DVA ROKY NOVÉ EVROPSKÉ OCHRANY OSOBNÍCH ÚDAJŮ

Sandra Brožová

Shrnutí

Příspěvek obsahuje informace o zásadních změnách, které přineslo obecné nařízení o ochraně osobních údajů (GDPR) a analyzuje naplnění očekávání, která byla spojena s deklarovanou vyšší komplexností a efektivitou regulace. Dále jsou v článku zmíněny nejvýznamnější dopady legislativních změn do podnikové praxe v oblasti zajištění compliance. Ačkoli některá dílčí očekávání související s harmonizačními ambicemi unijní legislativy nebyla dosud prakticky realizována, lze říci, že zákonná odpovědnost správců osobních údajů za případná zneužití při zpracování externími subjekty má velký potenciál přispět skutečně k lepšímu zajištění prevence a kontroly před zneužíváním osobních dat.

Klíčová slova: GDPR, ochrana osobních údajů, odpovědnost správce, compliance

Key words: GDPR, personal data protection, liability of the controller, compliance

Úvod – legislativní a institucionální kontext ochrany osobních údajů

GDPR je již více než dva roky zavedenou zkratkou pro obecné nařízení o ochraně osobních údajů (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, v textu dále jako „nařízení GDPR"). V českém právním řádu ho s účinností od loňského dubna doprovází adaptační zákon č. 110/2019 Sb., o zpracování osobních údajů. Ochrana osobních údajů slouží podle tohoto zákona k naplnění práva každé osoby na ochranu jejího soukromí.

V současné době dynamického rozvoje elektronického obchodu, služeb infomační společnosti a souvisejícími výzvami z hlediska zajištění bezpečnosti informací v digitálním prostoru se ochrana osobních údajů jeví jako velmi recentní fenomén. Základy mezinárodní harmonizace v této oblasti však Evropa položila již před téměř 40 lety, a to na půdě Rady Evropy, kde byla 28. ledna 1981 podepsána Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat. Ta je v současnosti ratifikována 47 členskými státy Rady Evropy včetně ČR a 28. leden se stal připomínaným významným dnem ochrany osobních údajů. Už tato úmluva vyjádřila základní zásady, na kterých stojí ochrana osobních údajů dodnes. Stanovila, že zpracování údajů musí být přiměřené ve vztahu ke sledovanému oprávněnému účelu a ve všech fázích zpracování musí odrážet vyváženost mezi všemi

dotčenými zájmy. Zpracování musí být tedy především přiměřené, účelné a nesmí přesahovat potřebné účely.

Na půdě Evropské unie byla v 90. letech přijata směrnice, nahrazená současným nařízením. Z hlediska vnitrostátního provádění unijního práva, které je povinností členských států, je zajímavá vazba unijního nařízení jakožto přímo použitelného a bezprostředně závazného předpisu, a českého adaptačního zákona. Je ustáleným pravidlem, že nařízení na rozdíl od směrnic žádné vnitrostátní prováděcí předpisy nepotřebují a je to dokonce kontraproduktivní kvůli riziku rozmělnění jednotnosti unijní úpravy při jejím provádění ve členských státech. Evropský soudní dvůr se takto vyjádřil v dnes již klasickém rozsudku ve věci *Variola* v roce 1973.

S tím, jak jsou postupně rozšiřovány výlučné pravomoci EU a je přijímáno více přímo použitelných nařízení na úkor směrnic, vzrůstá i technokratický charakter a komplexnost unijní úpravy. Pro řádné provádění ve vnitrostátním právním řádu je proto zapotřebí i speciální adaptační předpis, který není primárně zaměřen na transpozici jako u směrnic, tj. na zakotvení nových povinností pro vnitrostátní subjekty. Ty přináší samotné přímo použitelné nařízení. Zákon slouží k adaptaci unijních pravidel do českého právního řádu, tj. zejména k vybudování institucionální struktury a k stanovení pravidel ochrany osobních údajů v rámci české veřejné správy. Navazuje v mnohém na předchozí legislativní rámec v již zrušeném zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, tj. nadále u nás funguje Úřad pro ochranu osobních údajů.

Úřad pro ochranu osobních údajů má některé významné kompetence: je připomínkovým místem v legislativním procesu, a tak je oprávněn se vyjadřovat ke všem předkládaným návrhům zákonů z hlediska ochrany osobních údajů. V neposlední řadě je nadán pravomocí rozhodovat o pokutách za přestupky fyzických nebo právnických osob, podle § 61 – 65 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Sankce jsou předvídány jako potenciálně velmi vysoké, a to až do 10 000 000 Kč pro právnickou osobu nebo do 5 000 000 Kč pro fyzickou osobu, jde-li o přestupek spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem. Dosud však byly uložené pokuty spíše relativně nízké. Např. na jaře 2019 rozhodl Úřad pro ochranu osobních údajů ve věci č.j. UOOU-10138/18-8 o pokutě ve výši 250 000 Kč pro úvěrovou společnost, která porušila zásadu „minimalizace údajů." To znamená, že o svých klientech uchovávala více údajů, než bylo pro splnění účelu bezpodmínečně nutné. Šlo o uzavírání úvěrových smluv elektronicky prostřednictvím biometrického podpisu, kde byly archivovány i takové detaily, jako rychlost a tlak pohybu pera při podpisu, za účelem jednoznačné identifikace osob. Úřad zjistil, že to šlo zajistit i jiným způsobem (postačí naskenovaný podpis). Biometrický podpis klienta tedy nebyl pro účely uzavření a uchování smluvní dokumentace shledán za nezbytný, a to mj. z důvodu, že v případě uzavírání smluv v listinné podobě není zapotřebí. Úvěrová společnost v daném případě porušila více povinností, když ještě navíc uchovávala záznamy veškerých telefonních hovorů s klienty po celou dobu trvání smluvního vztahu a ještě po dobu dalších 10 let po řádném splacení všech úvěrů. Tím došlo k zásahu do principu „omezení uložení," protože doba uložení byla delší, než je nezbytné pro účely zpracování.

Pokuty, které zákon předvídá, se na své horní hranici zdají dost vysoké, čímž naplňují svou preventivní funkci a demotivují subjekty od případného protizákonného jednání, ale na druhou stranu, skutečně uložené pokuty jsou přiměřenou sankcí a nejsou pro porušitele a jejich podnikání nijak likvidační.

Hlavní změny v nové evropské ochraně osobních údajů

Co přinesla nová právní úprava v nařízení GDPR? Obecně lze říci, že základní parametry právní úpravy ochrany osobních údajů zůstaly zachovány, došlo ke zpřesnění a zpřísnění některých dílčích aspektů. Nadále platí, že osobním údajem je jakákoli informace o identifikované nebo identifikovatelné fyzické osobě, která je tzv. subjektem údajů. Jako zpracování chápeme veškeré operace nebo soubor operací s osobními údaji, ať už za pomoci automatizovaných postupů nebo i bez nich. Tyto definice nalezneme v článku 4 nařízení GDPR a obdobně v § 3 českého zákona č. 110/2019 Sb., o zpracování osobních údajů.

Klíčovým ustanovením nařízení GDPR je bezesporu článek 24, který zakotvuje odpovědnost správce osobních údajů za to, že jejich zpracování probíhá v souladu s pravidly nařízení GDPR. Tato odpovědnost je chápána široce a zahrnuje i sféru smluvních vztahů s třetími stranami, které pro správce zajišťují dílčí činnosti v procesu správy osobních údajů (tzv. zpracovatelé). Právním titulem pro zpracování osobních údajů musí být písemná smlouva podle článku 28 odst. 9 nařízení GDPR.

Jak dále vyplývá z článku 28 nařízení GDPR, je tedy nezbytné nejen na počátku nastavit a ověřit řádný soulad s požadavky nařízení, ale také zavést takové kontrolní procesy, které umožní mapovat zajišťování souladu u externích zpracovatelů průběžně. Správce musí být schopen takový soulad kdykoli doložit. Ochrana osobních údajů jako jeden z nejdůležitějších aspektů proto vstupuje do tvorby interních compliance systémů již od počáteční fáze jejich tvorby. (Nonneman, 2018). Je k tomu zapotřebí komplexně prověřit bezpečnostní hledisko spolupráce s konkrétními externími subjekty (Galdies, 2019). Většina incidentů spojená s úniky dat totiž vzniká právě tam, kde dochází k předávání dat třetím stranám. (Goldman, 2019). Mezi nejdůležitější prvky analýzy rizik smluvních vztahů s třetími subjekty patří posouzení metod předávání dat zpracovatelům, způsob přístupu třetích stran k interním podnikovým systémům nebo míra závislosti správce na službách daného zpracovatele. (Andreisová, 2020, s. 4)

Na první pohled viditelnou změnou je povinnost jmenovat osobu pověřence pro ochranu osobních údajů v případech stanovených článkem 37 nařízení GDPR. Činnost pověřence může vykonávat jak interní zaměstnanec podnikatele nebo instituce v pozici správce osobních údajů, tak externí expert nebo advokátní kancelář. Opomenutí jmenovat pověřence zakládá přestupkovou odpovědnost podle § 63 odst. 1 písm. t) zákona o zpracování osobních údajů.

Největší očekávání a jejich naplnění

A jaká byla očekávání spojená s novou právní úpravou? S osobou pověřence jsou spojena legitimní očekávání větší profesionality a systematického přístupu. Institut pověřence pro ochranu osobních údajů, resp. povinnost jej jmenovat všude tam, kde se osobní data zpracovávají v situacích podle článku 37 odst. 1 nařízení GDPR, je významnou novinkou zavedenou novou úpravou.

Článek 37 nařízení GDPR uvádí, že pověřenec má být „jmenován na základě svých profesních kvalit," výslovně jsou zdůrazněny odborné znalosti právní úpravy ochrany osobních údajů, znalosti praxe v této oblasti a kompetence k plnění stanovených úkolů. Svého pověřence musí mít nejen podnikatelé a poskytovatelé služeb, ale i různé veřejné instituce, např. školy. Podniková praxe v ČR ukazuje, že nejčastěji vykonávají funkci

pověřence na smluvním základě advokátní kanceláře, příp. interní právníci. Nepřekvapí, že sofistikovaná a pro laika obtížně srozumitelná právní úprava v nařízení GDPR si vyžádala zapojení právníků na pozicích pověřenců.

Na trhu consultingových služeb fungují i experti, kteří nutně nemají právní vzdělání, ale profilují se přímo na oblast ochrany dat. Pokud však poskytují své služby pro více zpracovatelů současně, je otázkou, zda nehrozí riziko střetu zájmů a nežádoucího překrývání agend a dodavatelských řetězců. Zejména v případě advokátů někdy jejich jméno uvedené na webových stránkách společnosti funguje jen jako splnění formální povinnosti a jejich služby jsou poskytovány v nevelkém rozsahu, pouze ve formě jednorázových konzultací problému dle potřeby. Takové omezené naplnění funkce pověřence jistě není možné považovat za splnění předvídaných očekávání. Advokátní kanceláře jsou připraveny zaštítit funkce pověřenců pro různé podnikatele napříč sektory. Ačkoli orientace v právní úpravě založené nařízením GDPR včetně souvisejícího legislativního kontextu je nezbytná, je vhodné funkci pověřence svěřit spíše osobám s praktickou znalostí dotčeného odvětví a jeho podnikatelských specifik. U nich je totiž zřetelnější vhled do vnitropodnikových procesů a tedy potenciál ovlivnit ty jejich aspekty, které se dotýkají osobních údajů, ale kromě čistě právní analýzy vyžadují i znalost věcnou. Zpracování osobních dat klientů má přesah do řízení marketingových aktivit, údaje zaměstnanců se zpracovávají v rámci agend personalistiky a celá agenda vyžaduje fundované kompetence v digitálních technologiích a jejich zabezpečení.

Kromě toho, zatímco již zrušená směrnice č. 95/46/ES byla nástrojem harmonizace národních úprav, nařízení přináší unifikaci a přímo aplikovatelná pravidla. Tento jednoznačný efekt je ovšem rozmělněn skutečností, že adaptace některých ustanovení nařízení GDPR si stejně vyžádala přijetí prováděcích vnitrostátních zákonů, které nemohou být z povahy věci shodné. Přímo k tomu vybízí i ustanovení nařízení GDPR, ponechávající členským státům prostor pro uvážení a výběr z alternativ, jako např. stanovení minimálního věku dítěte v souvislosti s přímou nabídkou služeb informační společnosti v rozmezí 13 až 16 let podle článku 8 nařízení GDPR. Např. podle § 7 zákona č. 110/2019 Sb., o zpracování osobních údajů, v ČR nabývá dítě způsobilosti k udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo jemu dovršením patnáctého roku věku. Právě tato variantní ustanovení jsou důvodem, proč je z hlediska legislativní techniky nutné přijmout vnitrostátní adaptační zákon i pro bezprostředně závazné unijní nařízení. Je zřejmé, že poskytovatelé těchto služeb na vnitřním trhu EU budou muset zohlednit různé věkové hranice zvolené v jednotlivých členských státech, což si vyžádá dílčí náklady na diversifikované nastavení compliance.

Jak vyplývá z analýzy vypracované advokátní kanceláří DLA Piper, přístup společnosti obecně a podnikatelské sféry k právní úpravě ochrany dat a jejímu porušení se napříč Evropou stále značně liší. Vypovídá o tom kvantitativní pohled na nahlášený počet bezpečnostních incidentů v prvním roce platnosti nařízení GDPR (Schwartz, 2020). Nejvíce incidentů bylo hlášeno v Nizozemsku, a to téměř čtvrtina z celkového počtu (téměř 15 000 z 60 000). Na druhém místě bylo nepoměrně větší Německo s přibližně pětinovým podílem, zatímco např. srovnatelně velká sousední Belgie vykázala pouze necelých 500 oznámení. Ve státech střední a východní Evropy vč. ČR (s výjimkou Polska) proběhly pouze stovky oznámení.

Nařízení GDPR předvídá v článku 40 vypracování kodexů chování na úrovni podniků, které budou specificky zohledňovat konkrétní povahu různých odvětví ekonomiky. Kodexy chování mají ambici být nástrojem posilujícím prvkem seberegulace ve světle

výše analyzovaného ústředního principu odpovědnosti správce. Potenciál kodexů chování však u nás dosud nebyl naplněn, protože v ČR zatím nebyl přijat ani jeden kodex chování (Nonneman, 2020).

Závěr

Praxe v ČR ukázala, že většina firem, veřejných institucí i územních samosprávných celků věnovala nařízení GDPR zpočátku malou pozornost a nebyl tak efektivně využit časový prostor dvou let před jeho plnou implementací (Nezmar, 2017, str. 13). Povinné subjekty se tak vystavily hrozbě vysokých pokut, které nařízení předvídá pro případ nesplnění uložených povinností.

Hlavním očekáváním, které by mělo být spojeno s každou právní regulací v této oblasti, je zefektivnění a zvýšení úrovně ochrany osobních údajů. V každodenním životě, jako koncoví zákazníci a uživatelé různých služeb jsme zaznamenali častou nutnost vyslovit „souhlas podle GDPR" jako podmínku pro realizaci téměř jakékoli obchodní transakce. Může se zdát, že odpovědnost, která byla správcům osobních údajů uložená, je vede jen ke splnění této formální povinnosti opatřit si souhlas k jeho případnému pozdějšímu prokazování.

V širších souvislostech, které byly v příspěvku nastíněny, lze důvodně očekávat, že obchodníci a podnikatelé v důsledku uložené odpovědnosti zavedli hlubší a sofistikovanější kontrolní mechanismy, zejména ve vztahu ke třetím stranám a externím dodavatelům, což v dlouhodobé perspektivě skutečně má nemalý potenciál zkvalitnit právní prostředí ochrany citlivých dat.

Zdroje

ANDREISOVÁ, L. Analysis of the Impact of the GDPR on Third-Party Risk Management Programs and Related Recommendations for Domestic as Well as International Corporate World. *Business and Management Studies*. Vol. 6, No. 1, 2020, s. 4.

GALDIES, P. Six Steps for Managing the GDPR Third-Party Threat. [on-line, 2019-14-01] *Data Quality Management Group*. Dostupné z: < https://www.dqmgrc.com/article/6-steps-managing-gdpr-third-party-threat > [cit. 2020-04-14]

GOLDMAN, D. Compliance Takeaways from 5 Third-Party Data Breaches in 2019. [on-line, 2019-11-17] *Corporate Compliance Insights*. Dostupné z: <https://www.corporatecomplianceinsights.com/compliance-takeaways-third-party-breaches/ > [cit. 2020-04-14]

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. Úř. věst. L 119, 4.5.2016, s. 1.

NEZMAR, L. *GDPR. Praktický průvodce implementací*. Praha: Grada, 2017, ISBN: 9788027109203, 304 s.

NONNEMANN, F. Je co slavit? Den ochrany osobních údajů, aneb rok a půl s GDPR. [on-line, 2020-01-24] *Tayllorcox.cz* Dostupné z: < https://www.tx.cz/blog/den-ochrany-osobnich-udaju-aneb-rok-a-pul-s-gdpr-28-01-2020 > [cit. 2020-04-14]

NONNEMANN, F. Privacy by design jako jedno z nových pravidel pro zpracování osobních údajů? [on-line, 2018-04-20] *Epravo.cz*. Dostupné z: <https://www.epravo.cz/top/clanky/privacy-by-design-jako-jedno-z-novych-pravidel-pro-zpracovani-osobnich-udaju-107367.html > [cit. 2020-04-14]

Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. 3. 2019, č. j. UOOU-10138/18-8. Dostupné z: < https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34470> [cit. 2020-06-03]

Rozsudek Soudního dvora ze dne 10. října 1973. *Fratelli Variola S.p.A. proti Amministrazione italiana delle Finanze*. Žádost o rozhodnutí o předběžné otázce: Tribunale civile e penale di Trieste - Itálie. Věc C-34-73. ECLI:EU:C:1973:101

SCHWARTZ, M. J. Data Breach Reports in Europe Under GDPR Exceed 59,000. Netherlands, Germany and UK Have Logged the Most Data Breach Reports. [on-line, 2019-02-06] *Bank Info Security*. Dostupné z: <https://www.bankinfosecurity.com/data-breach-reports-in-europe-under-gdpr-exceed-59000-a-12006> [cit. 2020-04-14]

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Úř věst. L 281, 23.11.1995, s. 31 -50.

Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat. *Rada Evropy*. Dostupné z: < https://rm.coe.int/1680994818 > [cit. 2020-06-03]