Hlavní dopady GDPR na obce

Mgr. Tomáš Lechner, Ph.D.

VŠE v Praze, Národohospodářská fakulta, katedra práva

Úvod

Ochrana osobních údajů je na evropské úrovni definována v čl. 8 **Listiny základních práv Evropské unie** jako samostatné právo. Řadí se tak mezi základní stanovené svobody jako právo na svobodu a bezpečnost, právo na respektování svého soukromého a rodinného života, obydlí a komunikace, právo uzavřít manželství a založit rodinu a další. Již v tomto předpise je stanoveno, že osobní údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem (čl. 8 odst. 2). Kromě toho je v cit. předpise dále uvedeno, že každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu. A dále, že na dodržování těchto pravidel dohlíží nezávislý orgán. Detailní informace ke stávajícímu právnímu stavu na evropské úrovni lze najít v publikaci [1].

Listina základních práv a svobod jako součást ústavního pořádku České republiky (ústavní zákon č. 2/1992 Sb.) je v tomto ohledu mnohem stručnější. Ustanovení čl. 10 odst. 3 říká, že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Základem zákonné regulace je 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 do českého právního řádu implementována v podobě **zákona č. 101/2000 Sb., o ochraně osobních údajů** a o změně některých zákonů. Rozbor problematiky ochrany osobních údajů podle stávající právní úpravy je velmi pěkně pojednán v publikaci [2].

S cílem přispět k dotvoření prostoru svobody, bezpečnosti a práva a hospodářské unie, dále přispět k hospodářskému a sociálnímu pokroku, k posílení a sblížení ekonomik v rámci vnitřního trhu a k dobrým životním podmínkám fyzických osob v rámci Evropské unie bylo dne 27. dubna 2016 schváleno **Nařízení Evropského parlamentu a Rady EU 2016/679, 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), pro které se často používá zkratka **GDPR** z anglického označení „General Data Protection Regulation“. Toto nařízení bylo publikováno v Úředním věstníku Evropské unie dne 4. května 2016 a v platnost vstoupilo 24. května 2016, přičemž **účinnosti nabude až 25. května 2018**. Do té doby musí být v České republice připraven adaptační zákon, který nahradí stávající zákon o ochraně osobních údajů a novelizuje další ustanovení zákonů tak, aby byla v souladu s tímto nařízením. Nařízení samo je samozřejmě z principu závazné v celém rozsahu a přímo použitelné ve všech členských státech.

Předmětem tohoto příspěvku je základní rozbor dopadů GDPR na obce v České republice. Samozřejmě, že všechny detailní souvislosti bude možné postihnout, až bude schválen zmíněný adaptační zákon, nicméně již nyní je mnoho věcí jasných, plynoucích přímo z vlastního nařízení.

Struktura a pojmy v nařízení

Nařízení Evropského parlamentu a Rady EU 2016/679 (dále jen „GDPR“) je rozděleno na 11 kapitol. První kapitole je definován základní předmět nařízení, věcná a místní působnost a pojmy. V druhé kapitole jsou definovány základní zásady zpracování osobních údajů. Třetí kapitola se věnuje právům subjektu údajů, čtvrtá pak povinnostem správců a zpracovatelů. Pátá kapitola specifikuje postupy a pravidla pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím.

Šestá kapitola se týká nezávislých dozorových úřadů na národní úrovni, tedy z pohledu České republiky jde o **Úřad pro ochranu osobních údajů** [3]. Sedmá kapitola GDPR dále navazuje na předchozí kapitolu a rozvíjí oblast spolupráce mezi dozorovými úřady navzájem i mezi dozorovými úřady a **Evropským sborem pro ochranu osobních údajů**, který vzniká nově právě na základě GDPR. Tento sbor jako subjekt Unie s právní subjektivitou (viz čl. 68 GDPR) zejména monitoruje a zajišťuje řádné uplatňování GDPR, vydává pokyny, doporučení a osvědčené postupy podle tohoto nařízení a přezkoumává jejich praktické uplatňování, podporuje výměnu znalostí a dokumentů o právních předpisech v oblasti ochrany osobních údajů a zavedených postupech s dozorovými úřady pro ochranu údajů po celém světě, dále provozuje veřejně přístupný elektronický registr rozhodnutí přijatých dozorovými úřady a soudy k otázkám řešeným v rámci mechanismu jednotnosti a plní další úkoly podle cit. nařízení (detailně k úkolům sboru viz čl. 70 GDPR).

Osmá kapitola GDPR stanoví další práva subjektu údajů a dále se věnuje odpovědnosti a sankcím. Devátá kapitola se věnuje zvláštním situacím, při nichž dochází ke zpracování osobních údajů. Desátá kapitola se týká prováděcích právních předpisů a poslední jedenáctá kapitola obsahuje závěrečná ustanovení včetně vztahu ke směrnici 2002/58/ES. Je zde také specifikována již zmíněná účinnost stanovená na 25. května 2018. Blíže ke struktuře GDPR viz [4].

Z hlediska definice vlastního předmětu ochrany, tedy osobních údajů, se GDPR neliší od stávající právní úpravy. To, v čem se původní a nový přístup liší, jsou příklady daných možností identifikace fyzické osoby, tedy subjektu údajů. GDPR přidává do výčtu příkladů lokační údaje nebo síťový identifikátor. Tyto se ale stávají osobními údaji pouze za podmínky, že jimi lze fyzickou osobu skutečně identifikovat. Je tedy zcela nesprávné domnívat se, že GDPR obecně považuje IP adresu počítače za osobní údaj. Stejně jako jméno a město trvalého bydliště mohou být osobními údaji, pokud se v daném městě nevyskytuje jiná osoba stejného jména, ale nejsou jimi, pokud je v daném městě jmenovců více, tak IP adresa se může osobním údajem stát, pokud pomocí ní lze v rámci daného procesu konkrétní osobu identifikovat. Vždy je tedy třeba posuzovat okolnosti a procesy, které v daném případě zpracování jsou implementovány, abychom mohli rozhodnout, zda určitá množina údajů odpovídá či neodpovídá definici osobních údajů.

GDPR přináší několik nových pojmů právě v oblasti souvztažných procesů souvisejících buď se zpracováním osobních údajů, jako např. profilování, nebo s jejich ochranou, jako je např. pseudonymizace. Protože jde o zcela nové pojmy, ocitujme zde přímo konkrétní definice.

- **Profilováním** se podle čl. 4 odst. 4 GDPR rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů

týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu. Z definice je zřejmé, že tento proces se primárně týká soukromého sektoru, nicméně může být součástí některých manažerských výstupů i informačních systémů provozovaných na obcí a sloužící třeba např. pro generování podkladů pro posouzení přiznání dotace.

- **Pseudonymizací** se podle čl. 4 odst. 5 GDPR rozumí zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě. Asi nejvýznamnějším příkladem pseudonymice použité v České republice je systém základních a agendových identifikátorů fyzických osob použitý v základních registrech veřejné správy [5].

Z hlediska obecného rozboru GDPR si povšimněme ještě jeho působnosti. Z pohledu orgánů veřejné moci se **GDPR ve věcné působnosti vztahuje na veškeré automatizované zpracování osobních údajů**, kromě zpracování osobních údajů prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, jejichž zpracování bude upravovat nová směrnice Evropského parlamentu a Rady EU 2016/680, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

Z hlediska místní působnosti se GDPR vztahuje na zpracování všech osobních údajů správcem nebo zpracovatelem usazeným v Evropské unii bez ohledu na to, kde toto zpracování probíhá. A také se vztahuje na osobní údaje všech subjektů údajů, které se nacházejí v Unii, tedy zejména občanů všech členských států, ať jsou zpracovány subjektem usazeným v Unii nebo mimo ni s tím, že na správce a zpracovatele mimo Unii se vztahuje jen, pokud činnosti zpracování souvisejí s nabídkou zboží anebo monitorováním chování. Z hlediska občanů členských států Evropské unie je tedy má toto nařízení chránit, ať zpracování jejich osobních údajů probíhá kdekoliv a kýmkoliv.

Zpracování osobních údajů orgány veřejné moci

Vyjděme ze základních zásad zpracování osobních údajů, které jsou následující [4]:

- **Zákonnost** je základní principem. Podmínky zákonnosti zpracování osobních údajů jsou dány čl. 6 GDPR a patří mezi ně zejména udělení souhlasu subjektem údajů, nebo nezbytnost pro splnění právních povinností, nebo nezbytnost pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby. Z hlediska municipalit jako jednoznačně nejčastějším odůvodněním zpracování osobních údajů je plnění právních povinností. Nicméně musíme si uvědomit, že jsou i činnosti, které obec nebo jí zřizované organizace vykonávají nad rámec povinností, byť samozřejmě podložených vhodným zmocněním vycházejícím např. z § 2 odst. 2 zákona č. 128/2000 Sb., o obcích. V takových případech je pak samozřejmě nezbytné udělení souhlasu subjektem údajů.

- **Korektnost a transparentnost** se týkají nejen obecného způsobu zpracování, ale též poskytování informací subjektu údajů dle čl. 12, 13 a 14 GDPR.

- **Účelové omezení** znamená, že osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.

- **Minimalizace údajů** patří nejen mezi základní zásady zpracování osobních údajů, ale také mezi opatření aplikovaná pro jejich ochranu. V praxi to znamená, že osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

- **Přesnost** zpracovávaných osobních údajů je další zásadou. Ta znamená také případnou povinnou aktualizaci a přijetí opatření zajišťující, aby nepřesné údaje byly vymazány nebo opraveny.

- **Omezení uložení** znamená uložení na dobu nezbytnou pro účel zpracování osobních údajů.

- **Integrita a důvěrnost** znamená mimo jiné, že osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických a organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

- **Odpovědnost** správce i zpracovatele je poslední ze základních zásad zpracování osobních údajů.

Všechny tyto zásady musí být dodržovány všemi správci i zpracovateli osobních údajů, ať už patří mezi subjekty veřejného nebo soukromého sektoru. Z pohledu obcí je, jak už bylo zmíněno, nejčastějším účelem zpracování plnění zákonných povinností. Je však třeba mít na paměti, že daná zákonná povinnost např. vedení matričních knih a související sbírky listin, nebo evidence účastníků správního řízení nezprošťuje obce povinnosti dodržovat pro tyto činnosti základní zásady zpracování osobních údajů.

Stávající zákon o ochraně osobních údajů obsahuje ustanovení o oznamovací povinnosti, které jsou zproštění ti, kdo zpracovávají osobních údaje podle zvláštního zákona nebo je zpracování osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona (viz § 16 a § 18 zákona č. 101/2000 Sb., o ochraně osobních údajů, v aktuálním znění), což je tedy zejména případ obcí či jiných orgánů veřejné moci. Avšak ustanovení § 18 odst. 2 cit. zákona říká, že správce, který provádí zpracování z výše uvedeného důvodu, je povinen zajistit, aby informace, týkající se zejména účelu zpracování, kategorií osobních údajů, kategorií subjektů údajů, kategorií příjemců a doby uchování, které by byly jinak přístupné prostřednictvím registru vedeného Úřadem pro ochranu osobních údajů, byly zpřístupněny dálkovým přístupem nebo jinou vhodnou formou. Jinými slovy, každá obec musí dle stávající platné úpravy na svých webových stránkách zveřejnit informace o zpracování osobních údajů, které provádí v rámci plnění svých zákonných povinností. Jako příklady lze opět jmenovat vedení matričních knih, ale i evidenci poplatníků místních poplatků nebo vedeních stálého seznamu voličů.

GDPR žádné ustanovení o oznamovací povinnosti neobsahuje. V preambuli je k tomu přímo řečeno, že tato povinnost přináší administrativní a finanční zátěž, avšak nepřispívá ve všech případech ke zlepšení ochrany osobních údajů, a proto by měla být tato nerozlišená obecná ohlašovací povinnost zrušena a nahrazena účinnými postupy a mechanismy, které by se místo toho zaměřily na takové typy operací zpracování, jež mohou s ohledem na svou povahu, rozsah, kontext a účely představovat vysoké riziko pro práva a svobody fyzických osob (odst. 89 preambule). Podmiňovací způsob samozřejmě směřuje jako pokyn k adaptačním zákonům v jednotlivých členských státech. Jak se k tomu postaví zákonodárci v České republice, to samozřejmě ukáže až čas. Nicméně **GDPR nahrazuje tuto oznamovací povinnost zejména pravidly pro transparentnost**. Konkrétně čl. 12 odst. 1 GDPR stanoví, že správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků informace o zpracování osobních údajů v rozsahu stanoveném nařízením. Tento rozsah se liší podle toho, zda údaje jsou získávány přímo od subjektu údajů (např. při přihlášení majitele psa k místnímu poplatku), nebo jsou-li získávány z jiných zdrojů (např. ze základních registrů při vedení stálého seznamu voličů). Rozsah údajů pro první případ je dán čl. 13, pro druhý případ pak č. 14 GDPR. Lze se domnívat, že zveřejnění informací o zpracování osobních údajů na webových stránkách obce, jaké jsou již obce povinné realizovat nyní, plní zásadu transparentnosti danou ustanovením citovaného čl. 12. V tomto ohledu tedy nebude zřejmě třeba významných změn, avšak GDPR nové povinnosti přináší v dalších ohledech, jak bude ukázáno dále.

Nové povinnosti

Jednou ze zásadních novinek, kterou GDPR přináší, **je povinnost jmenovat pověřence pro ochranu osobních údajů**. Ne každý správce jej musí jmenovat, ale obce tuto povinnost mají. Pověřenec musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů (čl. 37 odst. 5 GDPR). Mezi základní úkoly pověřence patří zejména [4]:

- **poskytování informací a poradenství** správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle GDPR,
- poskytování poradenství, pokud jde o **posouzení vlivu na ochranu osobních údajů**, což souvisí s povinností správců v určených případech provést před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů,
- **monitorování souladu s GDPR** v oblasti ochrany osobních údajů,
- **monitorování souladu s koncepcemi** správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů,
- **spolupráce s dozorovým úřadem**, tedy s Úřadem pro ochranu osobních údajů, a působení jako kontaktní místo pro tento úřad,
- **působení jako kontaktní místo pro subjekty údajů** ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR.

Pověřenec pro ochranu osobních údajů může plnit pro organizaci i jiné úkoly a povinnosti, ale z hlediska jeho postavení je velmi důležité, ba přímo zásadní, aby žádný z jeho úkolů a povinností nevedl ke střetu zájmů. Znamená to, že tuto roli nemůže vykonávat např. vedoucí IT oddělení, který zároveň rozhoduje o vlastní realizaci záležitostí týkajících se IT. Role pověřence by se asi dala nejvíce připodobnit k vnitřnímu auditu. Z hlediska obcí je důležité, že jednoho pověřence může „sdílet" více organizací, za podmínky že bude z každé organizace snadno dosažitelný.

Platí obecně, že každý správce 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, jež s sebou zpracování nese, zavede vhodná technická a organizační opatření za účelem ochrany jím zpracovávaných osobních údajů, zejména k zajištění všech základních zásad zpracování osobních údajů (detailně viz čl. 25 GDPR). V případě, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Povinnost **zpracovat toto posouzení vlivu v rozsahu a kontextu čl. 35 GDPR je tedy další významnou novinkou**, kterou toto nařízení přináší, byť samozřejmě nejde o principiální novinku, neboť posouzení rizik přikazuje i stávající právní úprava – viz § 13 odst. 3 zákona č. 101/2000 Sb., o ochraně osobních údajů, v aktuálním znění. Nový je hlavně rozsah a atributy tohoto postupu. To, zda a pro jaké případy bude posouzení povinné pro obce, může ještě ovlivnit český adaptační zákon, popř. přímo Úřad pro ochranu osobních údajů, neboť podle čl. 35 odst. 4 a 5 GDPR dozorový úřad každého státu sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů, a rovněž může sestavit a zveřejnit seznam druhů operací zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné. Otázka povinnosti provést ono posouzení může tedy posléze být různá pro různé agendy.

S ohledem na vyhodnocená rizika je třeba **přijmout vhodná technická a organizační opatření**. Mezi technická zabezpečení patří jednak využití vhodných softwarových nástrojů, ale také specifické postupy, které tyto nástroje aplikují, jako je pseudonymizace či šifrování osobních údajů (viz čl. 35 odst. 1 a čl. 32 odst. 1 GDPR). Dále je důležité zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování. Mezi organizační opatření patří zejména stanovení jasných koncepcí a metodik. V případě obcí se toto doporučuje řešit např. vnitřní směrnicí, byť její zavedení GDPR přímo nepožaduje. Součástí těchto opatření by mělo být také nastavení pravidel procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Protože technická i organizační opatření musí vždy působit synergicky, nelze se spolehnout pouze na prohlášení dodavatele příslušného softwarového nástroje, že tento splňuje podmínky GDPR. Vždy je důležitá i konkrétní implementace a nastavení organizačních pravidel.

Mezi další novinky GDPR patří **nové pojmenování práva subjektu údajů na výmaz jako „právo být zapomenut"**. Nejde tedy o principiální novinku, ale spíše o jasnější vymezení tohoto práva, o jehož naplnění může subjekt údajů v určených případech požádat. Jsou také případy, kdy je aplikováno automaticky s ohledem na jednu ze základních zásad zpracování osobních údajů, a sice „omezení uložení", tedy jakmile pomine důvod pro zpracování, má správce povinnost osobní údaje bez zbytečného odkladu vymazat [viz též § 37 odst. 1 písm.

a) GDPR]. Z pohledu obcí je asi nejdůležitější, že podle čl. 17 odst. 3 se toto právo neuplatní v případě, kdy je zpracování nezbytné při výkonu veřejné moci, kterým je správce pověřen, a také v případě, kdy je toto zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků.

Další novinkou GDPR je **právo na přenositelnost údajů**, jehož technická realizace bude asi poměrně složitá. Podle čl. 20 odst. 3 se ale toto právo neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen. Takže **na obce se toto právo nevztahuje**, pokud nezpracovávají údaje mimo výkon veřejné moci, např. ve zřizované knihovně.

Poslední novinkou GDPR, kterou zde zmíníme, je **povinnost ohlašování a oznamování případů porušení zabezpečení osobních údajů**. Stávající právní úprava v České republice zná tuto povinnost od roku 2012, leč pouze pro oblast elektronických komunikací. Poskytovatelům služeb elektronických komunikací je výslovně uloženo případy porušení ochrany osobních údajů (tzv. „data breaches“) oznámit Úřadu pro ochranu osobních údajů (detailně viz [6]). Obdobné principy hlášení incidentů jsou také zakotveny v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti (viz zejména § 8 cit. zákona). **Povinnost ohlašování a oznamování případů porušení zabezpečení osobních údajů není tedy principiálně novým institutem, ale z hlediska rozsahu dopadů na všechny správce je významnou novinkou GDPR**. Ustanovení čl. 33 a 34 GDPR jmenují tři případy této povinnosti:

- Pokud se správce dozví o jakémkoli porušení zabezpečení osobních údajů, pak bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí tuto skutečnost Úřadu pro ochranu osobních údajů. Hlášení není třeba podat, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

- Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

- Pokud se správce dozví o porušení zabezpečení osobních údajů, které může mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů. I zde jsou uvedeny specifické případy, kdy toto se toto hlášení nepodává, nebo se podává hromadným způsobem.

Shrnutí

GDPR přináší celou řadu nových povinností v oblasti ochrany osobních údajů. Vzhledem k poměrně vysokým centrálně definovaným sankcím za porušení jmenovaných ustanovení tohoto nařízení, se mu věnuje v současné době poměrně velká pozornost. Nutno konstatovat, že **ochrana osobních údajů si** tuto **pozornost jistě zaslouží** a že **přípravu na GDPR není radno podceňovat**. Na druhou stranu se ale v souvislosti s GDPR objevuje i celá řada zkreslujících informací, které snad z důvodů zjednodušování paušalizují některé postupy a zveličují změny, které GDPR přináší. Je třeba tedy přistupovat k tomuto tématu zodpovědně a uvážlivě.

Poděkování

Tento článek byl zpracován s podporou výzkumného projektu VŠE IGS F5/65/2017 „Změny v úkolech obcí v důsledku změn českých a evropských právních předpisů“.

Literatura

[1] AGENTURA EVROPSKÉ UNIE PRO ZÁKLADNÍ PRÁVA. *Příručka evropského práva v oblasti ochrany údajů*. Lucemburk: Úřad pro publikace Evropské unie, 2015. 194 s. ISBN 978-92-871-9933-1. DOI: 10.2811/53430.

[2] MATES, P., JANEČKOVÁ, E., BARTÍK, V. *Ochrana osobních údajů*. Praha: Leges, 2012. 208 s. ISBN 978-80-87576-12-0.

[3] Webové stránky *Úřadu pro ochranu osobních údajů* dostupné na adrese <https://www.uoou.cz/>.

[4] LECHNER, T. Základní rozbor nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR). In: PÁNKOVÁ, K. (ed.). *ISSS 2017*. Hradec Králové, 3.4.2017–4.4.2017. Praha: Triada, 2017, s. 45–53. ISBN 978-80-904566-9-3.

[5] MATES, P., SMEJKAL, V. *E-government v České republice: Právní a technologické aspekty.* 2. podstatně přepracované a rozšířené vydání, Praha: Leges, 2012.

[6] ÚOOÚ. *Narušení bezpečnosti v elektronických komunikacích – základní informace*. Dostupné na adrese <https://www.uoou.cz/zakladni-informace/ds-1575/archiv=0&p1=1569>.