Stanovisko Výboru podľa článku 64

Stanovisko 27/2024 ku kritériám certifikácie orgánu Brand Compliance, pokiaľ ide o ich schválenie výborom vo forme európskej pečate ochrany údajov podľa článku 42 ods. 5 (všeobecné nariadenie o ochrane údajov)

Prijaté 2. decembra 2024

Translations proofread by EDPB Members.
This language version has not yet been proofread.

OBSAH

1 ZHRNUTIE SKUTOČNOSTÍ 4
2 POSÚDENIE 5
3 DODATOČNÉ KRITÉRIÁ EURÓPSKEJ PEČATE OCHRANY ÚDAJOV 7
4 ZÁVERY/ODPORÚČANIA 8
5 ZÁVEREČNÉ POZNÁMKY 8

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 certifikačných mechanizmov 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 systému 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 dozornými orgánmi, prevádzkovateľmi a sprostredkovateľmi 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“ (ďalej len „usmernenia“) a ich dodatku, v ktorom sa stanovuje „Usmernenie k posudzovaniu kritérií certifikácie“ (ďalej len „dodatok“).

[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.

(5) EDPB príslušne uznáva, že každým certifikačným mechanizmom sa treba zaoberať individuálne a nie je ním dotknuté posúdenie akéhokoľvek iného certifikačného mechanizmu.

(6) Certifikačné mechanizmy by mali umožniť prevádzkovateľom a sprostredkovateľom preukázať súlad s všeobecným nariadením o ochrane údajov. Ich 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 systému by mal zároveň zabezpečiť zosúladenie a zhodu certifikačného mechanizmu s akýmikoľvek zahrnutými alebo uplatnenými normami a certifikačnými postupmi ISO.

(8) V dôsledku toho preto certifikácie majú mať pre prevádzkovateľov a sprostredkovateľov pridanú hodnotu tým, že pomáhajú implementovať 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 systémov v záujme vypracovania certifikačných mechanizmov, 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 prostredníctvom zvýšenia 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 kritériá certifikácie. 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 EDPB 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:

1 ZHRNUTIE SKUTOČNOSTÍ

1. V súlade s článkom 42 ods. 5 všeobecného nariadenia o ochrane údajov a týmito usmerneniami certifikačný orgán Brand Compliance B.V., právny subjekt v Holandsku (ďalej len „vlastník systému“), vypracoval návrh s názvom „Normy a kritériá certifikácie všeobecného nariadenia o ochrane údajov, BC 5701:2024, verzia 0.7“ (ďalej len „návrh kritérií certifikácie“, „kritériá certifikácie“ alebo „kritériá“) a predložil ho úradu Autoriteit Persoonsgegevens (Úrad na ochranu osobných údajov), ktorý je príslušným dozorným orgánom Holandska.

2. Dozorný orgán Holandska 26. septembra 2024 predložil EDPB návrh kritérií certifikácie na schválenie podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov. Rozhodnutie o úplnosti spisu bolo prijaté 12. novembra 2024.

3. Certifikačný mechanizmus orgánu Brand Compliance nie je certifikáciou podľa článku 46 ods. 2 písm. f) všeobecného nariadenia o ochrane údajov, ktorá je určená 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 organizácie sa totiž uskutoční len vtedy, ak sa dodržia ustanovenia kapitoly V všeobecného nariadenia o ochrane údajov.

2 POSÚDENIE

4. EDPB vykonal posúdenie kritérií certifikácie, aby mohli byť schválené podľa článku 42 ods. 5 všeobecného nariadenia o ochrane údajov v súlade so štruktúrou stanovenou v prílohe 2 k usmerneniam (ďalej len „príloha“) a ich dodatku.

2.1 Rozsah pôsobnosti certifikačného mechanizmu a predmet hodnotenia

5. Certifikačný mechanizmus orgánu Brand Compliance obsahuje kritériá certifikácie na certifikáciu spracovateľských operácií, ktoré s osobnými údajmi vykonávajú prevádzkovatelia alebo sprostredkovatelia usadení v Európskej únii (EÚ) alebo v Európskom hospodárskom priestore (EHP).

6. Hlavné kritériá tohto certifikačného mechanizmu sú rozdelené do šiestich súborov požiadaviek, a to: kontext spracúvania údajov vrátane súladu s príslušnými právnymi predpismi EÚ alebo členských štátov (súbor 1), organizačné rámcové podmienky (súbor 2), základy spracovateľských činností vrátane zásad týkajúcich sa spracúvania osobných údajov (súbor 3), technická a organizačná ochrana (súbor 4), prevádzkové vykonávanie vrátane práv dotknutých osôb (súbor 5) a systém riadenia (súbor 6).

7. Žiadatelia o certifikáciu v rámci tohto systému musia byť prevádzkovateľmi alebo sprostredkovateľmi. To zahŕňa sprostredkovateľov, ktorí sú prevádzkovateľom, ako aj ďalšími sprostredkovateľmi priamo poverení spracúvaním osobných údajov v zmysle článku 4 ods. 7 všeobecného nariadenia o ochrane údajov. Spracovateľské operácie vykonané (čiastočne) v ďalšom spracúvaní budú certifikované v rámci organizačnej kapacity sprostredkovateľa.

8. Výbor poznamenáva, že certifikačný mechanizmus nemožno použiť na certifikáciu spracovateľských operácií, pri ktorých dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania podľa článku 26 ods. 1 všeobecného nariadenia o ochrane údajov (tzv. spoloční prevádzkovatelia). Certifikačný mechanizmus nemôže na certifikáciu spracovateľských operácií použiť organizácia so sídlom mimo EÚ alebo EHP. Okrem toho certifikačný mechanizmus nemožno použiť ako nástroj prenosu v zmysle článku 42 ods. 2 a článku 46 ods. 2 písm. f) všeobecného nariadenia o ochrane údajov.

2.2 Spracovateľské operácie

9. Certifikačný mechanizmus sa môže uplatniť na spracúvanie osobných údajov bez ohľadu na typ a veľkosť organizácie a bez ohľadu na povahu produktov alebo služieb, ktoré poskytuje. Rozsah

pôsobnosti certifikačného mechanizmu preto nie je obmedzený na určité typy spracovateľských operácií a umožňuje, aby prevádzkovateľ alebo sprostredkovateľ vykonal certifikáciu všetkých spracovateľských operácií. Preto je mimoriadne dôležité, aby sa dodržiavali metodické požiadavky, keďže je to jediný spôsob, ako možno zabezpečiť konzistentné uplatňovanie certifikačných kritérií a porovnateľnú úroveň testovania v rámci rôznych certifikačných postupov. Cieľom je zabezpečiť porovnateľnosť a reprodukovateľnosť vydaných certifikátov a ich výsledkov.

2.3 Zákonnosť spracúvania

10. Podľa kritérií sa má preskúmať, či sú spracovateľské operácie prevádzkovateľa v súlade s ustanoveniami článku 6 (oddiel 6.1.2 kritérií) a prípadne článku 9 [oddiel 6.1.2 písm. h) kritérií], ako aj článku 10 všeobecného nariadenia o ochrane údajov [oddiel 6.1.2 písm. i) kritérií]. Hoci je povinnosťou prevádzkovateľa dodržiavať zásady zákonnosti spracúvania, sprostredkovateľ musí stále v tejto súvislosti dodržiavať osobitné požiadavky (oddiel 6.2 kritérií). Tieto požiadavky sa týkajú najmä zabezpečenia toho, aby sa povolenie na spracúvanie údajov legitímne získalo od prevádzkovateľa a aby sprostredkovateľ podporoval prevádzkovateľa pri dodržiavaní všeobecného nariadenia o ochrane údajov vrátane zásady zákonnosti.

2.4 Zásady spracúvania údajov

11. Uvedené kritériá stanovujú osobitné požiadavky na posúdenie všetkých zásad, ktoré sa týkajú spracúvania osobných údajov v zmysle článku 5 všeobecného nariadenia o ochrane údajov (oddiel 6 kritérií). Pokiaľ ide o požiadavky na sprostredkovateľov, v tejto súvislosti sa musia posúdiť samostatné kritériá (oddiel 6.2 kritérií). Ako už bolo uvedené, od sprostredkovateľov sa v prvom rade požaduje to, aby podporovali prevádzkovateľa pri zaisťovaní súladu so zásadami.

2.5 Všeobecné povinnosti prevádzkovateľov a sprostredkovateľov

12. V kritériách je premietnutý vzťah medzi prevádzkovateľmi a sprostredkovateľmi. Kritériá najmä stanovujú, že prevádzkovatelia a sprostredkovatelia sú povinní splniť požiadavky týkajúce sa externého zabezpečovania spracovateľských činností, ktoré okrem iného zahŕňajú dodržiavanie ustanovení článku 28 ods. 3 všeobecného nariadenia o ochrane údajov (oddiel 8.5 kritérií). Pokiaľ ide o sprostredkovateľov, musia na základe poverenia prevádzkovateľa tiež splniť osobitné požiadavky na spracúvanie (oddiel 8.6 kritérií). Okrem toho sa stanovujú ďalšie požiadavky, aby sa zohľadnili okolnosti ďalšieho spracovania [oddiel 6.2 písm. e), a najmä oddiel 8.6. písm. g) kritérií].

13. Na základe kritérií sa skontroluje obsah záznamov o spracovateľských činnostiach v súlade s článkom 30 všeobecného nariadenia o ochrane údajov (oddiel 5.4 kritérií). V tejto súvislosti sa rozlišuje medzi požadovaným obsahom záznamu o spracovateľských činnostiach pre prevádzkovateľov a sprostredkovateľov v súlade s článkom 30 ods. 1 a 2 všeobecného nariadenia o ochrane údajov.

14. Podľa kritérií sa vyžaduje, aby žiadatelia vymenovali zodpovednú osobu v súlade s článkom 37 všeobecného nariadenia o ochrane údajov. Okrem toho kritériá zaisťujú splnenie požiadaviek podľa článkov 37 až 39 všeobecného nariadenia o ochrane údajov (oddiel 5.3.2 kritérií).

15. V súvislosti so zásadou zodpovednosti podľa článku 5 ods. 2 a článku 24 všeobecného nariadenia o ochrane údajov sú stanovené požiadavky na organizáciu mechanizmov pre ochranu údajov a ohlasovanie (oddiel 5.1 a 5.3 kritérií), ako aj na vykonávanie politík ochrany údajov (oddiel 5.2 kritérií).

2.6 Práva dotknutých osôb

16. Kritériá ustanovujú primerané požiadavky pre práva dotknutej osoby v súlade s kapitolou III všeobecného nariadenia o ochrane údajov. Najprv sa riešia požiadavky na poskytovanie transparentných informácií, komunikáciu a spôsoby uplatňovania práv dotknutých osôb, po ktorých nasleduje podrobné preskúmanie príslušných práv dotknutých osôb (oddiel 8.4 kritérií). Pokiaľ ide o požiadavky na sprostredkovateľov, stanovili sa osobitné ustanovenia týkajúce sa povinností poskytovať pomoc (oddiel 8.4.11 kritérií)

2.7 Riziká pre práva a slobodu

17. Podľa kritérií sa vyžaduje, aby si sprostredkovateľ uvedomoval možné riziká pre práva a slobody fyzických osôb pri spracúvaní údajov, ktoré súvisí s predmetom hodnotenia. Ak je pravdepodobné, že spracúvanie osobných údajov povedie k vysokému riziku pre práva a slobody fyzických osôb, viacerými kritériami sa zaisťuje, aby žiadateľ preukázal, že požiadavky článku 35 všeobecného nariadenia o ochrane údajov sú splnené (oddiel 7.3 kritérií). Okrem toho sa stanovujú osobitné požiadavky, aby sprostredkovateľ povinne poskytol pomoc podľa článku 35 všeobecného nariadenia o ochrane údajov.

2.8 Technické a organizačné opatrenia zaručujúce ochranu

18. Podľa kritérií sa vyžaduje, aby sa uplatňovali technické a organizačné opatrenia založené na norme bezpečnosti informácií, ktorými sa zabezpečuje dôvernosť, integrita a presnosť spracúvaných osobných údajov a odolnosť systému spracúvania. Podľa kritérií sa vyžaduje aj uplatňovanie opatrení na vykonávanie špecificky navrhnutej ochrany údajov a štandardnej ochrany údajov v súlade s článkom 25 všeobecného nariadenia o ochrane údajov (oddiel 7.4 kritérií). Týmito kritériami sa stanovujú osobitné požiadavky na prevádzkovateľov, ktoré sa týkajú posúdenia oznámenia o porušení ochrany osobných údajov dozornému orgánu a v prípade potreby oznámenia takéhoto porušenia ochrany osobných údajov dotknutej osobe v súlade s článkami 33 a 34 všeobecného nariadenia o ochrane údajov (oddiel 8.8 kritérií). V tejto súvislosti sú opísané aj osobitné povinnosti sprostredkovateľov, najmä pokiaľ ide o identifikáciu porušenia ochrany osobných údajov a komunikáciu s prevádzkovateľom (oddiely 8.8.1 a 8.8.4 kritérií).

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

19. Podľa kritérií sa vyžaduje identifikácia všetkých prenosov osobných údajov do tretích krajín a medzinárodným organizáciám zapojeným do predmetu hodnotenia a odôvodnenie výberu mechanizmu prenosu údajov poskytujúceho primerané záruky podľa kapitoly V všeobecného nariadenia o ochrane údajov (oddiel 8.7 kritérií). Kritériami sa stanovuje postup na posúdenie plánovaných prenosov, napríklad monitorovanie ich zákonnosti.

3 DODATOČNÉ KRITÉRIÁ EURÓPSKEJ PEČATE OCHRANY ÚDAJOV

20. Podľa usmernení posúdenie má zahŕňať otázku, „či kritériá dokážu zohľadniť právne predpisy alebo scenáre členských štátov v oblasti ochrany údajov“. V oddiele 4.3 kritérií sa vyžaduje, aby žiadateľ dodržiaval platné vnútroštátne a príslušné odvetvové právne predpisy o ochrane údajov. Organizácia

správne a komplexne identifikuje, analyzuje a dokumentuje príslušné zákony a iné právne predpisy členského štátu alebo odvetvia, ktoré sa vzťahujú na spracúvanie osobných údajov v rámci predmetu hodnotenia. V dokumentácii sa uvedie osoba zodpovedná za vypracovanie vnútroštátneho alebo odvetvového právneho rámca, ktorý je relevantný pre predmet hodnotenia, a jej právnu odbornosť. Výbor okrem toho chápe, že vhodnosť identifikácie a vypracovania tohto právneho rámca určuje certifikačný orgán.

4 ZÁVERY/ODPORÚČANIA

21. Na záver sa EDPB domnieva, že kritériá certifikácie týkajúce sa orgánu Brand Compliance 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).

22. EDPB zaregistruje certifikačný mechanizmus „Normy a kritériá certifikácie všeobecného nariadenia o ochrane údajov, BC 5701:2024, verzia 0.7“ vo verejnom registri certifikačných mechanizmov a pečatí a značiek ochrany údajov podľa článku 42 ods. 8.

5 ZÁVEREČNÉ POZNÁMKY

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

Za Európsky výbor pre ochranu údajov

predsedníčka
(Anu Talus)