Stanovisko sboru (podle článku 64)

Stanovisko 14/2020 k návrhu rozhodnutí příslušného dozorového úřadu Irska ohledně schválení požadavků na akreditaci subjektu pro vydávání osvědčení podle čl. 43 odst. 3 obecného nařízení o ochraně osobních údajů

Přijato dne 25. května 2020

Přijato

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na článek 63, čl. 64 odst. 1 písm. c), odst. 3 až 8 a čl. 43 odst. 3 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 EHP a zejména přílohu XI a protokol 37 k uvedené 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 ze dne 25. května 2018,

vzhledem k těmto důvodům:

1) Hlavní úlohou sboru je zajistit jednotné uplatňování nařízení 2016/679 („obecného nařízení o ochraně osobních údajů“) v celém Evropském hospodářském prostoru. V souladu s čl. 64 odst. 1 obecného nařízení o ochraně osobních údajů vydá sbor stanovisko, pokud má dozorový úřad v úmyslu schválit požadavky na akreditaci subjektů pro vydávání osvědčení podle článku 43. Cílem tohoto stanoviska je tedy zavést jednotný přístup, pokud jde o požadavky, které bude dozorový úřad pro ochranu osobních údajů nebo vnitrostátní akreditační orgán uplatňovat v případě akreditace subjektu pro vydávání osvědčení. Přestože obecné nařízení o ochraně osobních údajů přímo nestanoví jednotný soubor požadavků na akreditaci, prosazuje jejich jednotnost. Sbor se bude snažit o dosažení tohoto cíle ve svých stanoviscích zaprvé tím, že bude vybízet dozorové úřady k tomu, aby vypracovávaly své požadavky na akreditaci v souladu se strukturou uvedenou v příloze 1 pokynů sboru EDPB 4/2018 týkajících se akreditace subjektů pro vydávání osvědčení, a zadruhé jejich analýzou za použití šablony poskytnuté sborem, která umožňuje srovnávání požadavků (na základě pokynů uvedených v normě ISO 17065 a pokynů sboru týkajících se akreditace subjektů pro vydávání osvědčení).

2) S odkazem na článek 43 obecného nařízení o ochraně osobních údajů budou požadavky na akreditaci přijímat příslušné dozorové úřady. Uplatní však mechanismus jednotnosti s cílem umožnit vytvoření důvěry v mechanismy vydávání osvědčení, a to zejména stanovením vysoké náročnosti těchto požadavků.

3) Ačkoli požadavky na akreditaci podléhají mechanismu jednotnosti, neznamená to, že by tyto požadavky měly být totožné. Příslušné dozorové úřady mají určitý prostor pro uvážení s ohledem na vnitrostátní nebo regionální souvislosti a musí přihlédnout ke svým místním právním předpisům. Cílem stanoviska sboru není dosáhnout jediného souboru požadavků EU, ale spíše zamezit závažným nejednotnostem, které by mohly ovlivnit například důvěru v nezávislost nebo odbornost akreditovaných subjektů pro vydávání osvědčení.

4) Při uplatňování mechanismu jednotnosti poslouží jako vodítko „pokyny 4/2018 týkající se akreditace subjektů pro vydávání osvědčení podle článku 43 obecného nařízení o ochraně údajů (2016/679)“ (dále jen „pokyny“) a „pokyny 1/2018 týkající se vydávání osvědčení a určování kritérií pro vydávání osvědčení v souladu s články 42 a 43 nařízení 2016/679“.

[1] Pokud se v tomto stanovisku hovoří o „Unii”, rozumí se tím „EHP“.

5) Pokud členský stát stanoví, že subjekty pro vydávání osvědčení má akreditovat dozorový úřad, měl by tento dozorový úřad stanovit požadavky na akreditaci, které budou mimo jiné zahrnovat požadavky uvedené v čl. 43 odst. 2 obecného nařízení o ochraně osobních údajů. Ve srovnání s povinnostmi vztahujícími se na akreditaci subjektů pro vydávání osvědčení vnitrostátními akreditačními orgány uvádí článek 43 obecného nařízení o ochraně osobních údajů méně bližších informací o požadavcích na akreditaci v případě, že akreditaci provádí sám dozorový úřad. V zájmu přispění k harmonizovanému přístupu k akreditaci by se požadavky na akreditaci uplatňované dozorovým úřadem měly řídit normou ISO/IEC 17065 a měly by být doplněny o dodatečné požadavky, které stanoví dozorový úřad v souladu s čl. 43 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů. Sbor konstatuje, že ustanovení čl. 43 odst. 2 písm. a) až e) obecného nařízení o ochraně osobních údajů odrážejí a upřesňují požadavky normy ISO 17065, což přispěje k jednotnosti[2].

6) Stanovisko sboru musí být podle čl. 64 odst. 1 písm. c) a odst. 3 a 8 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 rozhodli, že předložená dokumentace je úplná. Z rozhodnutí předsedy může být tato lhůta s přihlédnutím k náročnosti dané věci prodloužena o dalších šest týdnů,

PŘIJAL TOTO STANOVISKO:

1 SHRNUTÍ SKUTEČNOSTÍ

1. Irský dozorový úřad předložil sboru svůj návrh požadavků na akreditaci podle čl. 43 odst. 1 písm. b). Dokumentace byla ke dni 13. února 2020 uznána za úplnou. Vnitrostátní akreditační orgán Irska (INAS) bude provádět akreditaci subjektů pro vydávání osvědčení za použití kritérií pro vydávání osvědčení podle obecného nařízení o ochraně osobních údajů. To znamená, že orgán INAB bude při akreditaci subjektů pro vydávání osvědčení používat normu ISO 17065 a dodatečné požadavky stanovené irským dozorovým úřadem, jakmile tyto budou irským dozorovým úřadem schváleny v návaznosti na stanovisko sboru k návrhu těchto požadavků.

2. V souladu s čl. 10 odst. 2 jednacího řádu sboru se předsedkyně vzhledem ke složitosti dané záležitosti rozhodla prodloužit počáteční období pro přijetí v délce osmi týdnů o dalších šest týdnů.

2 POSOUZENÍ

2.1 Obecná argumentace sboru ve vztahu k předloženému návrhu rozhodnutí

3. Účelem tohoto stanoviska je posoudit požadavky na akreditaci vypracované dozorovým úřadem, a to buď ve vztahu k normě ISO 17065, nebo kompletní soubor požadavků, s cílem umožnit vnitrostátnímu akreditačnímu orgánu nebo dozorovému úřadu podle čl. 43 odst. 1 obecného nařízení o ochraně osobních údajů provádět akreditace subjektů pro vydávání osvědčení, které jsou

[2] Pokyny 4/2018 týkající se akreditace subjektů pro vydávání osvědčení podle článku 43 obecného nařízení o ochraně osobních údajů, bod 39. K dispozici na adrese: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_cs.

odpovědné za vydávání a obnovování osvědčení v souladu s článkem 42 obecného nařízení o ochraně osobních údajů. Tím nejsou dotčeny úkoly a pravomoci příslušného dozorového úřadu. V tomto konkrétním případě sbor bere na vědomí, že se irský dozorový úřad rozhodl obrátit se v otázce vydávání akreditací na svůj vnitrostátní akreditační orgán poté, co sestavil soubor požadavků v souladu s pokyny, které by jeho vnitrostátní akreditační subjekt měl používat při vydávání akreditací.

4. Účelem tohoto posouzení dodatečných požadavků irského dozorového úřadu na akreditaci je prozkoumat oblasti, ve kterých došlo k odchylkám od pokynů a zejména od přílohy 1 pokynů (ve smyslu doplnění nebo vypuštění jednotlivých ustanovení). Stanovisko sboru se dále zaměřuje na všechny aspekty, které mohou mít dopad na jednotný přístup k akreditaci subjektů pro vydávání osvědčení.

5. Je třeba poznamenat, že cílem pokynů týkajících se akreditace subjektů pro vydávání osvědčení je pomáhat dozorovým úřadům při stanovování jejich požadavků na akreditaci. Příloha pokynů nepředstavuje požadavky na akreditaci jako takové. Požadavky na akreditaci subjektů pro vydávání osvědčení proto musí dozorový úřad definovat způsobem, který umožní jejich praktické a důsledné uplatňování, jak to vyžadují okolnosti, za kterých dozorový úřad svou činnost vykonává.

6. Sbor uznává, že vzhledem k jejich odbornosti by měla být vnitrostátním akreditačním subjektům dopřána určitá diskrece při formulaci některých zvláštních ustanovení v rámci příslušných požadavků na akreditaci. Sbor ale považuje za nutné zdůraznit, že pokud mají být stanoveny jakékoli dodatečné požadavky, měly by být formulovány tak, aby bylo možné jejich praktické a důsledné uplatňování a případně i přezkoumání.

7. Sbor bere na vědomí, že normy ISO, a zejména norma ISO 17065, podléhají právům duševního vlastnictví, a proto v tomto stanovisku nebude odkazovat přímo na text tohoto souvisejícího dokumentu. Namísto toho se sbor rozhodl, že bude na příslušných místech poukazovat na konkrétní části norem ISO, aniž by samotný text přímo reprodukoval.

8. V neposlední řadě provedl sbor své posouzení v souladu se strukturou, kterou stanoví příloha 1 pokynů (dále jen „příloha“). Pokud se toto stanovisko nevyjadřuje k některé části návrhu požadavků irského dozorového úřadu na akreditaci, znamená to, že sbor nemá připomínky a nepožaduje, aby irský dozorový úřad podnikal další kroky.

9. Toto stanovisko se nezabývá body vznesenými irským dozorovým úřadem, které nespadají do oblasti působnosti čl. 43 odst. 2 obecného nařízení o ochraně osobních údajů, jako jsou odkazy na vnitrostátní právní předpisy. Sbor nicméně poznamenává, že tyto vnitrostátní právní předpisy by měly být v příslušných případech v souladu s obecným nařízením o ochraně osobních údajů.

2.2 Hlavní body zájmu pro posouzení (čl. 43 odst. 2 obecného nařízení o ochraně osobních údajů a příloha č. 1 pokynů sboru) toho, zda požadavky na akreditaci umožňují důsledné posouzení následujících skutečností:

1) řešení všech klíčových oblastí zdůrazněných v příloze pokynů a posouzení případných odchylek od přílohy;

2) nezávislost subjektu pro vydávání osvědčení;

3) střety zájmů subjektu pro vydávání osvědčení;

4) odbornost subjektu pro vydávání osvědčení;

5) příslušné záruky, které zajistí, aby subjekt pro vydávání osvědčení řádně uplatňoval kritéria pro vydávání osvědčení podle obecného nařízení o ochraně osobních údajů;

6) postupy pro vydávání, pravidelný přezkum a odebírání osvědčení a

7) transparentní řešení stížností týkajících se porušování vydávání osvědčení.

10. S přihlédnutím k tomu, že:

a. ustanovení čl. 43 odst. 2 obecného nařízení o ochraně osobních údajů stanoví seznam oblastí akreditace, kterými se musí subjekt pro vydávání osvědčení zabývat, aby mohl být akreditován;

b. ustanovení čl. 43 odst. 3 obecného nařízení o ochraně osobních údajů stanoví, že požadavky na akreditaci subjektů pro vydávání osvědčení schvaluje příslušný dozorový úřad;

c. ustanovení čl. 57 odst. 1 písm. p) a g) obecného nařízení o ochraně osobních údajů stanoví, že příslušný dozorový úřad musí vypracovat a zveřejnit požadavky na akreditaci subjektů pro vydávání osvědčení a může sám rozhodnout o provedení akreditace subjektů pro vydávání osvědčení;

d. ustanovení čl. 64 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů stanoví, že sbor vydá stanovisko, pokud bude mít dozorový úřad v úmyslu schválit požadavky na akreditaci subjektu pro vydávání osvědčení podle čl. 43 odst. 3;

e. pokud akreditaci provádí vnitrostátní akreditační subjekt v souladu s normou ISO/IEC 17065/2012, je třeba rovněž uplatnit dodatečné požadavky stanovené příslušným dozorovým úřadem;

f. příloha 1 pokynů týkajících se akreditace k vydávání osvědčení počítá s návrhem požadavků, které vypracuje dozorový úřad pro ochranu osobních údajů a které budou použity při akreditaci subjektu pro vydávání osvědčení prováděné vnitrostátním akreditačním subjektem;

je sbor toho názoru, že:

2.2.1 VÝCHODISKA (Oddíl 0 návrhu požadavků irského dozorového úřadu na akreditaci)

11. Sbor uznává, že podmínky spolupráce, upravující vztah mezi vnitrostátním akreditačním orgánem a jeho dozorovým úřadem pro ochranu osobních údajů, nepředstavují *faktický* požadavek na akreditaci subjektů pro vydávání osvědčení. Z důvodů úplnosti a transparentnosti ale sbor zvažuje, že takové podmínky spolupráce, pokud existují, budou zveřejněny ve formě, kterou bude dozorový úřad považovat za vhodnou.

2.2.2 POJMY A DEFINICE

12. Sbor konstatuje, že odkaz na pokyny týkající se akreditace jako na „WP 261“ není aktualizován. Sbor EDPB přijal pokyny 4/2018 týkající se akreditace subjektů pro vydávání osvědčení podle článku 43 obecného nařízení o ochraně osobních údajů (2016/679). Sbor proto irský dozorový úřad vybízí, aby znění pozměnil a aby odkazoval na pokyny 4/2018.

2.2.3 OBECNÉ POZNÁMKY

13. Sbor si všímá, že v návrhu požadavků irského dozorového úřadu se opakovaně odkazuje na „příslušný dozorový úřad“. Jelikož příslušným dozorovým úřadem je v tomto případě irský dozorový úřad, vybízí sbor irský dozorový úřad, aby tyto odkazy nahradil zkratkou „DPC“ (*Data Protection Coordinator*, koordinátor ochrany údajů) nebo slovním spojením „irský dozorový úřad“, aby se předešlo nejasnostem.

14. Sbor uznává, že návrh požadavků irského dozorového úřadu obsahuje oddíl týkající se pojmů a definic. Některé pojmy však nejsou používány jednotně v celém dokumentu (např. „předmět hodnocení“ a „cíl hodnocení“). Aby se předešlo nejasnostem, vybízí sbor irský dozorový úřad, aby v návrhu požadavků používal jednotnou terminologii.

2.2.4 OBECNÉ POŽADAVKY NA AKREDITACI (Oddíl 4 návrhu požadavků na akreditaci)

15. Pokud jde o sedmou větu v pododdílu 4.1.2 návrhu požadavků irského dozorového úřadu na akreditaci, sbor má za to, že formulace je poněkud nejasná s ohledem na to, komu se předkládají důvody pro schválení vydání osvědčení. Kromě toho je také nejasný odkaz na „usnadnění fungování“ registru. Proto sbor irský dozorový úřad vybízí, aby tuto formulaci přepracovat tak, aby byla jasnější.

2.2.5 POŽADAVKY NA ZDROJE (Oddíl 5 návrhu požadavků na akreditaci)

16. Sbor konstatuje, že návrh požadavků irského dozorového úřadu na akreditaci odkazuje na jmenování „osoby s odpovídající profesní zkušeností a s odpovědností za dohled nad dodržováním ochrany údajů a za správu a řízení informací“. Odkaz na odpovídající profesní zkušenost by měl být objasněn, pokud jde o zkušenosti a oblast působnosti. Kromě toho se zdá, že úkoly této osoby jsou podobné úkolům pověřence pro ochranu osobních údajů. Sbor vybízí irský dozorový úřad, aby jasně stanovil úkoly této osoby a upřesnil relevantní zkušenosti.

2.2.6 POŽADAVKY NA ZDROJE (Oddíl 6 návrhu požadavků na akreditaci)

17. Pokud jde o pracovníky subjektu pro vydávání osvědčení (pododdíl 6.1), sbor konstatuje, že mezi požadavky na pracovníky s technickými odbornými znalostmi, kteří budou zodpovědní za přijímání rozhodnutí, patří alespoň pětiletá odborná praxe věcně související s vydáváním osvědčení, zatímco pracovníci odpovědní za hodnocení by měli mít alespoň dvouletou odbornou praxi. Obdobně musejí mít pracovníci s odbornými znalostmi v oboru práva, kteří přijímají rozhodnutí, alespoň pětiletou praxi, zatímco pracovníci pověření hodnocením musejí mít alespoň dvouletou praxi. Sbor konstatuje, že se významně liší minimální délka odborné praxe pro pracovníky pověřené rozhodováním a pro pracovníky pověřené hodnocením. V této souvislosti se sbor domnívá, že důraz je třeba klást na různé druhy odborných znalostí, nikoliv na délku odborné praxe. Sbor zastává názor, že hodnotitelé by měli mít specializovanější odborné znalosti a odbornou praxi v oblasti technických postupů (např. audity a osvědčení), zatímco osoby přijímající rozhodnutí by měly mít obecnější a komplexnější odborné znalosti a odbornou praxi v oblasti ochrany údajů. Sbor v tomto ohledu irský dozorový úřad vybízí, aby kladl větší důraz na různé odborné znalosti a/nebo na praxi hodnotitelů a osob přijímajících rozhodnutí a aby omezil odchylky v požadované délce odborné praxe mezi těmito pracovními místy.

2.2.7 PROCESNÍ POŽADAVKY (Oddíl 7 návrhu požadavků na akreditaci)

18. S ohledem na pododdíl 7.10 návrhu požadavků irského dozorového úřadu na akreditaci („Změny s dopadem na vydávání osvědčení“) sbor konstatuje, že se nikde neodkazuje na procesy změny, které je třeba schválit, jak stanoví oddíl 7.10 přílohy. Sbor vybízí irský dozorový úřad, aby doplnil takovýto odkaz a zmínku ohledně některých z těchto postupů, jež je možné zavést (např. přechodná období, proces schvalování s příslušnými dozorovými úřady...). Kromě toho se sbor domnívá, že změny špičkových technologií jsou rovněž relevantní a mohou mít dopad na vydávání osvědčení. Proto sbor vybízí irský dozorový úřad, aby tuto možnost doplnil do seznamu změn s dopadem na vydávání osvědčení. V neposlední řadě sbor vítá skutečnost, že do seznamu změn, které mohou mít dopad na vydávání osvědčení, byla zařazena porušení zabezpečení osobních údajů a porušení obecného nařízení o ochraně osobních údajů. Aby však byla zajištěna jednoznačnost, vybízí sbor irský dozorový úřad, aby upřesnil, že je třeba zohlednit porušení zabezpečení údajů nebo porušení obecného nařízení o ochraně osobních údajů v rozsahu, v jakém se týkají vydávání osvědčení.

19. Pokud jde o změny s dopadem na vydávání osvědčení (pododdíl 7.10 návrhu požadavků irského dozorového úřadu), a zejména pátou odrážku, sbor konstatuje, že irský dozorový úřad odkazuje na „použitelná závazná rozhodnutí Evropského sboru pro ochranu osobních údajů“ a také na článek 39 jednacího řádu sboru EDPB, což zahrnuje „všechny konečné verze dokumentů přijatých sborem EDPB“. S cílem zajistit naprostou jednoznačnost toho, co se rozumí „rozhodnutím Evropského sboru pro ochranu osobních údajů“, sbor vyzývá irský dozorový úřad, aby vysvětlil obsah tohoto pojmu. Příkladem lze uvést formulaci „dokumenty přijaté Evropským sborem pro ochranu osobních údajů“.

20. Sbor konstatuje, že pododdíl 7.11 návrhu požadavků irského dozorového úřadu (skončení platnosti, omezení, pozastavení nebo odebrání osvědčení) neobsahuje povinnost subjektu pro vydávání osvědčení přijmout rozhodnutí a příkazy vydané irským dozorovým úřadem odebrat nebo odmítnout vydat žadateli osvědčení v případě, že již nejsou splněny požadavky na vydání osvědčení. Sbor proto irskému dozorovému úřadu doporučuje, aby tuto povinnost začlenil.

3 ZÁVĚRY/DOPORUČENÍ

21. Návrh požadavků irského dozorového úřadu na akreditaci může vést k nejednotnému uplatňování akreditace subjektů pro vydávání osvědčení a je třeba provést následující změny:

22. Pokud jde o „procesní požadavky“, sbor doporučuje, aby irský dozorový úřad:

1) do pododdílu 7.11 doplnil povinnost subjektu pro vydávání osvědčení přijmout rozhodnutí a příkazy vydané irským dozorovým úřadem odebrat nebo odmítnout vydat žadateli osvědčení v případě, že již nejsou splněny požadavky na vydání osvědčení.

4 ZÁVĚREČNÉ POZNÁMKY

23. Toto stanovisko je určeno irskému dozorovému úřadu a bude zveřejněno podle čl. 64 odst. 5 písm. b) obecného nařízení o ochraně osobních údajů.

24. Podle čl. 64 odst. 7 a 8 obecného nařízení o ochraně osobních údajů sdělí irský dozorový úřad předsedkyni elektronickou cestou do dvou týdnů od obdržení stanoviska, zda svůj návrh seznamu změní nebo zachová. Ve stejné lhůtě předloží pozměněný návrh seznamu, nebo pokud nemá v úmyslu řídit se stanoviskem sboru, uvede pádné důvody, proč nemá v úmyslu se tímto stanoviskem zcela nebo zčásti řídit.

25. Irský dozorový úřad sdělí sboru konečné rozhodnutí pro zařazení do registru rozhodnutí, na která se vztahuje mechanismus jednotnosti, v souladu s čl. 70 odst. 1 písm. y) obecného nařízení o ochraně osobních údajů.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)