Stanovisko 28/2022 k certifikačným kritériám Europrivacy, pokiaľ ide o ich schválenie Výborom ako európskej pečate ochrany údajov podľa článku 42 ods. 5 (všeobecné nariadenie o ochrane údajov)

Prijaté 10. októbra 2022

Európsky výbor pre ochranu údajov

so zreteľom na článok 63, článok 64 ods. 2 a článok 42 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679/EÚ z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o Európskom hospodárskom priestore (ďalej len „EHP“), najmä na jej prílohu XI a protokol 37, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018[1],

so zreteľom na článok 10 a článok 22 rokovacieho poriadku,

(1) Členské štáty, dozorné orgány, Európsky výbor pre ochranu údajov (ďalej len „EDPB alebo Výbor“) a Európska komisia podporujú, najmä na úrovni Únie, vytvorenie certifikačných mechanizmov ochrany údajov (ďalej len „certifikačné mechanizmy“) a pečatí a značiek ochrany údajov na účely preukázania súladu spracovateľských operácií prevádzkovateľov a sprostredkovateľov so všeobecným nariadením o ochrane údajov, pričom sa zohľadnia osobitné potreby mikropodnikov, malých a stredných podnikov.[2] Vytvorenie mechanizmov certifikácie môže okrem toho zlepšiť transparentnosť a umožní dotknutým osobám posúdiť úroveň ochrany údajov v prípade relevantných produktov a služieb.[3]

(2) Kritériá certifikácie tvoria neoddeliteľnú súčasť certifikačného mechanizmu. V dôsledku toho sa vo všeobecnom nariadení o ochrane údajov vyžaduje, aby kritériá vnútroštátneho certifikačného mechanizmu schválil príslušný dozorný orgán [článok 42 ods. 5 a článok 43 ods. 2 písm. b) všeobecného nariadenia o ochrane údajov] alebo v prípade európskej pečate ochrany údajov EDPB [článok 42 ods. 5 a článok 70 ods. 1 písm. o) všeobecného nariadenia o ochrane údajov].

(3) Ak má dozorný orgán v úmysle navrhnúť, aby EDPB schválil európsku pečať ochrany údajov podľa článku 42 ods. 5 všeobecného nariadenia o ochrane údajov, dozorný orgán by mal uviesť zámer vlastníka schémy ponúknuť certifikačný mechanizmus vo všetkých členských štátoch. V tomto prípade je hlavnou úlohou EDPB zabezpečiť jednotné uplatňovanie všeobecného nariadenia o ochrane údajov prostredníctvom mechanizmu konzistentnosti uvedeného v článkoch 63, 64 a 65 všeobecného nariadenia o ochrane údajov. V tomto rámci EDPB podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov schvaľuje kritériá certifikácie.

(4) Cieľom tohto stanoviska je zabezpečiť konzistentné uplatňovanie všeobecného nariadenia o ochrane údajov, a to aj zo strany dozorných orgánov, prevádzkovateľov a sprostredkovateľov vzhľadom na základné prvky, ktoré musia certifikačné mechanizmy vypracovať. Posúdenie EDPB sa vykonáva najmä na základe „Usmernení č. 1/2018 týkajúcich sa certifikácie a určovania kritérií certifikácie podľa článkov 42 a 43 nariadenia 2016/679“ (ďalej len „usmernenia“) a ich dodatku, v ktorom sa stanovuje „Usmernenie k posudzovaniu kritérií certifikácie“ (ďalej len „dodatok“), v prípade ktorého lehota na verejné konzultácie uplynula 26. mája 2021.

(5) V súlade s tým EDPB uznáva, že každým certifikačný mechanizmus je potrebné sa zaoberať individuálne a nie je ním dotknuté posúdenie akéhokoľvek iného certifikačného mechanizmu.

[1] Odkazy na „členské štáty“ uvedené v tomto stanovisku sa majú chápať ako odkazy na „členské štáty EHP“.
[2] Článok 42 ods. 1 všeobecného nariadenia o ochrane údajov.
[3] Odôvodnenie 100 všeobecného nariadenia o ochrane údajov.

(6) Certifikačné mechanizmy by mali umožniť prevádzkovateľom a sprostredkovateľom preukázať súlad s všeobecným nariadením o ochrane údajov. Jeho kritériá by preto mali náležite odrážať požiadavky a zásady týkajúce sa ochrany osobných údajov stanovené vo všeobecnom nariadení o ochrane údajov a prispievať k jeho konzistentnému uplatňovaniu.

(7) Vlastník schémy by mal zároveň zabezpečiť zosúladenie a súlad certifikačného mechanizmu s akýmikoľvek zahrnutými alebo uplatnenými normami a certifikačnými postupmi ISO.

(8) V dôsledku toho by certifikácie mali pre prevádzkovateľov a sprostredkovateľov predstavovať pridanú hodnotu tým, že pomáhajú vykonávať štandardizované a špecifikované organizačné a technické opatrenia, ktoré preukázateľne uľahčujú a zlepšujú súlad spracovateľských operácií so všeobecným nariadením o ochrane údajov, pričom sa zohľadnia požiadavky špecifické pre dané odvetvie.

(9) EDPB víta úsilie vlastníkov schémy vypracovať certifikačné mechanizmy, ktoré sú praktickými a potenciálne nákladovo efektívnymi nástrojmi na zabezpečenie väčšieho súladu so všeobecným nariadením o ochrane údajov a na podporu práva na súkromie a ochranu údajov dotknutých osôb zvýšením transparentnosti.

(10) EDPB pripomína, že certifikácie sú dobrovoľné nástroje zodpovednosti a že dodržiavanie certifikačného mechanizmu neznižuje zodpovednosť prevádzkovateľov alebo sprostredkovateľov za dodržiavanie všeobecného nariadenia o ochrane údajov ani nebráni dozorným orgánom vo vykonávaní ich úloh a právomocí podľa všeobecného nariadenia o ochrane údajov a príslušných vnútroštátnych právnych predpisov.

(11) EDPB sa v tomto stanovisku zaoberá otázkami, ako je rozsah kritérií, uplatniteľnosť a relevantnosť kritérií vo všetkých členských štátoch.

(12) Toto stanovisko sa zameriava na certifikačné kritériá. V prípade, že EDPB vyžaduje informácie na vysokej úrovni o metódach hodnotenia, aby mohol dôkladne posúdiť kontrolovateľnosť kritérií v kontexte svojho stanoviska, dané stanovisko nezahŕňa žiadne schválenie takýchto metód hodnotenia.

(13) Stanovisko Výboru sa prijme podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov v spojení s článkom 10 ods. 2 rokovacieho poriadku EDPB do ôsmich týždňov od prvého pracovného dňa po tom, ako predseda a príslušné dozorné orgány rozhodnú, že spis je úplný. Na základe rozhodnutia predsedu sa toto obdobie môže predĺžiť o ďalších šesť týždňov, pričom sa zohľadní zložitosť predmetu. Ak sa v stanovisku EDPB dospeje k záveru, že kritériá nemožno schváliť, dozorný orgán môže opätovne predložiť kritériá na schválenie, keď sa vyriešia obavy vyjadrené v pôvodnom stanovisku EDPB.

PRIJAL TOTO STANOVISKO:

ZHRNUTIE SKUTOČNOSTÍ

1. V súlade s článkom 42 ods. 5 všeobecného nariadenia o ochrane údajov a usmerneniami Európske centrum pre certifikáciu a súkromie (ďalej len „vlastník schémy“) vypracovalo kritériá Europrivacy v. 60 (ďalej len „návrh certifikačných kritérií“, „certifikačné kritériá“ alebo „kritériá“).

2. Dozorný orgán Luxemburska predložil 28. septembra 2022 EDPB kritériá certifikácie Europrivacy na schválenie podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov. Rozhodnutie o úplnosti spisu bolo prijaté 28. septembra 2022.

3. Certifikačný mechanizmus Europrivacy nie je certifikáciou podľa článku 46 ods. 2 písm. f) všeobecného nariadenia o ochrane údajov určenou na medzinárodné prenosy osobných údajov, a preto

neposkytuje primerané záruky v rámci prenosu osobných údajov do tretích krajín alebo medzinárodným organizáciám za podmienok uvedených v článku 46 ods. 2 písm. f). Akýkoľvek prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa totiž uskutoční len vtedy, ak sa dodržia ustanovenia kapitoly V všeobecného nariadenia o ochrane údajov.

2 POSÚDENIE

4. EDPB vykonal posúdenie kritérií certifikácie na schválenie podľa článku 42 ods. 5 všeobecného nariadenia o ochrane údajov v súlade so štruktúrou stanovenou v prílohe 2 k usmerneniam (ďalej len „príloha“) a jej dodatku.

5. EDPB poznamenáva, že vykonávacie usmernenia a navrhované prostriedky overovania certifikačného mechanizmu, ktoré poskytol vlastník schémy, nie sú vždy konzistentné v celom katalógu kritérií. Napríklad v oddiele T.2.3.2 sa vyžaduje, aby boli zavedené pravidlá, politiky, postupy alebo mechanizmy na odhaľovanie a hlásenie narušení (napr. systém detekcie narušenia, ktorý monitoruje sieťovú prevádzku na účely podozrivej činnosti a upozorňuje v prípade zistenia takejto činnosti), zatiaľ čo navrhované prostriedky overovania sa vzťahujú na kontrolu a skúšku penetrácie (požadované v oddiele T.2.3.1). Hoci takéto nezrovnalosti nepatria do rozsahu jeho posúdenia, EDPB zdôrazňuje, že môžu byť prekážkou akreditácie certifikačného subjektu, pokiaľ ich vlastník schémy neodstráni.

2.1 Rozsah pôsobnosti certifikačného mechanizmu a cieľ hodnotenia

6. Certifikačný mechanizmus Europrivacy je všeobecný systém, keďže sa zameriava na širokú škálu rôznych spracovateľských operácií, ktoré vykonávajú prevádzkovatelia a sprostredkovatelia z rôznych odvetví činnosti. Hlavné kritériá tohto certifikačného mechanizmu pozostávajú zo „základných kritérií“ a „previerok a kontrol TOO“, ktoré sa týkajú technologických a organizačných opatrení (ďalej len „TOO“) zavedených na zabezpečenie spracúvaných osobných údajov. Súbor kritérií „previerky a kontrol TOO“ sa uplatňuje len vtedy, ak cieľ hodnotenia spracúva osobitné kategórie údajov, údaje súvisiace s trestným činom alebo osobné údaje dieťaťa.

7. Okrem toho kritériá zahŕňajú aj „doplnkové kontextové previerky a kontroly“, ktorých cieľom je zabezpečiť, aby spracúvanie údajov v rámci cieľa hodnotenia bolo v súlade s požiadavkami špecifickými pre danú oblasť a špecifickými technológiami. V informatívnej matici, ktorú poskytol vlastník schémy, sa opisuje, na ktoré kategórie spracovateľských operácií údajov sa uplatňuje každý súbor kritérií „doplnkových kontextových previerok a kontrol“.

8. EDPB víta všeobecné systémy, ktoré obsahujú osobitné kritériá, ktoré im umožňujú škálovateľnosť a uplatnenie na konkrétne spracovateľské operácie alebo odvetvie činnosti. EDPB by však chcel tiež objasniť, že v kontexte všeobecnej schémy sa úplnosť kritérií týkajúcich sa konkrétnych spracovateľských operácií nevyžaduje, a preto nebola posudzovaná v rámci tohto stanoviska. EDPB okrem toho pripomína, že ak zverejní dokumenty týkajúce sa konkrétnych spracovateľských činností, vlastník schémy a akreditované certifikačné orgány takéto dokumenty majú zohľadniť.

9. Kritériá uplatniteľné na špecifikáciu cieľa hodnotenia sú vymedzené v požiadavkách uvedených v bode A.2.1.1. Osobitné pravidlá, ktoré sa vzťahujú na postup, ktorý má žiadateľ a certifikačný orgán dodržiavať s cieľom vymedziť cieľ hodnotenia, sú špecifikované v schéme Europrivacy (10.2 – Činnosti pred certifikáciou).

10. Výbor v dokumentácii týkajúcej sa rozsahu certifikačného mechanizmu poskytnutého LU SA poznamenáva, že schéma Europrivacy sa vzťahuje na prevádzkovateľov a sprostredkovateľov usadených v Európskej únii (EÚ) alebo v Európskom hospodárskom priestore (EHP). Uplatniteľnosť kritérií je vymedzená v závislosti od úlohy a zodpovedností žiadateľa.

11. Výbor poznamenáva, že prevádzkovateľ môže predložiť v rámci procesu certifikácie Europrivacy cieľ hodnotenia, ktorý podlieha spoločným prevádzkovateľom (kritériá A.2.7.1). V prípade, že cieľ hodnotenia podlieha spoločným prevádzkovateľom, Výbor by chcel zdôrazniť, že akreditovaný certifikačný orgán bude musieť starostlivo vykonať proces podávania žiadostí, aby sa zabezpečilo, že cieľ hodnotenia je zmysluplný a že žiadateľ je plne zodpovedný za plnenie všetkých povinností podľa všeobecného nariadenia o ochrane údajov, ktoré má certifikačný mechanizmus preukázať. V dôsledku toho by dohoda uzavretá medzi žiadateľom a ostatnými spoločnými prevádzkovateľmi zapojenými do cieľa hodnotenia, pokiaľ ide o ich príslušné zodpovednosti za dodržiavanie povinností podľa všeobecného nariadenia o ochrane údajov[4], mohla – v závislosti od kontextu spracovateľských činností cieľa hodnotenia – brániť žiadateľovi v tom, aby splnil kritériá certifikácie.

12. Výbor poznamenáva, že spracúvanie údajov týkajúcich sa genetických údajov je vylúčené z rozsahu pôsobnosti certifikačného mechanizmu Europrivacy. V dôsledku toho sa posúdenie kritérií, ktoré vykonal Výbor, nevzťahuje na vhodnosť kritérií pre cieľ hodnotenia, ktoré by zahŕňali takéto spracúvanie údajov.

2.2 Spracovateľské operácie

13. Kritériá sa týkajú príslušných zložiek spracovateľských operácií (údaje, systémy a spracúvanie) so zreteľom na všeobecný rozsah pôsobnosti certifikačného mechanizmu. Kritériá umožňujú najmä identifikáciu osobitných kategórií údajov vymedzených v článku 9 všeobecného nariadenia o ochrane údajov (oddiel G.2 kritérií – Spracúvanie osobitných údajov).

2.3 Zákonnosť spracúvania

14. Kritériá si vyžadujú kontrolu zákonnosti spracúvania údajov pre každú jednotlivú spracovateľskú operáciu v rámci cieľa hodnotenia a vyžadujú si kontrolu požiadaviek právneho základu, ako sa vymedzuje v článku 6 všeobecného nariadenia o ochrane údajov (oddiel G.1 kritérií – Zákonnosť spracúvania údajov).

2.4 Zásady spracúvania údajov

15. Kritériá primerane zohľadňujú zásady ochrany údajov podľa článku 5 všeobecného nariadenia o ochrane údajov. Kritériá predovšetkým vyžadujú, aby žiadateľ preukázal, že osobné údaje sú primerané, relevantné a obmedzené na to, čo je nevyhnutné vzhľadom na účely, na ktoré sa spracúvajú (minimalizácia údajov).

[4] *Pri určovaní svojich príslušných povinností musia zohľadniť najmä uplatňovanie práv dotknutých osôb a povinnosti poskytovať informácie. Okrem toho by sa rozdeľovanie zodpovedností malo týkať aj ďalších povinností prevádzkovateľov, napríklad pokiaľ ide o všeobecné zásady ochrany údajov, právny základ, bezpečnostné opatrenia, povinnosť oznamovať porušenia ochrany údajov, posúdenia vplyvu na ochranu údajov, využívanie sprostredkovateľov, prenosy z tretích krajín a kontakty s dotknutými osobami a dozornými orgánmi* (Usmernenia EDPB 07/2020 týkajúce sa pojmov prevádzkovateľ a sprostredkovateľ vo všeobecnom nariadení o ochrane údajov).

2.5 Všeobecné povinnosti prevádzkovateľov a sprostredkovateľov

16. Kritériá odrážajú povinnosti prevádzkovateľa podľa článku 24 všeobecného nariadenia o ochrane údajov (G.4 – Zodpovednosť prevádzkovateľa) a vyžadujú si hodnotenie zmluvných dohôd medzi sprostredkovateľom a prevádzkovateľom v súlade s článkom 28 všeobecného nariadenia o ochrane údajov (oddiel G.5 kritérií – Sprostredkovatelia alebo ďalší sprostredkovatelia).

17. Na základe kritérií sa od všetkých žiadateľov vyžaduje, aby vymenovali zodpovednú osobu, a to aj v prípade, že žiadateľ nie je povinný určiť zodpovednú osobu podľa článku 37 všeobecného nariadenia o ochrane údajov. Kritériá kontrolujú, či zodpovedná osoba spĺňa požiadavky podľa článkov 37 až 39 (oddiel G.9 kritérií – zodpovedná osoba).

18. Kritériá kontrolujú obsah záznamov o spracovateľských činnostiach v súlade s článkom 30 všeobecného nariadenia o ochrane údajov (oddiel G.5.3 kritérií – Záznamy o spracovateľských činnostiach).

2.6 Práva dotknutých osôb

19. V kritériách sa primerane rieši právo dotknutej osoby na informácie v súlade s kapitolou III všeobecného nariadenia o ochrane údajov a vyžadujú si zavedenie príslušných opatrení. Kritériá si takisto vyžadujú zavedené opatrenia, ktorými sa stanovuje možnosť zasiahnuť do spracovateľskej operácie s cieľom zaručiť práva dotknutých osôb a umožniť opravy, vymazanie alebo obmedzenia (oddiel G.3 kritérií – Práva dotknutých osôb).

2.7 Riziká pre práva a slobodu

20. Kritériá si vyžadujú posúdenie rizika pre práva a slobody fyzických osôb pri spracúvaní údajov v rámci cieľa hodnotenia v súlade s článkom 35 všeobecného nariadenia o ochrane údajov (oddiel G.8 kritérií – Posúdenie vplyvu na ochranu údajov).

2.8 Technické a organizačné opatrenia zaručujúce ochranu

21. Kritériá si vyžadujú uplatňovanie technických a organizačných opatrení zabezpečujúcich dôvernosť, integritu a dostupnosť spracovateľských operácií. Kritériá si takisto vyžadujú uplatňovanie technických opatrení na vykonávanie špecificky navrhnutej a štandardnej ochrany údajov v súlade s článkom 25 a článkom 32 všeobecného nariadenia o ochrane údajov (oddiel G.6 kritérií – Bezpečnosť spracúvania a špecificky navrhnutá ochrana údajov, oddiel T.1/T.2 kritérií – Základné bezpečnostné požiadavky/Rozšírené bezpečnostné požiadavky).

22. Kritériá si vyžadujú uplatňovanie opatrenia na zabezpečenie toho, aby sa oznamovacie povinnosti v prípade porušenia ochrany osobných údajov vykonávali v primeranom čase a rozsahu v súlade s článkami 33 a 34 všeobecného nariadenia o ochrane údajov (oddiel G.7 kritérií – Správa porušení ochrany údajov).

2.9 Kritériá na účely preukázania existencie primeraných záruk v prípade prenosu osobných údajov

23. Kritériá si vyžadujú identifikáciu všetkých prenosov osobných údajov do tretích krajín a medzinárodným organizáciám zapojeným do cieľa hodnotenia a odôvodnenie výberu mechanizmu prenosu údajov poskytujúceho primerané záruky podľa kapitoly V všeobecného nariadenia o ochrane údajov (oddiel G.10 kritérií – Prenos osobných údajov do tretích krajín alebo medzinárodným organizáciám).

3. DODATOČNÉ KRITÉRIÁ EURÓPSKEJ PEČATE OCHRANY ÚDAJOV

24. Podľa usmernení posúdenie má zahŕňať otázku, „či kritériá dokážu zohľadniť právne predpisy alebo scenáre členských štátov v oblasti ochrany údajov“. V oddiele G.1.1.3 kritérií sa vyžaduje, aby žiadateľ poskytol takéto posúdenie v správe o posúdení súladu s vnútroštátnymi povinnosťami (NOCAR). Výbor poznamenáva, že takáto správa obsahuje posúdenie vnútroštátnych povinností, ktoré sa vzťahujú na cieľ hodnotenia, a zdokumentuje opatrenia, ktoré žiadateľ prijal na dosiahnutie súladu s platnými pravidlami a prípadne prebiehajúce nápravné opatrenia. Žiadateľ nesmie použiť zoznam kľúčových doplnkových vnútroštátnych požiadaviek, ktorý poskytol vlastník schémy pre každú krajinu ako vyčerpávajúci zoznam vnútroštátnych povinností relevantných pre cieľ hodnotenia. Orientačný zoznam minimálnych požiadaviek na doplnkové previerky a kontroly, ktorý poskytol vlastník schémy, nie sú kritériami certifikácie v rozsahu pôsobnosti tohto stanoviska.

ZÁVERY/ODPORÚČANIA

25. Na záver sa EDPB domnieva, že kritériá certifikácie týkajúce sa Europrivacy sú v súlade so všeobecným nariadením o ochrane údajov, a schvaľuje ich v súlade s úlohou Výboru vymedzenou v článku 70 ods. 1 písm. o) všeobecného nariadenia o ochrane údajov, ktorej výsledkom je spoločná certifikácia (európska pečať ochrany údajov).

26. EDPB zaregistruje certifikačný mechanizmus Europrivacy vo verejnom registri certifikačných mechanizmov a pečatí a značiek ochrany údajov podľa článku 42 ods. 8.

ZÁVEREČNÉ POZNÁMKY

27. Toto stanovisko je určené luxemburskému dozornému orgánu a bude zverejnené v súlade s článkom 64 ods. 5 písm. b) všeobecného nariadenia o ochrane údajov.

Za Európsky výbor pre ochranu údajov

predsedníčka