
Stručný popis obsahu nového Obecného nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů (2016/679/EU) představuje reformu ochrany osobních údajů v rámci Evropské unie. Obecné nařízení zasáhne většinu oblastí života státu a hospodářství, které podléhají právu EU (v podstatě s výjimkou činnosti policie a dalších orgánů činných v trestním řízení).

Ochranu osobních údajů upravuje v ČR primárně zákon č. 101/2000 Sb., který implementuje evropskou směrnici z roku 1995. Z této směrnice koncepčně vychází i nové Obecné nařízení, takže jejich základní struktura a klíčové instituty jsou do značné míry podobné. Po stanovení působnosti a definicích jsou pojednány principy nebo zásady ochrany dat, pak práva subjektu údajů, povinnosti správců a zpracovatelů, mezinárodní transfery, dozorové úřady a jejich spolupráce, soudní a správní ochrana, odpovědnost a sankce, sektorová ustanovení.

GDPR je nařízení EU, nahradí tedy český zákon č. 101/2000 Sb., o ochraně osobních údajů. Přestože bude přijat nový zákon o zpracování osobních údajů, primárním předpisem v oblasti ochrany osobních údajů bude přímo nařízení.

Některé povinnosti zaváděné obecným nařízením jsou však zcela nové (mj. povinnost zpracovávat záznamy o činnostech zpracování osobních údajů a v některých případech jmenovat pověřence pro ochranu osobních údajů).

Ministerstvo vnitra se v rámci metodické podpory adresátů právní úpravy zaměřilo především na oblast veřejné správy.

Nejvýznamnější množinou cílových příjemců metodické podpory jsou územní samosprávné celky.

Obecné porovnání nové a dosavadní právní úpravy

Porovnáním Obecného nařízení o ochraně osobních údajů a platné směrnice z roku 1995 lze zjistit následující hlavní rozdíly:

- posílení působnosti (včetně silnější působnosti extraterritoriální)
- posílení ochrany dětí (podmínky souhlasu se zpracováním, podmínky výmazu dat)
- posílení informačních povinností správců (bezplatnost, lhůty)
- posílení některých práv subjektů údajů (bezplatnost, lhůty, rozsah)

Nové nebo nově upravené oblasti a hlavní změny:

- právo „být zapomenut“ (čl. 17)
- právo na přenositelnost osobních údajů (čl. 20)
- podrobná úprava vztahu správce a zpracovatele
- posílení kontroly nad správci mimo území EU
- posílení řady požadavků na správce a zpracovatele, včetně hodnocení dopadů na soukromí a předběžných konzultací s dozorovým orgánem
- upuštění od notifikace všech nových zpracování osobních údajů dozorovému orgánu
- posílení pravidel o zabezpečení dat (zejm. technickém) a hlášení narušení bezpečnosti osobních dat
- pro veřejnou správu a pro část podniků povinný pověřenec pro ochranu osobních údajů
- podrobná úprava instrumentů soft law (kodexy chování, certifikace)
- zásadní sjednocení pravomocí dozorových úřadů (pro ochranu osobních údajů)
- podrobná úprava spolupráce dozorových úřadů
- zcela nová a principiálně nevyzkoušená úprava společného rozhodování dozorových úřadů v různých typech přeshraničních případů
- zavedení rozhodovací pravomoci pro Evropský sbor dozorových úřadů v konkrétních věcech
- sjednocení prostředků pro soudní ochranu před rozhodnutím či nečinností dozorového úřadu a pro soudní ochranu před nezákonným zpracováním, včetně náhrady škody
- sjednocení a zásadní zvýšení sankcí formou 2 %, nebo dokonce 4 % podílu z ročního globálního obrátu podnikatele nebo absolutní částkou 20 mil. eur pro všechny ostatní
- sektorové úpravy pro smíření práva na ochranu údajů se svobodou projevu, s přístupem k úředním dokumentům, pro národní identifikační čísla (RČ apod.), pro zaměstnanecké vztahy atd.

Naopak Obecné nařízení od platné směrnice v zásadě přebírá nebo jen mírně upravuje:

- většinu hlavních definic (osobní údaj, citlivé údaje, správce, koncept souhlasu atd.)
- většinu zásad ochrany osobních údajů (principy a zákonnost zpracování)

- většinu práv subjektů údajů a základní povinnosti správců
- systém opt-out z přímého marketingu
- koncept bariéry u přenosů do třetích zemí s důkladnými restrikcemi a požadavky na ochranu osobních údajů
- zásadní prvky postavení nezávislých dozorových úřadů
- koncept výjimek pro privilegovaná zpracování (archivní, statistická, vědecká, historická)
- koncept výjimek pro ochranu veřejných zájmů (bezpečnost, ekonomika, ochrana práv jiných atd.).

Deset otázek a odpovědí k Obecnému nařízení o ochraně osobních údajů (GDPR)

1. Co je GDPR, proč vzniklo a kdy začne platit?

Obecné nařízení o ochraně osobních údajů (známé též pod anglickou zkratkou GDPR – General Data Protection Regulation) je přímo použitelný předpis Evropské unie. To znamená, že místo stávajícího zákona o ochraně osobních údajů se práva a povinnosti při zpracování osobních údajů budou řídit přímo tímto Obecným nařízením. Nová pravidla o ochraně osobních údajů se tak zásadně nebudou přepisovat do českého práva.

Obecné nařízení bude platit od 25. května 2018, a to ve všech členských státech EU. Cílem je totiž zajistit stejné podmínky ochrany osobních údajů v rámci celé EU, což mělo ušetřit podnikům právní náklady na plnění různých národních předpisů. Ochrana soukromí fyzických osob je základním právem občana EU. Zjednodušeně lze konstatovat, že o každém z nás se zpracovává v důsledku technologického pokroku velké množství osobních údajů, aniž si to uvědomujeme. Cílem jednotné evropské ochrany dat je zajistit, aby naše data byla chráněna stejně.

2. V čem je hlavní odlišnost od platného zákona o ochraně osobních údajů?

Právní předpisy pro ochranu osobních údajů platí již dnes a již dnes se vztahují na každého správce. Nařízení stanoví na platné směrnici z roku 1995, kterou u nás provádí zákon o ochraně osobních údajů (101/2000 Sb.). Jinými slovy, při zpracování osobních údajů již platí řada povinností podle stávajících předpisů. Některé povinnosti Obecné nařízení rozšiřuje (zejm. ty informační) a další povinnosti stanov. Mezi ty hlavní patří:

- rozšíření práva na výmaz („právo být zapomenut“)
- v některých případech zajistit, aby dotčená osoba mohla údaje přenést k jinému správci (přenositelnost)
- před zpracováním i při něm si počínat co nejšetrněji (záměrná ochrana osobních údajů)
- hlásit hackerské útoky a jiné případy, kdy bylo porušeno zabezpečení dat, ÚOOÚ a v některých případech i dotčeným osobám
- v některých případech jmenovat pověřence pro ochranu osobních údajů
- jiná výše pokut.

Na zpracovatele tyto a další povinnosti budou dopadat v různé míře, v závislosti na tom, jak riziková zpracování osobních údajů provádějí.

Oba předpisy mají hodně společného – nemění se základní definice, základní povinnosti a práva ani dozorová role ÚOOÚ.

3. Na koho se vztahuje a na koho nevztahuje GDPR?

Obecné nařízení o ochraně osobních údajů (GDPR) se vztahuje na všechny úřady, podniky i jednotlivce, kteří zpracovávají na území Evropské unie osobní údaje nebo o takovém zpracování rozhodují. Na některé důležité oblasti lidské činnosti se ale GDPR nevztahuje:

- čistě osobní nebo domácí zpracování (videa s rodinnými příslušníky, fotoalba, osobní adresáře a korespondence, bezpečnostní kamery zabírající jen vlastní soukromé prostory apod.)
- zpracování mimo působnost práva EU (např. činnost zpravodajských služeb a obranných zařízení)
- činnost orgánů činných v trestním řízení a podobných bezpečnostních orgánů (policie, státní zastupitelství, věznice apod.).

GDPR se vztahuje i na osoby a podniky, které mimo území Evropské unie provádějí zpracování údajů o lidech, kteří se nacházejí v Evropské unii, pokud jim při tom nabízejí zboží nebo služby nebo monitorují jejich chování.

4. Co je osobní údaj, je někde jejich seznam?

Osobním údajem je informace, která se týká určené nebo přímo či nepřímo určitelné fyzické osoby. Obecně se tak jedná o jakoukoliv informaci, která se určeného nebo určitelného člověka týká, na základě které ho dokáže správce, zpracovatel nebo kdokoliv jiný identifikovat. Není nikde kompletní seznam osobních údajů, např. se

však jedná o jméno, datum narození, ale i jednoznačný identifikátor osoby, fotografie. Údaj vždy směřuje k identifikaci osoby nebo se týká identifikované osoby.

5. Kdo je subjekt údajů a jaká práva má?

Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují. Mezi nová práva patří právo na přenositelnost údajů mezi jednotlivými správci. Rozšířeno bylo právo na výmaz údajů.

6. Kdo je správce a kdo je zpracovatel?

Správce je osoba, která v rámci vykonávání své činnosti zpracovává osobní údaje. Musí proto mít prostředky pro jejich zpracování, tedy cíl dané činnosti (např. ochrana majetku pomocí kamerového systému). To znamená, že správce stanovuje důvod, proč se osobní údaje zpracovávají a jakým způsobem, tedy konkrétní způsob zpracování (nástroj, který bude pro zpracování použit).

Zpracovatel pak zpracovává osobní údaje pro správce, sám však neurčuje účel a prostředky zpracování údajů.

7. Kdy mohu zpracovávat osobní údaje?

Obdobně jako ve stávajícím zákoně o ochraně osobních údajů bude i podle GDPR platit šest právních základů pro zpracování osobních dat:

- Souhlas subjektu údajů (tedy toho člověka, kterého se údaje týkají. Např. vyjádřím souhlas s tím, aby se pro marketingové účely zpracovávaly moje údaje). Pokud byl souhlas vyjádřen svobodně, konkrétně, informovaně a jednoznačně, není potřeba vyžadovat nové souhlasy se zpracováním osobních údajů
- Smlouva nebo příprava smlouvy na žádost subjektu údajů (např. pokud uzavírám kupní či jinou smlouvu nebo žádám o hypotéku)
- Právní povinnost správce (např. pokud správce údajů má v zákoně stanovenou povinnost údaje vést, např. banka má stanovené povinnosti uchovávat údaje o určitých typech bankovních transakcí)
- Životně důležitý zájem subjektu údajů nebo jiného člověka (např. zasahující zdravotník má právo získat moje osobní údaje v okamžiku, kdy mi poskytuje lékařskou pomoc a já nejsem schopen mu je říci sám)
- Úkol správce ve veřejném zájmu, výkon veřejné moci správcem (orgán veřejné moci zpracovává osobní údaje k plnění úkolů veřejné správy)

- Oprávněný zájem správce či jiné osoby, pokud však nepřeváží zájem subjektu údajů (např. ochrana vlastního majetku typicky v případě instalování kamerového systému).

Platí, že právní tituly ke zpracování osobních údajů jsou si rovnocenné a mohou se vzájemně překrývat.

8. Jaké hlavní nové povinnosti podle GDPR má správce (pověřenec, hlášení porušení zabezpečení, záměrná ochrana dat, záznamy o činnostech zpracování, posouzení vlivu, konzultace)

Základní povinnosti správce se příliš nemění. Mezi nové povinnosti patří hlášení o porušení zabezpečení, pokud správce zjistí, že bylo narušeno zabezpečení osobních údajů, například hackerským útokem, vloupáním nebo ztrátou nosiče dat (ne dílčí neoprávněná využití údajů např. zaměstnanci správce). V takovém případě to musí vždy nahlásit na ÚOOÚ a navrhnout způsoby řešení rizik. V případě, že narušení vede k velkému riziku pro subjekty údajů (např. data nejsou šifrována), musí to oznámit subjektům údajů (případně veřejně).

Posouzení vlivu na ochranu osobních údajů platí pro zpracování zahájená po květnu 2018. Pokud je pravděpodobné, že zpracování povede k vysokému riziku pro subjekt údajů, musí se provést hodnocení dopadů, posoudit rizika a kompenzovat je. Pokud ale bude zpracování osobních údajů probíhat na základě právního předpisu, nejsou nutná další hodnocení dopadů ani konzultace s ÚOOÚ

Konzultace s ÚOOÚ lze u rizikových zpracování vést již dle současného znění zákona. Povinná konzultace bude platit pro zpracování zahájená po květnu 2018, pokud zpracování přináší vysoké riziko, má správce před jeho zahájením konzultovat s ÚOOÚ, který má na posouzení asi čtvrt roku a může doporučit další opatření.

Záznamy o činnostech zpracování jsou povinni vést správci a zpracovatelé. Na žádost ÚOOÚ jsou pak povinni tyto údaje zpřístupnit. Součástí těchto záznamů mají být kontaktní údaje správce, účel a rozsah zpracování, informace o příjemcích osobních údajů a lhůty pro výmaz, dále pak popis přijatých technicko-organizačních opatření k zajištění ochrany osobních údajů.

Pověřenec pro ochranu osobních údajů je jakýmsi svědomím správce. Jeho role má spočívat zejména v tom, že je na správci nezávislým rádcem pro oblast osobních údajů. Není tedy přímo odpovědný za stanovování účelu a prostředků při zpracování dat.

Ruší se oznamovací povinnost úřadu, která je nyní zakotvena v § 16 zákona o ochraně osobních údajů. Pokud tedy např. chce město zřídit kamerový systém, nemusí již tuto skutečnost oznamovat úřadu, musí ale posoudit vliv na ochranu osobních údajů.

9. Kdo potřebuje jmenovat pověřence?

Povinnost jmenovat pověřence je ve třech případech:

u soukromých subjektů:

1. pokud dochází ke zpracování osobních údajů, které vyžaduje rozsáhlé, pravidelné a systematické monitorování subjektu údajů (telefonní operátor)
2. činnost je zaměřena na rozsáhlé zpracování citlivých údajů

u veřejných subjektů:

3. je povinný pro orgány veřejné moci a „veřejné subjekty“ bez ohledu na rozsah zpracování
 - Zákon zužuje definici „veřejných subjektů“ tak, aby nedopadala např. na příspěvkové organizace či jiné pomocné instituce.
 - Zákon upřesňuje, že tato povinnost se vztahuje na instituce podobné orgánům veřejné moci, nikoli na příspěvkové organizace či jiné pomocné instituce.

Příklad: Jsem majitelem malé stavební společnosti. Vedu si seznam svých klientů, a to včetně jejich požadavků na dodávky. Rovněž si vedu osobní údaje o svých zaměstnancích. Musím mít pověřence pro ochranu osobních údajů?

Vzhledem k tomu, že hlavní činností stavební firmy není rozsáhlé zpracování citlivých údajů ani rozsáhlé, pravidelné a systematické monitorování subjektů údajů, nemusí mít pověřence pro ochranu osobních údajů.

10. Budou skutečně ukládány likvidační pokuty?

Horní hranice pokut je podle GDPR stanovena velmi vysoká aby se globálním technologickým firmám dlouhodobě nevyplácelo porušovat nebo obcházet pomocí malých firem. Pokuty jsou vždy ukládány s přihlédnutím na přiměřenost sankce stejně jako dosud. GDPR samo říká, že pokuty mají být odstrašující, nikoliv likvidační. Ostatně již ve stávajícím zákoně o ochraně osobních údajů jsou pokuty ve výši několika milionů. Likvidační pokuty ukládány být nesmějí, to by bylo protiústavní, což vyplývá i ze stávající judikatury jak správních soudů, tak Ústavního soudu.

Modelové příklady aplikace Obecného nařízení

Název: Osobní údaje uváděné na certifikátu o vzdělání

Popis situace vyžadující ochranu osobních údajů: Vzdělávací agentura v rámci prohlubování kvalifikace úředníků územních samosprávných celků uvádí na certifikátu pro účastníka jméno, příjmení, datum a místo narození. Je možné všechny tyto osobní údaje na certifikátu uvádět?

Řešení: Osobní údaje se na certifikát uvádějí proto, aby se zamezilo záměně osob při případné shodě jmen. Datum narození tedy může být údajem, který právě riziku záměny osob zamezí. Zpravidla je tento údaj postačující. Situace, kdy bude shodné datum narození, jméno i příjmení u účastníků téhož kurzu, pravděpodobně nenastane. V souladu s principem minimalizace zpracování osobních údajů na nezbytnou míru tedy již není důvod uvádět údaj o místě narození.

Název: Zveřejnění osobních údajů žadatele o informaci podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Popis situace vyžadující ochranu osobních údajů: Podle § 5 odst. 3 zákona č. 106/1999 Sb. povinný subjekt do 15 dnů od poskytnutí informací na žádost tyto informace zveřejní způsobem umožňujícím dálkový přístup. Má/může povinný subjekt při zveřejnění poskytnuté informace zveřejnit i osobní údaje žadatele o informaci?

Řešení: Při zveřejnění poskytnuté informace nesmějí být bez souhlasu žadatele – fyzické osoby zveřejněny jeho osobní údaje. Zveřejnění těchto údajů spolu s poskytnutou informací by bylo porušením práva na ochranu osobních údajů.

Podle § 14 odst. 2 zákona č. 106/1999 Sb. žadatel – fyzická osoba uvede v žádosti o poskytnutí informace jméno, příjmení, datum narození, adresu místa trvalého pobytu nebo, není-li přihlášen k trvalému pobytu, adresu bydliště a adresu pro doručování, liší-li se od adresy místa trvalého pobytu nebo bydliště. Povinný subjekt, který vyřizuje žádost o poskytnutí informace, je správcem těchto osobních údajů žadatele, tyto osobní údaje je však oprávněn zpracovávat pouze pro účely vyřízení žádosti o poskytnutí informace, nikoliv již pro účely zveřejnění těchto osobních údajů – podle § 5 odst. 3 zákona č. 106/1999 Sb. se zveřejňují poskytnuté informace, nikoliv údaje o žadateli.

Název: Zpracování osobních údajů obcí v souvislosti s životními jubilei občanů

Popis situace vyžadující ochranu osobních údajů: Starosta obce by rád poblahopřál k narozeninám občanům obce, kteří dosáhli významného životního jubilea (70 let). Je možné, aby obec pro tyto účely zjišťovala potřebné osobní údaje?

Řešení: Ano, zjišťování osobních údajů pro tento účel je možné. Podle ustanovení § 36a obecního zřízení obec může ocenit významné životní události svých občanů. I pro tento účel, který se nachází v působnosti obce, může obec v nezbytném rozsahu zjišťovat údaje ze základního registru obyvatel a dalších informačních systémů veřejné správy stanovených v § 149a obecního zřízení (mj. jméno a příjmení, datum narození a adresa místa trvalého pobytu). Pokud jde o možnost zveřejnit blahopřání v obecním zpravodaji, lze doporučit postup uvedený ve stanovisku Úřadu pro ochranu osobních údajů (srov. <https://www.uoou.cz/k-nbsp-blahoprani-jubilantum-obcemi/d-20337>):

„Úřad považuje za přípustné, jestliže jsou ve společenských rubrikách, např. „Blahopřejeme jubilantům naší obce“ nebo „Vítáme nové občanky naší obce“ v určitém měsíci i bez souhlasu zveřejněna pouze jména a příjmení bez jakýchkoliv dalších údajů. Pokud se obec pouze pro tuto formu ocenění významné životní události rozhodne, mělo by jít v případě blahopřání seniorům o významná životní jubilea, nikoli o každoroční zveřejňování jmen a příjmení v měsíci narození bez souhlasu jejich nositelů. K zveřejňování dalších údajů, např. věku, data narození, části obce, je však nutné, aby obec disponovala souhlasem subjektu údajů či zákonného zástupce.“

Název: Používání osobních údajů v obecních kronikách

Popis situace: Obec je podle zákona č. 132/2006 Sb., o kronikách obcí, povinna vést kroniku obce, do níž se zaznamenávají „zprávy o důležitých a pamětihodných událostech v obci pro informaci i poučení budoucím generacím“. Co může být v obecních kronikách uvedeno, aby nedošlo k porušení obecného nařízení o ochraně osobních údajů? Jak postupovat při zveřejnění kroniky na internetu?

Řešení: Účel vedení kroniky obce vyžaduje, aby v kronice byly uváděny osobní údaje. Jestliže za aktéry důležitých a pamětihodných událostí považujeme především lidi (nikoli jen přírodní živly), neobejde se kronika bez informací o lidech, kteří v kronikářově době žijí a konkrétně jednají. Je ovšem nutné mít na paměti, že kronika má sloužit pro informaci a poučení budoucím generacím, jde tedy o historický pramen, nikoli o „společenskou kroniku“. Na jedné straně z toho plyne využití některých speciálních ustanovení obecního nařízení o ochraně osobních údajů (například možnost zpracovávat osobní údaje o politických názorech pro účely historického výzkumu podle čl. 9 odst. 1 písm. j)), na druhou stranu nelze ospravedlnit jakýkoli

zásah do soukromí fyzické osoby. Lze tedy například uvést údaj o tom, že starosta obce vyjádřil podporu zahraniční politice prezidenta republiky při jeho návštěvě spojené se zprovozněním spojeneckého radaru, není však již přiměřené uvést, že z tohoto důvodu došlo v domácnosti starosty k ostré roztržce završené rozvodem, byť to je možná ještě zajímavější informace.

V obecních kronikách se pravidelně uvádějí zápisy o některých rodinných událostech, tyto záznamy však nesmí rozsahem uváděných osobních údajů zasahovat nepřiměřeným způsobem do soukromého života dotčených osob. Častým obsahem historických obecních kronik bývá zejména v malých obcích historie jednotlivých obydlí. Bývalo zvykem uvádět, kdo se kdy usadil na kterém gruntu, od koho jej nabyt nebo propachtoval, komu jej odkázal atd. Zřejmě ani dnes nic nebrání tomu uvést, že určitá nemovitost změnila vlastníka, a přiměřeně to zdokumentovat identifikací dřívějšího a nového majitele. Jako nepřiměřené by se již mohlo jevit uvedení údaje o kupní ceně (byť by ji kronikář zjistil zcela legálně z inzerátu realitní kanceláře). Podobně je potřeba pojímat s přiměřeností záznam o narození dětí – tedy lze uvést, že v tom a tom roce se narodily děti identifikované jménem a příjmením (lze případně i v souladu s tradicí uvádět, v kterém čísle popisném), není však již přiměřené uvádět konkrétní data narození, natožpak třeba údaje o zdravotním stavu.

V případě pochybností, zda určitý údaj lze v souladu s obecným nařízením o ochraně osobních údajů uvádět, lze doporučit, aby si kronikář opatřil souhlas subjektu údajů.

Pro úplnost se pak patří zdůraznit, že ochrana osobních údajů podle obecného nařízení se netýká zesnulých osob.

Velmi obecně formulovanou zákonnou povinností vést kroniku obce je tedy potřeba ve vztahu k čl. 6 odst. 1 písm. c) obecného nařízení vykládat s citem a se zřetelem k účelu stanovenému zákonem o kronikách obcí.

Pokud jde o zveřejnění kroniky na internetových stránkách obce, je nutné zdůraznit, že zákon obci zveřejňování kroniky na internetu neukládá. Na zpracování osobních údajů v kronice jejich zveřejněním na internetu tedy nelze použít důvod plnění právní povinnosti podle čl. 6 odst. 1 písm. c) obecného nařízení. Zveřejnění by bylo možné považovat za zpracování prováděné ve veřejném zájmu nebo pro účely oprávněných zájmů obce (prezentace obce navenek), zásada přiměřenosti zde však bude velet k anonymizování osobních údajů. V případě zveřejňování obecních kronik na internetu v zásadě nemusejí být anonymizována toliko jména osob, která jsou přiměřeně použita jako jména účastníků pamětihodných událostí obce a netýkají se soukromého života těchto osob.

Název: Osobní údaje na podpisové listině k návrhu na konání místního referenda – právo na výmaz

Popis situace vyžadující ochranu osobních údajů: Občan obce se podepsal na podpisovou listinu k návrhu na konání místního referenda o přesunutí místního autobusového nádraží. Následně si podpis rozmyslí a chce využít práva být zapomenut. Může požadovat po zmocněnci přípravného výboru a po obci, které byl doručen návrh na konání referenda s podpisovou listinou, aby jeho údaje z listiny vymazali?

Řešení: Rozsah osobních údajů, který je třeba uvést na podpisovou listinu k návrhu na konání místního referenda, je stanoven v § 11 odst. 2 zákona o místním referendu (jde o jméno, příjmení, datum narození, adresu a vlastnoruční podpis). Všechny tyto údaje je v souladu se zákonem třeba uvést, aby návrh přípravného výboru na konání místního referenda neobsahoval neúplné údaje a aby občanův podpis mohl být započítán do počtu podpisů nutných podle zákona ke konání místního referenda. Je zde tudíž dán zákonný titul pro zpracování osobních údajů, obec zpracovává osobní údaje při výkonu veřejné správy ve veřejném zájmu a zpracování osobních údajů ve veřejném zájmu lze shledat i na straně zmocněnce přípravného výboru. Údaje jsou nadále potřebné pro účely, ke kterým byly shromážděny (ať už pro účely konání referenda, nebo následně pro účely archivace), nejedná se o zpracování na základě souhlasu a údaje jsou zpracovávány oprávněně (srov. čl. 17 odst. 1 obecného nařízení o ochraně osobních údajů). Navíc se zde uplatní výjimka z práva být zapomenut stanovená v čl. 17 odst. 3 písm. b) – plnění právní povinnosti, plnění úkolu ve veřejném zájmu.

Občan – subjekt údajů zde tudíž nebude mít právo na výmaz svých údajů na podpisové listině.

Název: Osobní údaje dárce politické strany či hnutí uváděné ve výroční finanční zprávě – právo na výmaz

Popis situace vyžadující ochranu osobních údajů: Fyzická osoba uvedená jako dárce ve výroční finanční zprávě politické strany se domáhá výmazu osobních údajů z toho důvodu, že skutečným dárce byla obchodní společnost, jejímž je jednatelem.

Řešení: Politická strana či politické hnutí musí ve výroční finanční zprávě uvést podle § 19h odst. 1 písm. g) zákona č. 424/1991 Sb., o sdružování v politických stranách a v politických hnutích, přehled o dárcích a jejich darech s uvedením výše peněžitého daru a obvyklé ceny nepeněžitého daru, jména, příjmení a data narození; je-li dárce právnická osoba, uvede se její obchodní firma nebo název a identifikační číslo.

Pokud politická strana při vyplňování výroční finanční zprávy udělala chybu a místo právnické osoby, která byla dárce, uvedla jejího jednatele, má jednatel právo jako subjekt údajů na výmaz osobních údajů ve výroční zprávě podle čl. 17 odst. 1 písm. d) obecného nařízení o ochraně osobních údajů, neboť údaje byly zpracovány protiprávně. Toto právo má jak vůči politické straně, která je autorem výroční zprávy, tak vůči Úřadu pro dohled nad hospodařením politických stran a politických hnutí, jemuž jsou zprávy předávány a jenž je zveřejňuje na svých internetových stránkách.

Název: Rozsah práva na výmaz

Popis situace vyžadující ochranu osobních údajů: Správce byl požádán o výmaz všech osobních údajů, které o žadateli shromažďuje. Je povinen žádosti v plném rozsahu vyhovět?

Řešení: Na žádost je správce povinen odstranit údaje, které shromažďuje na základě souhlasu subjektu údajů. Nicméně to neplatí, pokud má správce povinnost uchovávat údaje na základě platných zákonů, např. účetních, daňových či pro archivační účely. Pokud tedy např. bývalý zaměstnanec požádá o výmaz veškerých údajů, které o něm jeho bývalý zaměstnavatel uchovává, je zaměstnavatel povinen smazat ty údaje, které nemusí uchovávat ze zákonných důvodů a k nimž mu dal souhlas zaměstnanec – např. osobní e-mail či telefonní číslo.

Název: Ohlašování porušení zabezpečení osobních údajů (čl. 33 obecného nařízení)

Popis situace vyžadující ochranu osobních údajů: Úředník obce potřeboval vypo-moci s přípravou správních rozhodnutí a chtěl zaslat kolegovi e-mailem seznam účastníků pěti správních řízení v rozsahu obecných identifikačních údajů účastníka řízení podle správního řádu. Omylem odeslal e-mail osobě mimo obecní úřad. Je potřeba do 72 hodin provést ohlášení tohoto případu Úřadu pro ochranu osobních údajů podle čl. 33 obecného nařízení o ochraně osobních údajů?

Řešení: Pochybení úředníka sice naplňuje znaky porušení zabezpečení osobních údajů, nicméně není pravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Údaje, které z úřadu unikly, nejsou způsobilé ke zneužití, které by mohlo subjektům údajů způsobit újmu, poškodit je na cti nebo ohrozit jiná jejich práva a svobody. Hlášení podle čl. 33 se tudíž neprovede. (Je však vhodné ohlásit toto pochybení pověřenci pro ochranu osobních údajů, aby mohl případ zadokumentovat podle čl. 33 odst. 5 obecného nařízení.)

Název: Posouzení vlivu na ochranu osobních údajů (čl. 35 obecného nařízení)

Popis situace vyžadující ochranu osobních údajů: Obec o 2000 obyvatelích hodlá pro občany zřídit informační SMS kanál. Prostřednictvím webové aplikace a v osobním kontaktu bude shromažďovat do databáze čísla mobilních telefonů občanů, kteří budou mít zájem dostávat informace o dění v obci SMS zprávami. Poskytování telefonních čísel bude dobrovolné a spojené se souhlasem subjektu údajů. Telefonní čísla nebudou přímo v databázi spojena s jinými osobními údaji občanů obce. Budou využívána pouze k hromadnému rozesílání SMS zpráv. Je potřeba provést posouzení vlivu na ochranu osobních údajů (tzv. DPIA)?

Řešení: Obcí zamýšlené zpracování osobních údajů nesplňuje znaky podle čl. 35 odst. 1 obecného nařízení o ochraně osobních údajů. Není totiž pravděpodobné, že daný „druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob“. Posouzení vlivu na ochranu osobních údajů ve smyslu čl. 35 obecného nařízení tudíž není potřeba provést.

Název: Možnost propuštění pověřence pro ochranu osobních údajů

Popis situace: Pověřenec pro ochranu osobních údajů, který je v pracovním poměru, opakovaně a dlouhodobě neplní své úkoly, neposkytuje správci vyžádané informace, odmítá poskytovat poradenství zaměstnancům, kteří provádějí zpracování, o povinnostech v souvislosti s právní úpravou ochrany osobních údajů, odmítá dodržovat stanovenou pracovní dobu s odůvodněním, že je nezávislý. Jakým způsobem lze tuto situaci řešit, když obecné nařízení o ochraně osobních údajů v čl. 38 odst. 3 uvádí, že pověřenec nesmí být v souvislosti s plněním svých úkolů správcem nebo zpracovatelem propuštěn ani sankcionován?

Řešení: Zákaz sankcionování či propuštění pověřence upravený obecným nařízením má za cíl posílit samostatné postavení pověřence a pomoci zajistit, aby pověřenec jednal nezávisle a požíval dostatečnou ochranu při plnění svých úkolů v oblasti ochrany osobních údajů.

Sankcionování či propuštění pověřence je obecným nařízením zapovězeno, jen pokud je následkem výkonu povinností pověřence. Například: pokud by pověřenec dospěl k názoru, že zpracovávání určitých osobních údajů zpracovatelem není účelné a není kryto žádným z právních titulů, a doporučil v tomto smyslu zpracovateli řešení této situace, se kterým by zpracovatel nesouhlasil, nebylo by možné v této souvislosti nesoulad názorů řešit tím, že by zpracovatel pověřence jakýmkoliv způsobem (přímým či nepřímým) sankcionoval, hrozil mu propuštěním, nebo ho dokonce skutečně propustil. Pověřenec však může být sankcionován nebo propu-

těn (stejně jako ostatní zaměstnanci) z důvodů jiných než v souvislosti s výkonem jeho povinností pověřence. Pokud pověřenec vůbec své povinnosti neplní, plní je prokazatelně nedostatečně či porušuje jiné povinnosti zaměstnance, které nemají přímou souvislost s výkonem funkce pověřence, způsobem, jenž je podle zákoníku práce důvodem ukončení pracovního poměru ze strany zaměstnavatele, je možné, aby byl pověřenec legitimně propuštěn. Je však třeba upozornit na to, že důkazní břemeno ohledně legitimního důvodu propuštění bude nést zaměstnavatel. Obdobně lze uvedené vztáhnout i na případ, kdy pověřenec plní své úkoly na základě smlouvy o poskytování služeb.

Cesta na dovolenou

Při objednávání cesty na dovolenou v zahraničí požaduje cestovní kancelář množství osobních údajů o každém účastníkovi. Musí mít jejich souhlas ke zpracování?

Nemusí mít souhlas, pokud údaje potřebuje k uzavření a splnění smlouvy (včetně případné rezervace letenky, vnitrostátní dopravy, hotelu, zajištění první lékařské pomoci atd.). Nemusí mít ani jejich souhlas s předáním údajů do zahraničí, pokud je to nutné pro plnění smlouvy.

Toto přece není osobní údaj!

Často není jasné, jaké údaje kromě jména, příjmení, data narození apod. se mají chránit. Pojem osobních údajů ale zůstává velmi široký a může zahrnovat i IP adresy, stejně jako zahrnuje různá evidenční čísla (RČ, SPZ). Postačí, pokud někdo (kdokoliv) dokáže pomocí takového údaje identifikovat člověka nebo pokud je údaj připojen k identifikované osobě. (Jde např. o situace „Karel Novák narozený 1.1.2000 má nemoc xy“.)

Správci a zpracovatelé musí jako doposud přihlídnout k širší pojmu „osobní údaje“.

Nápis na hrobě a úmrtní oznámení

Pozůstalí chtějí uvést jméno, příjmení a data narození a úmrtí zesnulého na náhrobku. Chtějí také vyvěsit oznámení o úmrtí a pozvánku na obřad v místě bydliště a na bývalém pracovišti. Jaké povinnosti mají?

GDPR se na osobní údaje zesnulých osob nevztahuje, žádné zvláštní povinnosti pozůstalí nemají. (Čest a důstojnost zesnulého dále chrání občanský zákoník, ochrany jeho osobnosti se mohou domáhat jemu blízké osoby.) Údaje o jiných lidech (manžel, rodina) se uvádějí podle jejich souhlasu.

Jak dlouho budou moje osobní údaje uloženy?

Často není jasné, jak dlouho bude nějaký podnik nebo úřad zpracovávat osobní údaje. Musí být doba uložení osobních údajů pevně stanovena?

Nemusí. Úřad zpravidla používá osobní údaje tak dlouho, jak podle zákona má, a po vyřešení věci začne běžet několikaletá skartační lhůta. Jinak záleží na situaci a na tom, k čemu správce osobní údaje potřebuje. Každý člověk má ale právo se na předpokládanou dobu uložení údajů správce zeptat.