29. 3. 2022

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Zabezpečení osobních údajů a pokuty

Obecné nařízení o ochraně osobních údajů[1] (GDPR) oslaví v květnu již čtyři roky účinnosti. Definice základních pojmů, hlavní principy zpracování a související práva a povinnosti byly z velké míry převzaty z předchozí právní úpravy[2]. Některé části GDPR však stále vyvolávají otázky, resp. neexistuje k nim jednotný výklad. Týká se to jak vztahu konkrétních ustanovení GDPR k předchozím právním předpisům upravujícím zpracování osobních údajů, zejména tam, kde se normativní text změnil, tak i některých zcela nových institutů, které GDPR přineslo.

Na konci února tohoto roku rozhodl Nejvyšší správní soud v kauze obsahující otázky z obou uvedených kategorií.[3] Ve sporu Úřadu pro ochranu osobních údajů a Nemocnice Tábor, a.s., se Nejvyšší správní soud vyjádřil k těmto sporným bodům:

1. Jsou požadavky čl. 32 GDPR na zabezpečení osobních údajů mírnější, než byly požadavky § 13 zrušeného zákona č. 101/2000 Sb.?
2. Je „veřejná“ nemocnice veřejným subjektem ve smyslu čl. 83 odst. 7 GDPR, a proto jí za porušení pravidel pro zpracování osobních údajů nelze uložit pokutu?

Nedostatečné logování přístupů ke zdravotnické dokumentaci

Oč se v daném sporu jednalo?

Nemocnice Tábor, a.s., dostala od Úřadu pro ochranu osobních údajů v říjnu roku 2018, tedy již po účinnosti GDPR, pokutu za nedostatečné logování přístupů k elektronicky vedené zdravotnické dokumentaci. Úřad nemocnici vyčítal, že logy neumožňovaly ověřit, z jakého důvodu bylo v konkrétním případě k údajům z dokumentace přistoupeno, a dále to, že nemocnice neprováděla pravidelné kontroly přístupů k elektronické zdravotní dokumentaci (logů). Za tato pochybení jí úřad uložil pokutu 80.000,- Kč, která byla na základě rozkladu předsedkyní úřadu snížena na 40.000,- Kč.

Nemocnice Tábor, a.s., se bránila tím, že pozdější úprava, tzn. GDPR, obsahuje mírnější požadavky na zabezpečení osobních údajů, než zákon č. 101/2000 Sb. GDPR, na rozdíl od již zrušeného zákona, explicitně nepožaduje, aby byl každý přístup k osobním údajům logován, tím spíše se zachycením důvodu přístupu. Nemocnice rovněž namítala, že je veřejným subjektem a že tedy za případné porušení GDPR nemůže dostat pokutu.

Nemocnice rozhodnutí úřadu napadla u Městského soudu v Praze. Ten však její správní žalobu zamítl. Proto se věc dostala až k Nejvyššímu správnímu soudu.

Zabezpečení osobních údajů před a po GDPR

Jak přesně se změnila právní úprava zabezpečení osobních údajů?

V zákoně č. 101/2000 Sb. byly povinnosti zabezpečit zpracovávané osobní údaje popsány poměrně detailně v § 13 takto:

(1) Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným

přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

(2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

(3) V rámci opatření podle odstavce 1 správce nebo zpracovatel posuzuje rizika týkající se

a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,

b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,

c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a

d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

(4) V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také

a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,

b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,

c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a

d) zabránit neoprávněnému přístupu k datovým nosičům.

A jak tuto otázku, zabezpečení osobních údajů, upravuje čl. 32 GDPR, konkrétně první a druhý odstavec tohoto článku[4]?

1. *S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:*

a) pseudonymizace a šifrování osobních údajů;

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Při pouhém jazykovém výkladu bychom mohli dospět k tomu, že existuje zjevný rozdíl v koncepčním přístupu k otázce zabezpečení osobních údajů: Zákon č. 101/2000 Sb. ukládal všem správcům údajů v oblasti zabezpečení dat v zásadě stejné povinnosti. Pokud správce zpracovával osobní údaje automatizovaně, což je již řadu let standardem, zákon definoval povinné minimum dalších bezpečnostních opatření. Jejich součástí bylo i logování veškeré aktivity s elektronicky zpracovávanými údaji, včetně náhledu na ně. Právě absence možnosti určit, proč k přístupu k osobním údajů došlo, byla jedním z důvodů pro uložení sankce Nemocnici Tábor, a.s.

Citovaný čl. 32 GDPR je naopak jedním z těch, ve kterých se projevuje tzv. přístup založený na riziku (risk-based approach). V kostce řečeno, GDPR správci a zpracovateli v oblasti zabezpečení dat ukládá, aby sám zhodnotil celé zpracování osobních údajů, jeho citlivost, související rizika pro správce či zpracovatele i pro subjekt údajů, své možnosti a varianty ochrany dat, a na základě tohoto vyhodnocení aplikoval taková bezpečnostní opatření, jaká jsou podle jeho názoru dostatečná. GDPR uvádí pouze příklad opatření, která správce či zpracovatel může zavést, pokud to po provedené analýze považuje za vhodné. Logování jako takové výslovně nezmiňuje.

A právě tímto rozdílem a neexistencí výslovně uložené povinnosti logovat přístupy k osobním údajům nemocnice argumentovala. S odkazem na takto vykládaný vývoj legislativy uvedla, že GDPR je v porovnání se zákonem č. 101/2000 Sb. příznivější právní úpravou. Příznivější, protože správcům údajů automaticky neukládá povinnost pořizovat logy o přístupu k osobním údajům způsobem, který umožní ověřit důvod konkrétního přístupu k datům. S ohledem na účinnost GDPR v době rozhodování o pokutě měl podle jejího názoru Úřad pro ochranu osobních údajů aplikovat právě GDPR, podle kterého by praxe nemocnice týkající se logování deliktem nebyla.

NSS: požadavky na zabezpečení osobních údajů se nezměnily

Nejvyšší správní soud této námitce nepřisvědčil. Soud s odkazem na svoje předchozí rozhodnutí[5], které se zabývalo obdobně formulovanou námitkou Ministerstva vnitra, potvrdil závěr Městského soudu v Praze. Můžeme tedy konstatovat, že k této otázce již máme relativně ustálenou judikaturu správních soudů.

A jak že se tedy správní soudy k vývoji právní úpravy zabezpečení osobních údajů staví?

K rozdílům v dikci čl. 32 GDPR a § 13 dřívějšího zákona č. 101/2000 Sb. se Nejvyšší správní soud dovodil, že § 13 odst. 1 ve spojení s odst. 3 původního zákona o ochraně osobních údajů implicitně také předpokládal jistou míru volnosti v opatření zavedených k ochraně zpracovávaných údajů. Podle Nejvyššího správního soudu bývalý zákon č. 101/2000 Sb. ukládal správcům a zpracovatelům nastavená opatření upravit dle rizik analyzovaných postupem podle § 13 odst. 3 zákona. A právě z tohoto důvodu podle názoru Nejvyššího správního soudu pozdější úprava v GDPR není fakticky jiná, protože i ona povinným subjektům umožňuje, resp. ukládá, aby bezpečnostní opatření přizpůsobila podmínkám svého zpracování. Výčet okolností, které mají být podle GDPR při rozhodování o jednotlivých opatření vzaty v potaz, obsah dané povinnosti jako takové nemění, pouze upřesňuje.[6] [7]

V předmětném sporu pak bylo důležité, že Úřad pro ochranu osobních údajů Nemocnici Tábor, a.s., uložil pokutu právě za porušení § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnosti zavést vhodná bezpečnostní opatření, nikoliv za nedostatky v logováním jako takovém. Jestliže, jak Nejvyšší správní

soud v komentovaném rozsudku potvrdil, je § 13 odst. 1 ve spojení s odst. 3 zákona č. 101/2000 Sb. obsahově totožný jako čl. 32 GDPR, pak se nejedná o příznivější úpravu, které by se účastník řízení mohl dovolávat.

Jinými slovy, jak zákon č. 101/2000 Sb., tak GDPR, správcům i zpracovatelům osobních údajů ukládají, aby technicko-organizační opatření k ochraně údajů přizpůsobili souvisejícím rizikům a dalším okolnostem a podmínkám zpracování. Skutečnost, že to předchozí zákon nečinil tak explicitně jako GDPR, není rozhodující. Jak uvádí Nejvyšší správní soud, určité formulační rozdíly nelze vykládat tak, že GDPR požadavky týkající se zabezpečení dat snižuje.

Kdo nemůže dostat pokutu za porušení GDPR?

Druhá řešená otázka naopak byla z kategorie novinek, které GDPR a s ní související legislativa přinesly.

GDPR v čl. 83 odst. 7 uvádí, že členské státy mohou stanovit pravidla týkající se toho, zda jaké je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě. Při projednávání českého zákona se objevovaly poplašné hlasy o tom, jak malé obce kvůli banálnímu porušení pravidel budou dostávat pokuty v řádech milionů euro a tím budou úplně zlikvidovány. Český zákonodárce využil možnosti dané mu uvedeným článkem GDPR a veřejným subjektům dal „generální pardon“, když zákonem absolutně vyloučil možnost je za porušení GDPR sankcionovat.[8]

Toto plošné vyloučení odpovědnosti je upraveno v § 62 odst. 5 zákona č. 110/2019 Sb., o zpracování osobních údajů: „Úřad upustí od uložení správního trestu také tehdy, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2016/679.“

Jak vidno, zákonodárce se příliš nezdržoval upřesněním, koho je v kontextu českého právního řádu nutno chápat jako orgán veřejném moci a zejména veřejný subjekt. Zejména u pojmu „veřejný subjekt“ to v praxi způsobuje řadu problémů.[9]

Není veřejný subjekt jako veřejný subjekt

Nemocnice Tábor, a.s., se pokusila uložené pokutě bránit i tvrzením, že jako „veřejná“ nemocnice je veřejným subjektem ve smyslu čl. 83 odst. 7 GDPR, a pokutu jí tudíž uložit nelze. Nemocnice argumentovala mj. tím, že:

- je převážně financovaná z veřejného zdravotního pojištění,
- je povinným subjektem, veřejnou institucí, ve smyslu zákona č. 106/1999 Sb.,
- je veřejným zadavatelem podle zákona č. č. 134/2016 Sb., o zadávání veřejných zakázek, a
- vede zdravotnickou dokumentaci, protože jí to ukládá zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování.

Nejvyšší správní soud však ani takto široce formulované a odůvodněné námitce nevyhověl. Po konstatování, že pojem veřejná instituce není v českém právu definován, soud uvedl alespoň základní znaky, které obvykle činí veřejnou instituci veřejnou institucí. Jsou jimi zejména zřízení daného subjektu zákonem a jeho určení k plnění úkolů ve veřejném zájmu a dále skutečnost, že nedisponuje vlastním majetkem.

Nemocnice Tábor, a.s., je akciovou společností, která dostává finanční plnění za poskytnutí zdravotních služeb, nikoliv přímo z veřejných rozpočtů. Ač je tedy jistě poskytování zdravotních služeb ve veřejném zájmu, Nemocnice Tábor, a.s., nemůže být podle Nejvyššího správního soudu

chápána jako veřejný subjekt ve smyslu čl. 83 odst. 7 GDPR.

Další argumenty o tom, že nemocnice je povinný subjektem podle zákona č. 106/1999 Sb., zadavatele veřejných zakázek či subjektem povinným vést zdravotnickou dokumentaci, pak soud označil za zcela irelevantní.[10]

Je pojem veřejný subjekt podle GDPR zcela vyjasněn?

Ne, bohužel není. Nejvyšší správní soud v komentovaném rozsudku výslovně uvádí, že se nechce pouštět do detailní definice pojmu veřejný subjekt podle GDPR. Rozsudek nicméně k vyjasnění tohoto pojmu i tak přispěl, když narýsoval hranice takříkajíc z obou stran.

Nejvyšší správní soud na jedné straně definoval základní prvky, které musí organizace obvykle (tedy nikoliv bezvýjimečně) splňovat, aby mohla být za veřejný subjekt v tomto smyslu považována. Je jimi zřízení zákonem, plnění veřejných úkolů či zajištění činnosti ve veřejném zájmu, zřejmě i financování přímo z veřejných rozpočtů a neexistence vlastního majetku.

Poslední bod, neexistence vlastního majetku, je důležitý pro posouzení společnosti, která je sice zřízena nebo kontrolována veřejnoprávním subjektem (typicky krajem či obcí), nicméně ve formě obchodní korporace, která má vlastní majetek. Otázkou však zůstává postavení dalších subjektů, například příspěvkových organizací, které získávají prostředky jak od zřizovatele, tak vlastní činností.[11] S ohledem na způsob jejich založení, obvyklý účel činnosti i převažující způsob hospodaření bych se v kontextu komentovaného rozsudku přikláněl k tomu, že se na ně výjimka z možnosti uložit pokutu pro porušení GDPR spíše uplatní. Záležet však bude na charakteru konkrétního subjektu.

Soud naopak jednoznačně uvedl, že výkon jiné veřejnoprávní agendy či podřazení činnosti organizace pod některou z veřejnoprávních regulací, např. v oblasti zadávání veřejných zakázek, nemůže být důvodem k tomu ji chápat jako veřejný subjekt podle GDPR. I když to tak Nejvyšší správní soud přímo neformuloval, můžeme zřejmě konstatovat, že české právo definici veřejného subjektu ve smyslu GDPR nemůžeme použít ani analogicky. Jinak řečeno, skutečnost, že je některá organizace například veřejnou institucí povinnou poskytovat informace podle zákona o svobodném přístupu k informacím, není rozhodující, není vodítkem, které bychom mohli následovat. Výklad týkající se toho, jaké subjekty jsou nebo nejsou povinnými podle jiných regulací, je tak z pohledu GDPR irelevantní.

Ač Nejvyšší správní soud pojem veřejný subjekt podle čl. 83 odst. 7 GDPR do jisté míry ohraničil, pozitivním i negativním vymezením, přímo jej nedefinoval. Na další vyjasnění otázky, kdo je a kdo není veřejným subjektem, a komu tedy hrozí či nehrozí sankce za porušení GDPR, si budeme muset počkat na rozhodnutí dozorového úřadu a správních soudů.

Mgr. František Nonnemann

Autor je konzultantem v oblasti ochrany osobních údajů a compliance a členem Výboru Spolku pro ochranu osobních údajů.

Článek vyjadřuje osobní názor autora.

e-mail: nonnemann@volny.cz

---

[1] 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 (obecné nařízení o ochraně osobních údajů).

[2] 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, která byla transponována zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[3] Rozsudek Nejvyššího správního soudu ze dne 25. února 2022, č.j. 10 As 190/2020.

[4] Třetí odstavec tohoto ustanovení se týká, v praxi dosud nepříliš rozšířené, certifikace, čtvrtý pak předávání osobních údajů mimo Evropskou unii. Pro témata tohoto článku je není nutné citovat.

[5] Rozsudek Nejvyššího správního soudu ze dne 27. června 2019, č.j. 4 As 140/2019 – 27.

[6] Bod 26 rozsudku Nejvyššího správního soudu ze dne 27. června 2019, č.j. 4 As 140/2019 – 27, resp. bod 24 rozsudku Nejvyššího správního soudu ze dne 25. února 2022, č.j. 10 As 190/2020.

[7] K podobnému závěru směrovala i dřívější komentářová literatura. Srov. komentář v § 13 v Kučerová, A. Nováková, L. Foldová, V. Nonnemann, F. Pospíšil, D. Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012.

[8] Výjimka se ovšem netýká jen (malých) obcí. ÚOOÚ informoval mj. o tom, že kvůli této právní úpravě nemohl dát pokutu například Ministerstvu vnitra, které v kontrolovaném období umožnilo 95.000 zcela nebo částečně neoprávněných přístupů do registru obyvatel… https://www.uoou.cz/uoou-nemohl-udelit-pokutu-ministerstvu-neumoznuje-mu-to-zakon/d-35454/p1=1483.

[9] Základní analýzu tohoto pojmu v českém právu obsahuje stanovisko Spolku pro ochranu osobních údajů „Komu nehrozí pokuty podle GDPR? K výkladu pojmu veřejný subjekt ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů“ publikované dne 17. září 2019 na epravo.cz (https://www.epravo.cz/top/clanky/komu-nehrozi-pokuty-podle-gdpr-k-vykladu-pojmu-verejny-subjekt-ve-smyslu-zakona-c-1102019-sb-o-zpracovani-osobnich-udaju-109978.html?mail)

[10] Srov. body 33-35 rozsudku Nejvyššího správního soudu ze dne 25. února 2022, č.j. 10 As 190/2020.

[11] Viz § 28 zákona č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů.

Další články:

- Pokuta za švarcsystém kurýrů Rohlíku potvrzena Ústavním soudem
- Metropolitní plán schválen. Je Váš projekt v bezpečí?
- Posouzení shody dle AI Act - zkušenosti z praxe
- Začínají soudy zohledňovat náklady podnikatelů při plnění právních povinností v oblasti e-commerce?
- Byznys a paragrafy, díl 35: Ručení za dluhy z podnikání u OSVČ a s.r.o.
- Bezpilotní systémy vlastní konstrukce v kategorii Specific: regulatorní požadavky a praktické aspekty
- Nefungující rozsah péče o dítě. Cesta přes využití terapie a dalších opatření podle ustanovení § 503 zákona o zvláštních řízeních soudních
- De iure traktor, de facto nákladní vozidlo, už ne tolik výhodná dualita
- Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?
- Pokuta 32 mil. EUR pro Dacia/Renault – evropské soutěžní úřady tvrdě došlapují na no-poaching. Měla by Vaše společnost být na pozoru?
- Rozdělení společného jmění manželů v případech výdělečné činnosti pouze jednoho z manželů