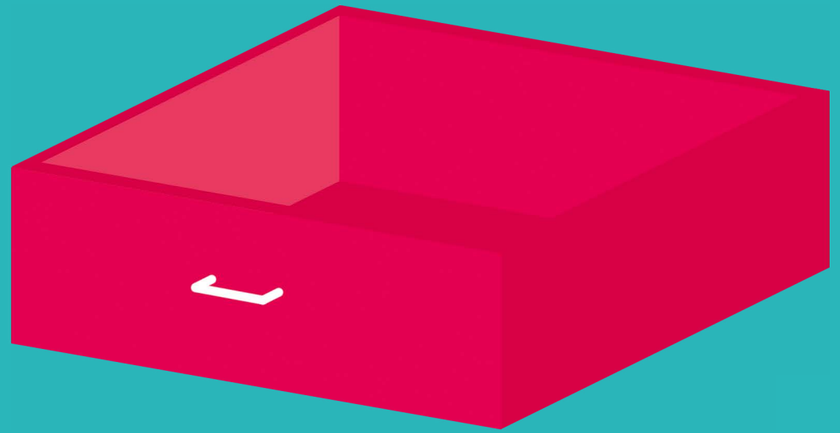
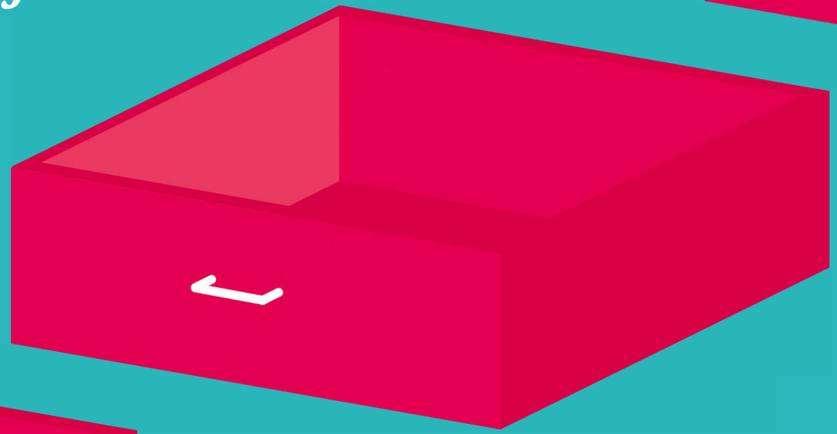
Ochrana osobních údajů (nejen) pro nevládní organizace

Iuridicum Remedium
2016

Dostupný z http://www.nusl.cz/ntk/nusl-204279

Ochrana osobních údajů...





...(nejen) pro nevládní organizace

Vznik této publikace byl podpořen grantem z Islandu, Lichtenštejnska a Norska v rámci EHP fondů. www.fondnno.cz a www.eeagrants.cz

DATA? TADÁ!

Proč by se nevládní organizace měly zabývat problematikou ochrany osobních údajů a k čemu může posloužit tato příručka?

Nevládní organizace obvykle vznikají ze zápalu pro řešení nějakého problému a mají své jasné cíle. Může to být náprava poměrů na místní radnici, proměna veřejného prostoru nebo třeba snaha pomoci nějaké ohrožené skupině lidí. Nevládní organizace jsou ovšem obvykle také právnickými osobami, nejčastěji spolky, obecně prospěšnými společnostmi, ústavy a podobně, které musí plnit řadu dalších povinností, které s jejich hlavními cíli úplně nesouvisí.

Takovou oblastí může být i ochrana osobních údajů. A to ať už údajů členů, zaměstnanců nebo klientů. Povinnosti chránit osobní údaje jsou dnes již nedílnou součástí činnosti jak soukromých firem, správních či samosprávných orgánů, tak i nevládních organizací. Nedodržování pravidel v této oblasti může mít i pro nevládní organizace vážné důsledky v podobě finančních postihů, ztráty prestiže nebo důvěry klientů.

Cílem této příručky je poskytnout nevládním organizacím nejrůznějšího druhu praktického a srozumitelného průvodce složitou problematikou ochrany osobních údajů. Příručka je vydána jako jeden z výstupů projektu Zvyšování know-how nevládních organizací při sdílení, šíření a ochraně informací *podpořeného grantem z Islandu, Lichtenštejnska a Norska v rámci EHP fondů. Jeho součástí bylo i uspořádání několika workshopů pro nevládní organizace a advokátní a IT poradenství v oblasti ochrany osobních údajů. Pro nás tato setkání s lidmi z jiných nevládních organizací byla důležitá v tom, že jsme zjišťovali, s jakými problémy se nejčastěji setkávají, co je pálí a v jakém směru bychom jim mohli být, jakožto organizace, která se ochraně soukromí věnuje již řadu let, nápomocni.*

Chceme poskytnout jak teoretický základ pro pochopení hlavních pravidel, která pro nakládání s osobními údaji platí, tak přinést praktické rady v oblastech, s nimiž se nevládní organizace setkávají častěji. Příručka není a ani nemůže být vyčerpávajícím přehledem. Na některé oblasti, jako je třeba složitá problematika předávání osobních údajů do zahraničí, se nám už nedostávalo prostoru. Pokud tedy řešíte konkrétní problém, vždy doporučujeme stejně nahlédnout do zákona (proto uvádíme v textu odkazy na příslušné paragrafy), do komentáře k zákonu, do literatury nebo třeba do stanovisek Úřadu pro ochranu osobních údajů na stránkách www.uoou.cz. Možné je také využít naší internetové poradny na www.slidilove.cz.

Naším cílem bylo shrnout přístupným způsobem, jaké povinnosti by nevládní organizace měly plnit a jak by tak měly činit, aby vše odpovídalo zákonu. Důležité ale je také to, aby je zároveň agenda ochrany osobních údajů co nejméně zatěžovala a ubírala čas, chuť i peníze na to, čemu se nevládní organizace a lidé v nich chtějí věnovat především.

Jan Vobořil

Iuridicum Remedium, z.s., únor 2016

Co je to vlastně osobní údaj?

U ochrany osobních údajů platí jeden paradox. Čím více se ponoříte do problematiky ochrany osobních údajů, tím méně si jste jistí, co všechno lze za osobní údaj považovat, a co už ne. Podle zákona o ochraně osobních údajů je **osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů**. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu (§ 4 písm. a) ZOOÚ).

Plná identita fyzické osoby (právnické osoby osobní údaje nemají) v současných podmínkách technologicky vyspělé společnosti ve své podstatě neznamená nic jiného, než možnost tuto osobu určitým způsobem **odlišit** od ostatních osob a **kontaktovat** ji, aniž by bylo nutno znát místo jejího aktuálního pobytu. Osobním údajem tak může být e-mailová schránka, pokud nejde například o schránku, k níž má přístup více osob. Může jít i o samotné číslo mobilního telefonu, který obvykle používá jediný člověk.

Při hodnocení toho, jestli něco je nebo není osobní údaj, záleží nejen na tom, jaké údaje o daném člověku aktuálně máme, ale i na tom, k jakým se můžeme legálně dostat například na internetu. Pokud třeba máme k dispozici nějaké jedinečné jméno a žádný další údaj, může se jednat o osobní údaj v případě, že ke jménu doplníte kontaktní adresu ze živnostenského rejstříku nebo ze sociálních sítí. Nemusí jít přitom nutně o adresu trvalého pobytu, ale třeba o e-mail, telefon nebo adresu zaměstnavatele.

Jestliže máme například údaj o datu narození, pak bude tento údaj jistě osobním údajem pro toho, kdo má toto datum propojeno se jménem a adresou daného člověka. Pokud ale někdo povede třeba z důvodu výzkumu databázi lidí, které bude řadit podle data narození, ale na základě souboru dalších údajů nebude možno danou osobu identifikovat, nebude se jednat o osobní údaj a ani přiřazené informace nebudou osobními údaji.

Závěrem je tedy třeba říci, že to jestli něco je nebo není osobní údaj, je nezbytné hodnotit v souvislostech. Často záleží na tom, jaké další údaje o dané osobě máme, k jakým dalším údajům se můžeme potenciálně a legálně dostat. A jestli nám tento soubor informací umožní osobu odlišit od jiné osoby a zda jsme zároveň schopni ji kontaktovat.

Co je to citlivý údaj?

Citlivé údaje jsou zvláštní kategorií osobních údajů, jejichž zpracování podléhá přísnějším pravidlům. Zákon k tomu říká, že jde o „údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“(§ 4 písm. b) ZOOÚ)

Oproti osobním údajům, které nejsou citlivé, obsahuje zákon rozdíly, zejména pokud jde o právní titul zpracování, ať už jde o souhlas, kde musí jít o souhlas výslovný nebo o jinak uspořádané výjimky, kdy lze citlivé údaje zpracovávat i bez souhlasu.

Kdy se je potřeba řídit zákonem o ochraně osobních údajů a co je to zpracování?

Zákon o ochraně osobních údajů platí pro všechny, byť s řadou odchylek obsažených v samotném zákoně nebo ve zvláštních právních předpisech. Základní podmínkou ale je, aby dotyčný subjekt údaje zpracovával.

Pro pochopení problematiky ochrany osobních údajů je nejprve potřeba si říci, co vlastně je **zpracování osobních údajů**. Jde v podstatě o **jakoukoli operaci**, kterou správce nebo zpracovatel osobních údajů provádí **systematicky** s osobními údaji. Zejména tedy půjde o jejich shromažďování, ukládání na nosiče informací, zpřístupňování, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměnu, třídění nebo kombinování, blokování a nakonec i likvidaci (viz § 4 písm. e) ZOOÚ).

Systematicky prováděnou činností bude zejména tvorba různých databází a rejstříků, které umožňují s osobními údaji dále pracovat. V praxi v podstatě jakékoli automatizované zpracování, které například umožňuje vyhledávání jednotlivých údajů, bude zpracováním osobních údajů. Systematické může být i zpracování údajů například od jediné osoby (např. jediného žadatele o zaměstnání) pokud je například dále uchováván jeho životopis za účelem vedení přijímacího řízení.

Pokud máte informace, které lze označit jako osobní údaje, tak to ještě nutně neznamená, že musíte plnit všechny povinnosti obsažené v zákoně o ochraně osobních údajů. **Zákon se předně nevztahuje na zpracování osobních údajů fyzickou osobou pro svoji potřebu**. To ovšem nebude zpravidla dopadat na údaje zpracovávané nevládními organizacemi, které jsou právnickými osobami.

Naopak i nevládních organizací se může týkat druhá výjimka, která říká, že se zákonem neřídí **nahodilé shromažďování osobních údajů**, pokud pak není dále zpracováváno. Mohou totiž nastat situace, kdy jsou shromážděny osobní údaje nahodile a nikoli z iniciativy správce. Správce zároveň nemá zájem tyto údaje dále zpracovávat. Může jít třeba o zaslání nevyžádané pošty obsahující osobní údaje nebo o případ uchovávání profesního životopisu, který obsahuje i zcela nadbytečné informace, které o sobě žadatel o zaměstnání sdělil.

Kdo je to správce a kdo zpracovatel?

Jde o další dva důležité pojmy. Roli správce a zpracovatele je třeba rozklíčovat zejména z toho důvodu, že se od toho odvíjí to, kdo má plnit jaké povinnosti. **Správce** je ten, kdo určuje účel a prostředky zpracování osobních údajů. Toto zpracování také zpravidla provádí. Některými úkoly nebo i celým zpracováním ale může pověřit **zpracovatele**. Případně toto pověření může vyplývat přímo ze zákona. Pokud správce zpracovatele pověří, musí spolu uzavřít písemnou smlouvu o zpracování osobních údajů, která vymezuje vzájemná práva a povinnosti. Zpracovatel na rozdíl od správce například nemusí plnit zákonnou informační povinnost při zpracování osobních údajů, podobně neodpovídá ani za to, jestli bylo zpracování zaregistrováno.

Zpracovatelem tak bude třeba provozovatel serveru, na němž je uložena klientská databáze, externí účetní, který pracuje s osobními údaji dárců nebo společnost, která zajišťuje skartaci klientských spisů.

Lze využívat cloudová úložiště pro uchovávání klientské databáze?

Obecně ano, ale je nezbytné, aby správce vyhodnotil veškerá rizika, protože případný únik dat z cloudu bude nejen problémem zpracovatele, ale zejména správce, který tím poruší povinnost osobní údaje zabezpečit proti neoprávněnému přístupu. Je vhodné přijmout opatření, jako je šifrování uložených dat. Je také nezbytné uzavřít smlouvu o zpracování osobních údajů, která bude garantovat zabezpečení dat. Vhodné je volit cloudové služby v zemích EU, kam mohou být data bez dalšího předávána.

Kdy je potřeba souhlas a jak by měl vypadat?

Jednou z nejdůležitějších povinností správce je mít ke zpracování osobních údajů právní titul. Nejčastěji jím bude souhlas, v řadě případů ale souhlas potřebovat nebudete. Jak by souhlas se zpracováním osobních údajů měl vlastně vypadat?

U běžných osobních údajů není forma souhlasu stanovena. Můžete ho mít tedy písemně, ústně anebo ho třeba můžete udělit i mlčky. Pokud vám třeba někdo podá občanský průkaz a je zřejmé, že kvůli tomu, abyste si z nějakého důvodu opsali jeho osobní údaje, jedná se právě o takový souhlas udělený mlčky. Naopak v případě citlivých údajů musí být souhlas udělen výslovně.

Vzhledem k tomu, že ten kdo osobní údaje zpracovává je případně povinen udělení souhlasu prokazovat, tak lze – samozřejmě s výjimkou případů, kdy to nedává smysl a zpracování osobních údajů by to neúnosně komplikovalo – doporučit písemnou formu.

Souhlas dále musí být informovaný. Nestačí tedy, že vám někdo podepíše nějaký papír, ale musíte také prokázat, že v době podpisu znal základní parametry zpracování osobních údajů a měl tak možnost se svobodně rozhodnout, jestli souhlas udělí, nebo nikoli. To souvisí i s plněním informační povinnosti.

Je možné souhlas se zpracováním osobních údajů odvolat?

Ano, odvolání souhlasu je možné. I z toho důvodu je vhodné nežádat souhlas v případech, kdy lze údaje zpracovávat na základě nějaké zákonné výjimky. Typicky se takto chybuje například ve smlouvách, kdy je souhlas se zpracováním osobních údajů nadbytečný, protože údaje je možno zpracovávat z důvodu zajištění plnění smluvních povinností v souladu s výjimkou dle § 5 odst. 2 písm. b) ZOOÚ. Pokud je zároveň vyžadován souhlas, tak v případě jeho odvolání může zbytečně dojít k nejasnostem, zda lze nebo nelze údaje dále zpracovávat.

I když je ale souhlas základním kamenem většiny zpracování osobních údajů, existuje řada výjimek, kdy souhlas není potřeba. Jedná se o tyto výjimky, kdy **souhlas nepotřebujete**:

1

Jestliže provádíte zpracování nezbytné pro dodržení právní povinnosti správce
To jsou hlavně případy, kdy vám zpracování ukládá nějaký zvláštní zákon. V praxi nevládních organizací může jít třeba o zákon o sociálních službách a údaje o kontaktech s klienty těchto služeb.

2

Jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,
Jakožto účastník smlouvy samozřejmě máte právo uchovávat údaje o svém smluvním partnerovi. Na základě této výjimky můžete například uchovávat smlouvy, faktury apod.

3

Pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,
Může se jednat třeba o případ, kdy sdělujete základní údaje o klientovi, který zkolaboval, lékaři.

4

Jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,
Se zpracováním údajů na základě této výjimky se setkáte relativně často. Půjde o osobní údaje zveřejněné například v tisku, ve veřejných rejstřících, nebo o údaje, které o sobě zveřejňují lidé v otevřených profilech na sociálních sítích. Důležité je, aby šlo o údaje zveřejněné v souladu s právem a nikoli například o jejich nelegální únik.

Budeme potřebovat souhlas, pokud chceme rozesílat žádosti o finanční příspěvek na adresy získané z telefonního seznamu?

Adresy zveřejněné v telefonním seznamu jsou zveřejněny na základě zákona. K využití těchto oprávněně zveřejněných adres k zasílání žádosti tedy nebude potřeba souhlas dané osoby, protože se budete řídit výjimkou dle § 5 odst. 2 písm. d) ZOOÚ. Zákon to sice neukládá, ale je určitě vhodné do dopisu napsat, jak by měl adresát postupovat, pokud napříště nechce od vás dostávat nevyžádanou poštu.

5

Pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,
O tuto výjimku správci opírají zpracování velmi často zejména v případě různých bezpečnostních opatření, jako jsou třeba kamerové systémy. Stejně jako u předchozí výjimky je ale potřeba vždy vážit zásah do soukromí s účelem, pro nějž údaje shromažďujete a dále zpracováváte.

6

Pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení,
Podle judikatury mezi údaje pokryté touto výjimkou bude patřit, vedle jména a kontaktních údajů, zejména funkční zařazení dané osoby, počty zpracovávaných případů, projektů či rozhodnutí. I zde je potřeba vážit veřejný zájem se zájmem na ochranu soukromí. To v praxi platí třeba u zveřejňování fotografií těchto osob bez jejich souhlasu.

7

Jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.
Tímto zvláštním zákonem bude zákon o archivnictví.

Právní titul pro zpracování osobních údajů je upraven v § 5 odst. 2 ZOOÚ. Pokud ale zpracováváme citlivé osobní údaje, je nezbytné vycházet z výjimek upravených v § 9 ZOOÚ, které se od obecné úpravy částečně liší.

Jaké další základní povinnosti je třeba dodržovat?

Různé povinnosti při zpracování osobních údajů najdete v řadě paragrafů napříč zákonem o ochraně osobních údajů. Některé z nich musí dodržovat pouze správce, jiné správce i zpracovatel. Do druhé skupiny patří povinnosti uvedené v § 5 odst. 1 ZOOÚ:

1

Stanovit účel, k němuž mají být osobní údaje zpracovány (§ 5 odst. 1 písm. a) ZOOÚ)
Stanovení účelu by mělo stát na začátku každého zpracování osobních údajů. Před činností si ujasněte cíl. Pouze tak lze nastavit správně pravidla pro zpracování osobních údajů.

2

Stanovit prostředky a způsob zpracování osobních údajů, (§ 5 odst. 1 písm. b) ZOOÚ)
Další povinností je určit, jakým způsobem budete osobní údaje zpracovávat a jaké prostředky k tomu využijete. Například k vedení adresáře kontaktů na příznivce organizace lze využít jak papírové adresáře, tak tabulky vytvořené na počítači, které mohou být uloženy buď na lokálním disku nebo v tzv. cloudu, který umožňuje i přístup prostřednictvím internetu. Nakonec lze využít i různé sofistikovanější programy, v nichž lze kontakty různým způsobem třídit a například zautomatizovat komunikaci s nimi.

Jak má v praxi vypadat stanovení účelu? Máme ho popsat v nějakém interním dokumentu?

Zákon obecně neukládá povinnost popsat účel zpracování někde písemně. Je ale pravda, že od samého počátku je s účelem operováno. Pokud je například nutné registrovat zpracování osobních údajů, je nutné účel uvést v oznámení. Podobně je nezbytné, aby účel byl součástí souhlasu se zpracováním osobních údajů nebo abychom ho uvedli při plnění informační povinnosti vůči subjektu údajů. Může být tedy přínosné sepsat interní pravidla pro dané zpracování osobních údajů a součástí těchto pravidel by pak měl být i popis účelu.

3

Zpracovat pouze přesné osobní údaje. Údaje aktualizovat, doplňovat nebo likvidovat pokud nejsou přesné. (§ 5 odst. 1 písm. c) ZOOÚ)
Tato povinnost správce neznamená, že by údaje měly být vždy zcela přesné, ale správce by měl mít nastavený mechanismus jejich aktualizace a kontroly. Podoba takového mechanismu bude záviset na účelu zpracování osobních údajů. V praxi nevládních organizací pracujících s klienty by třeba mělo být pravidlem zeptat se při každém kontaktu, zda se nezměnily kontaktní údaje apod.

4

Shromažďovat pouze údaje odpovídající stanovenému účelu a v rozsahu nezbytném k jeho naplnění.(§5 odst. 1 písm. d) ZOOÚ)
Každý správce by měl mít vždy na paměti účel zpracování osobních údajů. Od toho se odvíjí nastavení zpracování. Pokud třeba potřebujete udělat statistiku klientů podle věku, nepotřebujete znát jejich přesné datum narození, neřkuli dokonce rodné číslo nebo údaj o místě bydliště.

Provozujeme nízkoprahové zařízení pro uživatele drog. Z důvodu bezpečnosti našich zaměstnanců zde chceme instalovat kamerový systém. Na co si máme dát pozor?

V podobných zařízeních jistě může docházet ke konfliktům a případně i k napadení zaměstnanců. Předně je nutné si říci, že kamerový systém velmi pravděpodobně podobným incidentům nezabrání. Význam kamer ale už může být při potřebě identifikace útočníka. Pokud vezmeme v úvahu povinnost nastavit systém tak, aby shromažďoval minimum osobních údajů vzhledem ke stanovenému účelu, tak v daném případě bude účelné instalovat kameru sledující vchod do zařízení. Naopak instalace kamer v poradenských místnostech by tento účel zřejmě překračovalo a znamenalo by nejen nepřiměřené sledování klientů, ale i zaměstnanců. Pamatovat je třeba i na informování o instalaci kamerového systému, například textem „Prostor je sledován kamerovým systémem se záznamem“ spolu s identifikací správce a uvedením kontaktních údajů na osobu zodpovědnou za provoz systému. S provozováním takového systému je spojena i povinnost jeho registrace u ÚOOÚ.

Vedeme databázi našich dobrovolníků. Můžeme uchovávat i údaje o jejich zaměstnavateli?

Předně je nutné určit účel, proč tyto údaje je nezbytné vést. U registru dobrovolníků bude účelem zajištění efektivní spolupráce a jejich zapojení do činnosti organizace. Pro tento účel budou relevantní informace, jaké kompetence dobrovolník má a s čím a v jakém rozsahu může organizaci pomoci. Naopak informace o jeho zaměstnavateli nezbytná pravděpodobně nebude a její zpracování - a to i v případě, kdy by k tomu dobrovolník dal souhlas - bude zřejmě v rozporu s povinností uchovávat údaje pouze v rozsahu nezbytném k naplnění účelu zpracování.

5

Uchovávat osobní údaje pouze po dobu, která odpovídá stanovenému účelu. (§5 odst. 1 písm. e) ZOOÚ)
Stejně jako je třeba minimalizovat rozsah uchovávaných osobních údajů, je nutné minimalizovat, s ohledem na stanovený účel, i dobu zpracování. Jestliže například vedete evidenci osob, které hodláte pozvat na určitou akci, tak po této akci už další vedení této evidence ztrácí smysl, pokud není účelem třeba i informování o dalších akcích v budoucnu.

6

Zpracovávat údaje pouze k účelům, k nimž byly shromážděny (§5 odst. 1 písm. f) ZOOÚ)
Účel zpracování osobních údajů by se neměl měnit za pochodu. Z tohoto pravidla nicméně existují i výjimky týkající se například nabídky obchodu či služeb, kdy lze využít kontaktní údaje k zasílání obchodních nabídek, pokud byly získány v souvislosti s jinou činností nebo z veřejných rejstříků (§ 5 odst. 4 ZOOÚ). Výjimkou také mohou být pravidla upravená v dalších zákonech. Pokud třeba plníte zákonnou oznamovací povinnost u některých trestných činů, kterých se dopustili vaši klienti, sdělujete i údaje původně shromážděné k jiným účelům.

7

Shromažďovat osobní údaje pouze otevřeně (§5 odst. 1 písm. g) ZOOÚ)
Zpracování osobních údajů by mělo být pro ty, s jejichž osobními údaji nakládáte, vždy transparentní. Předstírání jiného účelu při shromažďování osobních údajů, než je účel skutečný, bude v rozporu se zákonem.

8

Nesdružovat osobní údaje, které byly získány k rozdílným účelům. (§5 odst. 1 písm. h) ZOOÚ)
Správce také nesmí sdružovat údaje shromážděné k různým účelům. To se týká například propojování údajů o jednotlivcích z dvou databází vedených k různým účelům.

Vedeme databázi našich dárců a zároveň databázi našich klientů. Rádi bychom zjistili, kdo z klientů nám zároveň přispívá na provoz, abychom mu poskytli nadstandardní služby. Je propojení těchto databází možné?

Účely vedení obou databází jsou zjevně odlišné. V případě klientů půjde o účel efektivního poskytování dané služby, naopak u dárců bude účelem třeba zaslání potvrzení o přijetí daru pro daňové účely nebo zaslání poděkování, výroční zprávy, či pozvánky na akce organizace. Propojení obou databází by tedy došlo ke spojení údajů zpracovávaných k různým účelům, což zákon zakazuje. Důležité je také to, že toto propojování údajů získaných k různým účelům není možné ani s dodatečným souhlasem subjektů údajů.

Jak a vůči komu plnit informační povinnost?

Plnění informační povinnosti je upraveno zejména v § 11 a § 12 ZOOÚ. Cílem této úpravy je zajistit transparentnost zpracování osobních údajů vůči těm, o jejichž údaje se jedná. Správce, nebo v případě pověření správcem i zpracovatel, mají obecně povinnost, už při shromažďování osobních údajů, **informovat subjekt údajů**, tj. sdělit tomu, koho se osobní údaje týkají (§ 11 odst. 1 ZOOÚ):

1. v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány,
2. kdo a jakým způsobem je bude zpracovávat,
3. komu mohou být zpřístupněny.

Současně musí být dotyčný informován i o právech přístupu k osobním údajům, právu na opravu, vysvětlení a nápravu nezákonností při zpracování osobních údajů.

Pokud jsou údaje shromažďovány od subjektu údajů, je nutné uvést, zda je poskytnutí údajů dobrovolné nebo zda je uloženo zákonem a co v případě odmítnutí hrozí.

I zde jsou výjimky, kdy informační povinnost **není potřeba plnit**:

1. Subjektu údajů jsou už tyto informace známy,
2. Zpracování osobních údajů ukládá zvláštní zákon
3. Osobní údaje je nezbytné zpracovávat z důvodu plnění povinností nebo uplatnění práv vyplývajících ze zvláštního zákona
4. Jsou zpracovávány výlučně oprávněně zveřejněné osobní údaje
5. Zpracovávají se údaje se souhlasem subjektu údajů. Vzhledem k tomu, že souhlas musí být informovaný, tak je stejně nezbytné informaci poskytnout.
6. Výjimky v oblasti statistického zpracování, vědecké a archivní účely

Musím informovat protistranu, když o ní shromažďuji osobní údaje, abych mohla žádat u soudu náhradu škody, kterou mi dotyčný způsobil?

V případě, že jsou údaje zpracovávány za účelem uplatnění práva na náhradu škody u soudu, nemusí se plnit informační povinnost v souladu s výjimkou uvedenou v § 11 odst. 3 písm. b) ZOOÚ, protože se jedná o shromažďování údajů za účelem uplatnění práva stanoveného zvláštním zákonem.

Vedle povinnosti aktivně informovat je správce také **povinen sdělovat informace na vyžádání** (§ 12 ZOOÚ).

Při vyžádání informace o zpracování osobních údajů by měl správce bez zbytečného odkladu sdělit subjektu údajů informace v rozsahu podobném jako v případě § 11 ZOOÚ. Pro správce je důležité vědět, že za poskytnutí takové informace může požadovat přiměřenou úhradu. Půjde například o náklady na zhotovení kopií, datové nosiče, poštovné. U manuálního zpracování osobních údajů může teoreticky jít i o náklady na osoby, které musely informace vyhledat. V případě automatizovaných zpracování, kde lze údaje vyhledat prakticky okamžitě, ale takové náklady nebude možno účtovat. Nutno je také zdůraznit, že poskytnutí informace nelze podmiňovat zaplacením této úhrady.

Kdy je/není potřeba zpracování registrovat na ÚOOÚ?

Další povinností, kterou je třeba plnit, je povinnost registrace zpracování osobních údajů u Úřadu pro ochranu osobních údajů (§ 16 ZOOÚ). Tato povinnost se vztahuje na všechny případy zpracování osobních údajů s třemi výjimkami (§ 18 odst. 1 ZOOÚ). **Registrovat není třeba**:

1

Zpracování osobních údajů, které jsou součástí datových souborů veřejně přístupných na základě zvláštního zákona.
Tuto výjimku, přes poněkud problematickou formulaci, je nutné chápat tak, že se vztahuje na oprávněně zveřejněné osobní údaje. Nepůjde tedy například jen o údaje z veřejných rejstříků, ale i o osobní údaje zveřejněné v přiměřeném rozsahu tiskem nebo o údaje, které o sobě zveřejňují přímo subjekty údajů. (k tomu viz Kučerová a kol., Zákon o ochraně osobních údajů – Komentář, Praha 2012, s. 268)

2

Zpracování osobních údajů, které správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona.
Sem patří stejné případy, u nichž platí výjimka z informační povinnosti. Vedle případů, kdy správce plní nějakou povinnost uloženou zákonem, půjde i o případy, kdy je zpracování nezbytné k tomu, aby například mohl uplatnit nějaké právo v rámci soudních nebo správních řízení.

Provozujeme ústav pro mentálně postižené, je nutné provést registraci zpracování osobních údajů klientů u Úřadu pro ochranu osobních údajů?

Záleží na tom, jaké údaje jsou o klientech zpracovávány. Pokud jde o rozsah údajů, jejichž zpracování ukládá například zákon o zdravotních službách, pak toto není nutné u úřadu registrovat. Pokud by ale například z bezpečnostních důvodů ústav instaloval kamerový systém se záznamem, tak se nejedná o plnění zákonné povinnosti a je na místě provést registraci.

3

Zpracování osobních údajů, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti sdružení, a které se týká pouze členů sdružení, nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení.
Tato výjimka z registrační povinnosti se týká například politických stran, náboženských spolků nebo odborových organizací. Zpracování by se mělo týkat členů nebo osob, s nimiž je daná organizace v opakujícím se kontaktu (např. pravidelní dárci). Zároveň musí být splněna podmínka, že osobní údaje nesmí být zpřístupňovány bez souhlasu subjektu údajů. Pokud tedy správce údaje zpřístupňuje a není zde nějaká jiná výjimka, je nezbytné zpracování registrovat.

Postup registrace je rozveden na stránkách Úřadu pro ochranu osobních údajů (www.uoou.cz). Začít se zpracováním osobních údajů lze buď zařazením oznámení do registru, nebo po uplynutí 30 ti denní lhůty, v níž může ÚOOÚ vyzvat k doplnění registrace nebo zahájit řízení, v němž prověří zákonnost oznamovaného zpracování. Zaslání a zpracování oznámení je zdarma.

Jak lze registrovat zpracování osobních údajů?

Podat oznámení o zpracování je možné zasláním vyplněného formuláře ve formátu pdf datovou schránkou nebo e-mailem s elektronickým podpisem. Možné je také zaslání vytištěného a ručně vyplněného formuláře poštou nebo oznámení podat bez použití formuláře.

Jak zabezpečit osobní údaje proti úniku?

DATA ATAK

Povinnost chránit údaje

Jedny z nejdůležitějších povinností, které je potřeba při zpracování osobních údajů plnit, souvisí se zabezpečením osobních údajů.

Údaje musí být chráněny před neoprávněným nebo nahodilým přístupem třetích osob (§ 13 odst. 1 ZOOÚ). Ať už jde o jakýkoli způsob zpracování, je tedy klíčové zajistit, aby přístup k osobním údajům měly jen oprávněné osoby, jen v rozsahu, který odpovídá jejich oprávnění a zejména v případě počítačového zpracování je nezbytné zajistit evidenci přístupů k osobním údajům (logování).

Jaké nastavení zabezpečení počítačového systému vyžaduje zákon, pokud v počítači vedeme klientské spisy s citlivými údaji?

Zákon nedává jasný návod, jak konkrétně mají být data zabezpečena. Ačkoli to klade na správce a zpracovatele vyšší nároky, tak je toto řešení logické, protože zákon nemůže dostatečně efektivně reagovat na rychlý vývoj technologií. Zabezpečení údajů tedy musí být správcem i zpracovatelem nastaveno tak, aby nedošlo k nežádoucí změně, zničení, ztrátě, či k přístupu neoprávněné osoby k osobním údajům. Pokud tedy k něčemu takovému dojde, je zřejmé, že správce či zpracovatel porušili zákon.

Při rozhodování se o tom, jak zabezpečit konkrétní zpracování osobních údajů, by se měla brát v úvahu zejména tato rizika:

1. Riziko, že se k osobním údajům dostane **neoprávněně třetí osoba nepůsobící v organizaci**. Toto se může stát buď úmyslně (např. krádež klientských spisů) nebo i neúmyslně (např. ztráta spisů mimo kancelář).
2. Riziko, že se k osobním údajům dostane **neoprávněně osoba pracující v organizaci** (např. ke klientským spisům se dostane uklízečka).
3. Riziko, že **osoba, která má k údajům přístup, nakládá s údaji v rozporu se zákonem**. Může jít třeba o uveřejnění klientské databáze na internetu ve snaze zdiskreditovat zaměstnavatele, nebo prodej klientské databáze za účelem neoprávněného finančního zisku. Může jít ale třeba i o případy, kdy je porušena povinnost mlčenlivosti a údaje jsou neoprávněně poskytnuty na vyžádání státním orgánům (např. policii) nebo třeba rodinným příslušníkům, aniž by k tomu byly splněny zákonné předpoklady.

Zabezpečení je nezbytné dokumentovat například v interních směrnicích organizací. Vedle zvážení rizik, by v nich mělo být zachyceno, jaká bezpečnostní opatření jsou přijata, ale i kdo za co odpovídá, kdo má k jakým osobním údajům přístup a kdo dodržování pravidel bude kontrolovat (§ 13 odst. 2 ZOOÚ).

Zaměstnanec naší organizace si vzal domů na prostudování klientský spis a zapomněl ho v autobuse. Hrozí nám za to nějaký postih?

Jedná se o porušení § 13 odst. 1 ZOOÚ ze strany organizace. V daném případě organizace nepřijala taková opatření, aby nedošlo ke ztrátě klientského spisu. Zejména by připadal v úvahu zákaz odnášení klientských spisů mimo kancelář. Pokud jde o případný postih, tak by rovněž záleželo na tom, jestli zaměstnanec jednal v rozporu s vnitřními předpisy a jestli dodržování těchto předpisů bylo ze strany organizace kontrolováno. Každopádně organizaci hrozí za správní delikt podle § 45 odst. 1 písm. h) ZOOÚ teoreticky pokuta až do výše 5 milionů korun.

Zpracování osobních údajů může být prováděno buď manuálně, nebo prostřednictvím výpočetní techniky. U manuálního zpracování – např. papírové klientské spisy – je nezbytné zejména zajistit, aby ke spisům měly přístup pouze osoby, které jsou k tomu podle interních pravidel oprávněny. Spisy tak například mohou být umístěny v uzamykatelných skříních, k nimž mají přístup pouze konkrétně určené osoby. Vedle uzamykatelných skříní mohou být dále například využity podle okolností mříže na oknech, bezpečnostní dveře nebo zámky. Pokud jde o zpracování prostřednictvím výpočetní techniky, tak této problematice věnujeme následující kapitolu.

Zabezpečení dat v NNO při využívání informačních technologií

LIDSKÝ FAKTOR JAKO ROZHODUJÍCÍ PRVEK

V jakékoliv obraně před útokem nebo zneužitím je třeba si uvědomit, že tím nejslabším článkem v řetězci všech bezpečnostních rizik je často sám uživatel. Ani nejmodernější ochranné prvky nemohou být dostatečně účinné, pokud je uživatel ignoruje, či si neuvědomuje základní pravidla bezpečného chování na internetu.

Mezi nejčastější rizika patří výběr nevhodného přihlašovacího **hesla**. Je nutné si uvědomit, že se heslo v kombinaci s přihlašovacím jménem (certifikátem apod.) stává unikátním klíčem, který doslova otevírá brány k užití dané služby (e-mailu, databáze, cloudového úložiště). Za žádných okolností proto nepoužívejte hesla příliš jednoduchá, či úzce související s Vaší osobou (jména členů rodiny, data narození, domácí zvíře, 12345, název firmy… apod.)! Obecně platí, že čím delší a na první pohled nesmyslnější kombinaci čísel, písmen a speciálních znaků heslo tvoří, tím je jeho prolomení složitější.

Problémem pak může být zapamatování takových řetězců. Ale v tom už nám mohou pomoci různé mnemotechnické pomůcky anebo programové aplikace typu 1Password, LastPass apod. Ty umožňují uživateli snadno spravovat více hesel a přístupů bez nutnosti jejich zapamatování.

Ovšem i ten nejsilnější bezpečnostní klíč lze prolomit tehdy, pokud s ním zacházíme neodpovědně. Stejně jako v běžném životě nenecháváme nikde bez dozoru ležet své klíče od domova, je nevhodné vystavovat svá hesla na papírcích na veřejně viditelných místech. Riskujeme tím jejich ukradení. Z důvodu možného odcizení je také vhodné hesla pravidelně obměňovat. Činíme tak obzvlášť v případech, kdy máme podezření na jejich zneužití nebo prolomení. Systém hesel zkrátka klade těžiště odpovědnosti na nás – uživatele. Bezpodmínečně vyžaduje, abychom k celému procesu přistupovali zodpovědně a uvědoměle.

Lidský faktor hraje zásadní roli také v obraně proti technikám založeným na sociálním inženýrství. Příkladem takového útoku je tzv. **phishing**. Jedná se o podvodný způsob elektronické komunikace, kdy se útočník snaží přesvědčit uživatele k „dobrovolnému“ vydání citlivých údajů nebo k nainstalování škodlivého softwaru, a to zejména tím, že se vydává za člověka nebo instituci, které věříme. Obratnou manipulací útočníka můžete i citlivé údaje sdělit zcela nevědomky např. při příjemné konverzaci v kavárně. Proti tomuto druhu ohrožení tedy může pomoci jen zdravá míra nedůvěřivosti a dodržení několika pravidel.

Phishing v internetovém prostředí probíhá především prostřednictvím rozesílání e-mailů nebo zpráv v aplikacích typu Skype, Messenger, Google chat ad. Zde se uživatel setkává s identicky vypadajícím, nicméně falešným profilem osoby nebo instituce, která vybízí k zadání přístupových údajů nebo k instalaci (škodlivého) software. Základním způsobem obrany proti podobnému jednání je ostražitost. Vedle ostražitosti a prověřování autenticity podobných výzev je důležitou prevencí také pravidelná aktualizace Vašeho operačního systému a instalace antivirových programů.

Obecně platí, že použité bezpečnostní prvky by neměly zásadním způsobem obtěžovat uživatele při běžné práci. Ze zkušeností totiž jednoznačně vyplývá, že pokud jsou nastavená bezpečnostní pravidla až příliš obtěžující, jsou uživateli spíše porušována a ignorována.

SOFTWARE A OPERAČNÍ SYSTÉMY

Zásadní roli při ochraně údajů hraje volba operačního systému. Především v neziskové sféře však narážíme na nedostatek finančních zdrojů při pořizování hardware a software. Kvůli tomu je obtížné zajistit unifikované prostředí pro všechny pracovníky, neboť je nutné improvizovat. Nemělo by to však znamenat rezignaci na požadavek chránit a zabezpečovat data.

Volba bezpečného operačního systému (OS), minimálně pro zařízení používané k práci s citlivými informacemi, může do budoucna ušetřit hodně starostí. OS by měl být nenáročný na výkon (hardware) počítače, jednoduše použitelný i pro laika, pravidelně aktualizovaný a měl by ideálně obsahovat i možnost šifrování dat.

Mezi nejrozšířenější OS pro stolní a přenosné počítače v současnosti patří Windows od firmy Microsoft, OSx od Apple a Open source systém Linux (Ubuntu, Mint, SuSe, Debian…).

Windows je v současnosti nejvíce užívaný OS s dlouhou historií, což je zároveň také jeho největší slabinou. Cílí na něj totiž rekordně největší počet virů a škodlivého software. Systémy postavené na Windows se kvůli tomu poměrně obtížně udržují bezpečné. Vyžadují časté aktualizace a bezpečnostní opravy („záplaty“). O systém se musí uživatel pravidelně starat – dbát o pravidelné aktualizace, někdy jej dokonce celý smazat a znovu instalovat, neboť během užívání dochází k výraznému poklesu výkonu a kapacity. Systém Windows by se navíc měl vždy používat v kombinaci s kvalitním antivirovým programem a firewallem – integrovaná ochrana od výrobce není příliš účinná, či bývá neaktuální.

OSx má na trhu menší zastoupení, protože jeho funkčnost je vázaná výhradně na použití s hardware firmy Apple. Díky tomu je však OSx stabilnější a výkonnější. Jádro systému stojí (stejně jako v případě Linuxu) na architektuře UNIX, která nabízí pružné, stabilní a mnoha desítkami let prověřené řešení. Tvorba efektivního viru a průnik do těchto složitých systémů bývá o poznání náročnější, a tedy pro většinu hackerů nezajímavá.

Vzhledem k uživatelsky příjemnému prostředí a při praktické absenci závažného škodlivého software se i přes počáteční vyšší náklady jedná o vhodný OS k práci s citlivými daty.

Linux je další poměrně rozšířený OS. Tentokrát Open source, tedy otevřený a distribuovaný zcela zdarma. Vzhledem ke své absolutní otevřenosti se objevuje v nepřeberném množství podob. Každá z mnoha distribucí má vlastní vzhled a specifika funkčnosti. Dlouho platilo, že pro výbornou modularitu systém ocení především IT nadšenci, s čímž ovšem úzce souvisela poměrně komplikovaná obsluha pro uživatele-laika. V posledních verzích (jako jsou Ubuntu, či SuSe) ovšem už toto tvrzení neplatí. Jde o operační systémy vhodné i pro méně náročné uživatele a začátečníky. Stejně jako systém OSx nabízí Linux výkonné a stabilní jádro UNIX, a aktuálně proto může být některá z distribucí Linuxu poměrně zajímavou volbou, zvláště vzhledem k široké podpoře a minimálním nákladům.

Na mobilních zařízeních dominují systémy Android od Google a iOS od Apple. Microsoft potom nabízí vlastní verzi mobilního OS Windows Phone.

K práci s citlivými daty nejsou příliš vhodná zařízení založená na platformě Android. Šifrování obsahů je sice možné, je však velmi náročné na výkon konkrétního přístroje. Práce s daty na některých zařízeních se proto může zpomalit až o 40% oproti nešifrované verzi. Vzhledem k velké rozšířenosti Androidu je také často vyhledávaným cílem pro malware útoky.

Existují i robustněji zabezpečené distribuce založené na Androidu, nelze je však považovat za běžný standard přístupný většině uživatelů.

iOS od firmy Apple jako druhý nejrozšířenější mobilní systém od verze 8 více akcentuje důležitost ochrany citlivých dat a nabízí 256 bitové AES šifrování jako nedělitelnou součást funkčnosti. Aktivuje se automaticky jednoduše zadáním unikátního hesla.

Společnost také deklaruje, že nemá žádnou možnost ke změně či prolomení tohoto uživatelem zadaného kódu, což ztěžuje případné možnosti skenování obsahů ze strany vládních agentur či bezpečnostních složek, které ochraně soukromí příliš nepřejí. Ani Applu se však nevyhýbají masivní uniky dat, a to převážně z externího on-line uložiště iCloud. Stejně tak se již několikrát objevily pokusy o propašování aplikací se škodlivým kódem do jinak vcelku bezpečného obchodu s aplikacemi App Store.

Mobilní zařízení používající OS Windows Phone nabízejí v současnosti šifrování jen přes uživatelsky složitou aktivaci EAS (Exchange Active Sync), což je činí pro většinu zájemců o jednoduchý a bezpečný mobilní OS prakticky nepoužitelnými. To se však může lehce změnit s příchodem nové verze systému. Navíc Windows Phone má na trhu jen velmi malé zastoupení, díky čemuž není příliš zajímavý pro cílené šíření škodlivého software.

Obecně platí, že i ten nejvíce zabezpečený OS může být lehce kompromitován neuváženou instalací škodlivých aplikací třetích stran samotným uživatelem. Je proto nezbytně nutné dbát na obecné zásady bezpečnosti při práci s počítačem a neinstalovat aplikace z pochybných zdrojů, nestahovat a nespouštět přílohy nevyžádaných, či jinak podezřelých e-mailů a zpráv.

Specifické oblasti zpracování osobních údajů v NNO

Během realizace našeho projektu jsme došli k několika oblastem, v kterých nevládní organizace řeší problematiku zpracování dat svých klientů. V následujících kapitolách se tak na tyto oblasti stručně zaměříme.

ZÁLOHOVAT, ZÁLOHOVAT, ZÁLOHOVAT… A ŠIFROVAT!

Ke ztrátě cenných dat může vést i ztráta samotného zařízení, jeho selhání nebo neočekávaná situace (např. požár či jiná živelná událost). Pravidelná a bezpečná archivace dat by tedy měla být samozřejmou denní rutinou pro každého, kdo citlivé údaje zpracovává.

Způsobů jak a kam zálohovat je mnoho: RAID síťové pole, externí pevné disky, on-line úložiště, či magnetooptická média… Vhodné řešení vybíráme vždy na míru konkrétní organizace, zejména podle objemu a typu ukládaných dat, počtu pracovníků apod. Ideální systém zálohování však kombinuje místní úložiště s tzv. off-site řešením, tedy úložištěm, které leží mimo místo zpracování dat, a to hlavně pro případ poruchy, krádeže nebo jiného nepředvídatelného zásahu v místě, kde archivační datové nosiče uchováváme.

V praxi se jedná například o specializovaný server či externí disk v kanceláři, doplněný například o různá placená nebo bezplatná online cloudová úložiště typu Dropbox, iCloud, Crash plan, Open drive apod. Vlastní firemní cloudový archivační systém lze i jednoduše a bezpečně vytvořit například pomocí webových aplikací typu OwnCloud, Sparkleshare. Tyto systémy lze pak nastavit na zcela automatické průběžné zálohování našich dat, bez nutnosti zásahu obsluhy.

Při výběru řešení doporučujeme hledat takové, které zároveň při archivaci data i zašifruje a zásadně tím znesnadní jejich zneužití v případě krádeže nebo nechtěného úniku.

SOCIÁLNÍ SLUŽBY, DOKUMENTACE A MLČENLIVOST

Řada nevládních organizací, která zpracovává údaje o svých klientech, je registrovanou sociální službou. V takovém případě je klíčový zákon č. 108/2006 Sb., o sociálních službách (ZSS). Uvedený zákon je zákonem speciálním ve vztahu k zákonu o ochraně osobních údajů.

Z pohledu ochrany osobních údajů zákon upravuje řadu povinností souvisejících zejména s dokumentováním poskytování sociální služby (§§ 88 a 89 ZSS). Jde například o povinnost uzavřít smlouvu o poskytování zdravotní služby, vedení písemných individuálních záznamů o průběhu poskytování dané služby, ale i vedení dalších evidencí, jako je například evidence osob, kterým nemohla být služba poskytnuta nebo evidence případů, kdy došlo k omezení pohybu osob.

Tyto povinnosti upravené zvláštním zákonem tak představují ve vztahu k povinnostem při zpracování osobních údajů například výjimku z povinnosti disponovat souhlasem subjektu údajů se zpracováním, výjimku z informační nebo registrační povinnosti.

Co máme dělat, pokud klient sociální služby odvolá svůj souhlas s tím, abychom uchovávali záznamy o kontaktu s ním?

Povinnost vést písemné individuální záznamy o poskytování sociální služby upravuje § 88 písm. f) ZSS. To znamená, že zpracování osobních údajů v těchto záznamech je upraveno přímo zvláštním zákonem a není tedy prováděno na základě souhlasu subjektu údajů. Proto ani není možné tento souhlas odvolat.

Řada dotazů pracovníků poskytovatelů sociálních služeb se týká povinnosti mlčenlivosti. V souladu se zákonem o sociálních službách (§ 100 ZSS) musí zaměstnanci poskytovatelů sociálních služeb zachovávat **mlčenlivost** o údajích týkajících se osob, kterým jsou poskytovány sociální služby, které se při své činnosti dozvědí.

Prolomení mlčenlivosti je možné se souhlasem klienta (musí být písemný s uvedením rozsahu zproštění a subjektu, na nějž se zproštění vztahuje) a dále v případech upravených zvláštními zákony. Jde například o sdělování informací dle zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí.

Jako problematickou se ukazují případy, kdy jsou informace vyžadovány ze strany policie v rámci trestních řízení. To se týká například organizací, které pracují s drogově závislými osobami nebo s problémovou mládeží. Poskytování informací se v takovém případě řídí § 8 odst. 4 trestního zákoníku, který říká, že osoba vázaná mlčenlivostí může odmítnout poskytnutí informací vyžadovaných v rámci trestních řízení. To se nevztahuje například na povinnost oznámit nebo překážet trestným činům dle §§ 367 a 368 trestního řádu. Prolomení mlčenlivosti je také možné pokud o tom rozhodne soudce (§ 8 odst. 5 TŘ). Ten by měl v usnesení rovněž jasně vymezit rozsah údajů, které mají být poskytnuty. Pokud by tedy poskytovatel předal údaje o klientech policii bez tohoto souhlasu soudu (a zároveň by zde nebyla žádná jiná

zákonná výjimka), jednalo by se o porušení zákonné povinnosti mlčenlivosti.

Obrátil se na nás telefonicky policista s žádostí, abychom mu sdělili aktuální telefon našeho klienta s tím, že ho potřebuje informovat o výsledku jeho trestního oznámení. Můžeme mu ho sdělit?

Sdělením kontaktního telefonu bez souhlasu klienta by došlo k porušení povinnosti mlčenlivosti a to i v případě, že by sdělení čísla bylo v prospěch klienta. Policista by tedy měl doložit souhlas soudu, který uloží povinnost tuto informaci poskytnout. Důležité je upozornit i na formu kontaktu, kdy u telefonických žádostí nelze ověřit totožnost žadatele.

OCHRANA OSOBNÍCH ÚDAJŮ VS. OCHRANA SOUKROMÍ

Ochrana osobních údajů se týká případů, kdy dochází ke zpracování osobních údajů. Existuje ovšem řada situací, kdy dochází rovněž k zásahu do lidského soukromí, ale nejedná se o zpracování a nelze tedy aplikovat zákon o ochraně osobních údajů. Typickým příkladem je třeba použití kamerového systému k zabezpečení budov. V případě, že je pořizován z kamerového systému záznam, na němž jsou zachyceny tváře osob vstupujících do domu, bude se zpravidla jednat o zpracování osobních údajů.

Pokud ale snímání probíhá pouze v on-line režimu a nikdo záznam nepořizuje, nebude se muset slídil za kamerou řídit zákonem o ochraně osobních údajů, i když samozřejmě může jít o nepříjemný zásah do soukromí, třeba pokud je kamerou nahlíženo do něčího bytu. Na tyto případy je pak nutno aplikovat ustanovení občanského zákoníku týkající se ochrany osobnosti (§ 86 OZ). Ten, komu je tedy zasahováno do soukromí, se může například domáhat toho, aby od zásahu bylo upuštěno (§ 82 OZ) nebo se domáhat náhrady nemajetkové újmy (§ 2957 OZ).

Nespokojený klient zveřejňuje na internetu nepravdivé hanlivé informace o našich zaměstnancích. Jak se můžeme chránit?

V daném případě se nebude pravděpodobně jednat o zpracování osobních údajů, pokud nejde například o informace, které klient získal z nějaké ukradené databáze nebo ze zaměstnaneckých spisů. Bránit se tedy nelze s využitím institutů zákona o ochraně osobních údajů, jako je třeba podnět zaslaný ÚOOÚ, ale bude možné využít institutů ochrany osobnosti v občanském zákoníku. Zejména se bude možno domáhat toho, aby klient od zveřejňování upustil a případně se i domáhat satisfakce za zásah do osobnostních práv.

Kdy se budeme řídit zákonem o ochraně osobních údajů a kdy občanským zákoníkem, pokud zveřejňujeme fotografie z našich akcí (workshopy, benefiční akce apod.)?

Občanský zákoník budeme aplikovat zejména tehdy, kdy se nejedná o případy zpracování osobních údajů. Občanský zákoník, pokud pomineme výjimky, zavádí jasné pravidlo, že s pořízením podobizny a jejím dalším šířením by měla souhlasit osoba, která je na této vyfocena. Taková fotografie ale ještě nemusí nutně znamenat, že jde o zpracování osobních údajů, pokud naším cílem není osoby identifikovat, ale například pouze zdokumentovat průběh nějaké akce. Zpracováním by ale zveřejnění fotografií bylo, pokud bychom například označily osoby na fotografii odkazem na jejich profily na sociálních sítích nebo jmenováním osob v popiscích fotografií. V takovém případě by bylo nutno se popasovat i s povinnostmi uloženými v ZOOÚ.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZAMĚSTNANCŮ

Každý zaměstnavatel, tedy i nevládní organizace, musí zpracovávat řadu osobních údajů zaměstnanců, což mu ukládá zákoník práce (ZP) i další zvláštní zákony. Důvodem je například realizace odvodů na povinná pojištění nebo odvodů záloh na dani. Podobně musí zaměstnavatel například evidovat pracovní dobu, po níž zaměstnanec vykonával práci nebo skutečnosti, které jsou významné pro hodnocení práce a výplatu mzdy.

Vedle povinnosti údaje zpracovávat vyplývá zaměstnavatelům i právo kontrolovat v přiměřené míře své zaměstnance, zda řádně plní pracovní povinnosti. S tím souvisí i případné zpracování osobních údajů s touto kontrolou spojené zejména v případech, kdy mají tyto informace sloužit jako důkazní materiál. Konkrétní podoba této kontroly by se měla odvíjet od charakteru práce. Zákoník práce přitom zapovídá zaměstnavateli, pokud to neodpovídá zvláštní povaze jeho činnosti, zasahovat do soukromí zaměstnance a podrobovat ho otevřenému nebo skrytému sledování, odposlechu, nebo třeba sledování elektronické pošty (§ 316 odst. 2 ZP). V prostředí nevládních organizací by se za zvláštní povahu činnosti považovaly zejména případy, kdy například hrozí napadení pracovníků daných organizací.

Od případů, kdy jsou osobní údaje zpracovávány

z důvodu plnění zákonných povinností nebo z důvodu ochrany oprávněných zájmů zaměstnavatele, je třeba odlišit případy, kdy jediným právním titulem ke zpracování osobních údajů může být souhlas.

Můžeme na našich webových stránkách zveřejnit seznam našich zaměstnanců s kontaktními údaji, údaji o jejich pracovním zařazení a s fotografií?

U pracovních kontaktních údajů (pracovní e-mail, pracovní telefon) by bylo možno dojít k tomu, že není třeba souhlas zaměstnance, protože zveřejnění těchto kontaktů může být nezbytné kvůli efektivnímu fungování organizace. Zejména se to bude týkat zaměstnanců, kteří přicházejí do kontaktu s lidmi mimo organizaci, jako jsou klienti, média apod. Takové zpracování by se pak mohlo opírat o výjimku, podle níž není třeba souhlas, pokud jde o ochranu zájmů správce (§ 5 odst. 1 písm. e) ZOOÚ. Zveřejnění fotografií by ale již mělo být děláno pouze se souhlasem.

ZVEŘEJŇOVÁNÍ OSOBNÍCH ÚDAJŮ NA INTERNETU

Většina nevládních organizací provozuje své webové stránky, má své profily na sociálních sítích. S tím je i spojena častá otázka, jaká pravidla platí pro zveřejňování osobních údajů na internetu.

Předně je nutné říci, že ten, kdo údaje na internetu zveřejňuje, bude zpravidla správcem osobních údajů a to bez ohledu na to, zda příslušné webové stránky provozuje. Zveřejnění osobních údajů pak bude způsobem jejich zpracování. Správce musí tedy také splnit veškeré podmínky pro zpracování osobních údajů. Základní podmínkou bude vypořádat se s právním titulem.

Můžeme na internetu zveřejnit poděkování našim dárcům, i když nám k tomu nedali výslovný souhlas?

Pokud by takové poděkování mělo být individuální s uvedením totožnosti dárců, pak by se tak určitě mělo dít pouze s jejich předchozím souhlasem, protože zde nebude žádná zákonná výjimka. Pokud by šlo o obecné poděkování všem dárcům, kteří nějak přispěli, pak by se samozřejmě nejednalo o zpracování osobních údajů a souhlasu by nebylo třeba.

Vezměme si třeba případ zveřejňování fotografií ze seminářů konaných nevládní organizací pro zájemce z řad veřejnosti. Takové zveřejnění fotografií, bez ohledu na to, zda je lze nebo nelze považovat za osobní údaje, by se principiálně mělo dít se souhlasem těchto osob, což upravuje jak zákon o ochraně osobních údajů, tak občanský zákoník. Souhlas může být nicméně projeven třeba i implicitně tím, že tyto osoby setrvají v místnosti i poté, co jsou upozorněny na to, že v průběhu semináře budou fotografovány a fotografie budou následně uveřejněny za účelem informování o proběhlém semináři na webových stránkách organizace.

Je potřeba si zejména dát pozor na to, že skutečnost, že správce zpracovává legálně osobní údaje, ještě nemusí znamenat, že je také oprávněn je zveřejnit.

Získali jsme souhlas s použitím fotografií našich klientů při poskytování konzultace ve výroční zprávě. Nyní dva klienti svůj souhlas s použitím fotografií odvolali. Co bychom měli dělat, když jsme již zprávy za nemalé peníze vytisknuli?

V souladu s občanským zákoníkem by použití uvedených ilustračních fotografií mělo být vázáno na souhlas osob, o jejichž podobiznu jde. Na tento problém by se aplikovala primárně ustanovení občanského zákoníku, podle nichž lze souhlas s publikací podobizny odvolat a to i bez důvodu. V daném případě by se tak neměly výroční zprávy s těmito podobiznami šířit, což samozřejmě může organizaci způsobit nemalé komplikace. V souladu s § 87 odst. 2 OZ by ale bylo možno uvažovat o vymáhání vzniklé škody po těch, kteří původně svůj souhlas udělili a následně odvolali, ačkoli k tomu nebyl rozumný důvodu spočívající například ve změně okolností.

Obsah

Ochrana osobních údajů (nejen) pro nevládní organizace
Vydalo Iuridicum Remedium, z.s.

O IuRe:

Iuridicum Remedium, z. s.
Sídlo: Přístavní 1236/35, 170 00 Praha 7
Kancelář: U Výstaviště 3, 170 00 Praha 7

tel.: +420 776 703 170
e-mail: iure@iure.org
www.slidilove.cz, www.iure.orr
Facebook: Ceny Velkého bratra ČR
Twitter: @iure_cz