajů v rámci daného cíle hodnocení v souladu s článkem 35 obecného nařízení o ochraně osobních údajů (oddíl G.8 kritérií - Posouzení vlivu na ochranu osobních údajů).

2.8 Technická a organizační opatření zaručující ochranu

21. Kritéria 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 osobních údajů v souladu s články 25 a 32 obecného nařízení o ochraně osobních údajů (oddíl G.6 kritérií - Zabezpečení zpracování a záměrná ochrana údajů, oddíl T.1/T.2 kritérií - Základní bezpečnostní požadavky/rozšířené bezpečnostní požadavky).

22. Kritéria vyžadují uplatnění opatření k zajištění toho, aby byly včas a v řádném rozsahu splněny povinnosti oznámit porušení zabezpečení osobních údajů v souladu s články 33 a 34 obecného nařízení o ochraně osobních údajů (oddíl G.7 kritérií - Řízení případů porušení zabezpečení osobních údajů).

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

23. Kritéria vyžadují identifikaci všech předání osobních údajů do třetích zemí a mezinárodním organizacím zainteresovaných na daném cíli hodnocení a zdůvodnění uskutečněné volby mechanismu pro předání údajů, který skýtá vhodné záruky podle kapitoly V obecného nařízení o ochraně osobních údajů (oddíl G.10 kritérií - Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím).

3. DALŠÍ KRITÉRIA PRO EVROPSKOU PEČEŤ OCHRANY ÚDAJŮ

24. Podle pokynů musí být součástí posouzení i otázka, „zda lze na základě kritérií zohlednit právní předpisy nebo scénáře ochrany údajů v členských státech". Oddíl G.1.1.3 kritérií vyžaduje, aby žadatel poskytl takové posouzení ve zprávě o posouzení plnění vnitrostátních povinností (NOCAR). Sbor bere na vědomí, že tato zpráva bude obsahovat posouzení vnitrostátních povinností vztahujících k danému cíli hodnocení a bude dokumentovat opatření přijatá žadatelem za účelem dosažení souladu s platnými pravidly a případně i probíhající nápravná opatření. Žadatel nebude používat seznam klíčových doplňkových vnitrostátních požadavků, který mu pro každou zemi poskytl vlastník systému,

jako vyčerpávající seznam vnitrostátních povinností relevantních pro daný cíl hodnocení. Orientační seznam minimálních požadavků na doplňkové kontroly poskytnutý vlastníkem systému nepřestavuje kritéria pro vydávání osvědčení, která by spadala do oblasti působnosti tohoto stanoviska.

ZÁVĚRY/DOPORUČENÍ

25. Na závěr sbor konstatuje, že kritéria pro vydávání osvědčení Europrivacy jsou v souladu s obecným nařízením o ochraně osobních údajů, a v rámci úkolu sboru definovaného v čl. 70 odst. 1 písm. o) obecného nařízení o ochraně osobních údajů schvaluje je, což znamená vydání společného osvědčení (evropská pečeť ochrany údajů).

26. Sbor zaregistruje mechanismus pro vydávání osvědčení Europrivacy ve veřejném registru mechanismů pro vydávání osvědčení a pečetí a značek dokládajících ochranu osobních údajů podle čl. 42 odst. 8.

ZÁVĚREČNÉ POZNÁMKY

27. Toto stanovisko je adresováno lucemburskému dozorovému úřadu a bude zpřístupněno veřejnosti podle čl. 64 odst. 5 písm. b) obecného nařízení o ochraně osobních údajů.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně