GDPR stručně

O ochraně osobních údajů stručně a jasně

Ač ochrana osobních údajů u nás platí od roku 1992, ač úřad zřízený zákonem o ochraně osobních údajů kontroluje povinnosti tímto zákonem uložené už téměř dvě desetiletí, pro mnohé, kteří si se zákonem starosti nedělali, jako by šlo o novou věc.

Pod vlivem kampaně rozpoutané kolem obecného nařízení o ochraně osobních údajů (GDPR), hlavně za účelem zisku řady poradenských firem, se podivují, s jakými novinkami ten zatracený Brusel opět přichází. Kampaň přitom provází řada nesprávných a zavádějících informací, šířených v médiích a zaznívajících i na některých přednáškách. Pro mnohé jsou nesrozumitelné i termíny, které zákon používá, například „zpracování osobních údajů“, což jsou operace s osobními údaji prováděné a pouze na ně se tato ochrana vztahuje. Tedy ne na každé použití údaje nějakého člověka v jakékoliv situaci, jak se často mylně domnívají ti, kdo ochranu osobních údajů ztotožňují s ochranou osobnosti podle občanského zákoníku. Dalšími podobnými pojmy jsou třeba „subjekt údajů“, což je člověk, o jehož údaje jde, „správce“, což je ten, kdo operace s osobními údaji provádí, buď z vlastního rozhodnutí, nebo proto, že je to jeho zákonnou povinností, a „zpracovatel“, což je někdo jiný, koho správce prováděním takové činnosti pro něj smlouvou pověří.

Pokusme se proto, bez použití těchto termínů a s ještě přípustným zjednodušením ve čtyřech bodech popsat to základní, co je třeba pro ochranu osobních údajů udělat a co nového k tomu přidává obecné nařízení o ochraně osobních údajů.

1. Důvod

Abychom mohli o nějaké kategorii lidí, například našich zákazníků nebo zaměstnanců, získávat a používat jejich údaje, musíme k tomu mít nějaký (právní) důvod. Velmi často jím bývají smlouvy, které s nimi uzavíráme. Pracovní smlouvy se zaměstnanci, kupní nebo jiné smlouvy se zákazníky.

Takovým důvodem je samozřejmě také zákon, který to ukládá, např. při vedení evidencí občanů státními orgány, ale i při vedení účetní a mzdové evidence v soukromé firmě. V některých případech může být důvodem ochrana našich práv, např. hlídá-li kamera náš cenný majetek před zlodějem nebo vandalem. Jindy to může být veřejný zájem na informacích o určitých osobách, zejména veřejně známých nebo veřejně činných.

Takové informace a jejich používání ale nemohou nepřiměřeně zasahovat do jejich soukromého života. Nenajdeme-li žádný z těchto důvodů, a přece bychom chtěli údaje o lidech získávat, např. o tom, jakému našemu zboží budou dávat přednost, je třeba je požádat, zda s vedením takových údajů budou souhlasit. Musíme ale mít na paměti, že souhlas je dobrovolný, nemůže jím být podmiňováno uzavření smlouvy, a když ho zákazník odvolá, má právo, aby byly takové údaje vymazány.

Když už si zákazník od nás něco koupil nebo objednal, nemusíme získávat jeho souhlas k zaslání další nabídky našeho zboží nebo služeb, nejčastěji zasílané na jeho e-mail. Jakmile však odpoví, že o takové obchodní sdělení nestojí, je nutné zasílání nabídek na jeho adresu ukončit. Není-li dán jiný důvod ke zveřejňování v databázi uchovávaných osobních údajů, např. kontaktních údajů zaměstnance do zaměstnání pro kontakt se zákazníky, je ke zveřejňování osobních údajů také třeba získat souhlas. Zvláštní důvody je třeba mít k tomu, abychom mohli získávat a používat kategorie údajů, které by mohly být zneužívány k diskriminaci lidí, např. údaje o zdravotním stavu.

2. Zásady

Vždy bychom si měli nejprve uvědomit, proč údaje o nějakých lidech potřebujeme nebo chceme získávat. Z toho je pak třeba vyjít při požadavku na poskytnutí údajů, abychom zbytečně o těch lidech nezaznamenávali informace, které vlastně vůbec nepotřebujeme. Rozsah údajů by tak měl být jen minimální, abychom dosáhli toho, co jsme si stanovili. Měli bychom dbát na to, aby získávané údaje byly přesné a jejich přesnost ověřovat. Možnost ověřit přesnost údajů z občanského průkazu dotyčné osoby není vyloučena, kopírování občanského průkazu i pasu je však až na zákonem stanovené výjimky nepřípustné.

Zaznamenané údaje nemohou být využívány v rozporu s původním cílem. Například na záznamu kamery je uložena spousta obrazových informací o všech osobách, které do sledovaného prostoru vstoupily. Jsou po přiměřenou dobu uchovávány, aby případně bylo možné policii doložit informace o pachateli trestného činu.

Nemohou být ale využívány k nedůvodnému sledování sousedů, třeba jen proto, že si někdo neočistil boty, nebo k nepřiměřenému kontrolování zaměstnanců na pracovišti.

Další zásadou je mít údaje jen tak dlouho, jak je potřeba. Ta doba se může v různých případech hodně odlišovat. Od několika dnů záznamu kamery, kdy je zřejmé, že se v té době nic mimořádného nestalo, až po desítky let u zákonem stanoveného uchovávání některých dokumentů, třeba mzdových listů. Ne vždy končí doba nutná k uchovávání všech údajů ukončením nějaké činnosti, např. ukončením pracovního poměru nebo naplněním smluvního ujednání. V úvahu je třeba brát jak lhůty stanovené zákonem pro uchovávání některých dokumentů, tak případné promlčecí lhůty pro možnost podání soudní žaloby a v případě listinných dokumentů i lhůty skartační.

3. Informace

Nejvíce nedorozumění a stížností vzniká z toho, že lidé nedostanou dostatečnou informaci o tom, proč své osobní údaje poskytují a co se s těmito údaji bude dále dít, komu budou případně předány. Již při získávání údajů je proto třeba dotyčnému člověku takové informace poskytnout, nejlépe v písemné podobě, ať již v místě, kde k získání údajů dochází nebo i prostřednictvím webových stránek.

Vyhovět je třeba i dalším právům, která mohou lidé uplatnit, jestliže jejich osobní údaje uchováváte a používáte. Právo na poskytnutí informací o svých údajích mají nejen ve chvíli jejich poskytnutí, ale mohou se dotázat i kdykoliv později. Pokud se to nedotkne práv jiných osob, má každý právo i na poskytnutí kopie svých údajů. Za další kopii už ale můžete požadovat přiměřený poplatek. K dalším právům patří i právo na opravu nepřesných údajů, právo vznést námitku, např. proti dalšímu zasílání marketingových nabídek, a také právo na výmaz údajů, ale pouze pokud není jiný důvod pro jejich další uchovávání.

4. Zabezpečení

Pokud máte údaje lidí jen na listinných dokumentech a ne v počítači, vztahuje se na ně ochrana jen v případě, že jsou vedeny formou evidence fyzických osob.

Je třeba, aby listinné dokumenty, pokud se s nimi nepracuje, byly uchovávány v uzamčené zásuvce stolu nebo v uzamčené skříni a nebyly ponechávány v neuzamčené místnosti, pokud z ní odchází ten, kdo s nimi má pracovat. K údajům uloženým v počítači nebo jiném elektronickém zařízení může mít na základě správně zvoleného hesla přístup vždy jen ten, kdo je pověřen, aby s určitými údaji pracoval. U větších a složitějších systémů je také třeba pořizovat elektronické záznamy, které umožňují určit a ověřit, kdy, kdo a z jakého důvodu údaje používá, tzv. logy.

Pravidla bezpečnosti je třeba zachovávat i u elektronických prostředků používaných při různých cestách, např. je neponechávat bez dozoru v automobilu. Osobní údaje musejí být odpovídajícím způsobem zabezpečeny i při jejich přenosu elektronickými prostředky. Je nutné si uvědomit, že běžná emailová komunikace není příliš bezpečná. Někdy je dokonce přirovnávána k ekvivalentu korespondenčního lístku. V některých případech je tak vhodné zvolit bezpečnější formu přenosu informací, např. jejich šifrováním. Šifrovaný soubor lze zaslat i méně zabezpečenými formami komunikace. Vždy je nutné zvážit vhodnost zasílání nikterak nezabezpečených dokumentů obsahujících větší penzům osobních údajů (či citlivých) prostřednictvím freemailových služeb. Neznamená to však, že by nebylo možné nikdy použít freemailovou službu, např. pokud jde jenom o jednoduchou domluvu se zákazníkem či zaslání nikterak rizikových informací.

Pokud osobní údaje, např. svých zákazníků nebo zaměstnanců, předáte někomu jinému, aby s těmito údaji pracoval pro vás a místo vás, musíte s ním uzavřít smlouvu, ve které se zaváže, že bude údaje chránit stejně jako vy. Bez takové smlouvy byste pro předání údajů jiným osobám mimo firmu nebo organizaci museli získat souhlas dotčeného člověka, pokud nejde o požadavek policie nebo jiného státního orgánu, který má právo si údaje potřebné pro svoji činnost vyžádat a je povinnost mu je poskytnout.

5. Co nového k tomu od 25. května 2018 přidává obecné nařízení o ochraně osobních údajů (GDPR)?

Pro menší firmu, která vede jen evidenci smluv se svými zákazníky a evidenci zaměstnanců, toho není zas až tak mnoho.

Záznamy o činnostech–všichni

Je třeba vést záznamy o činnostech, které se s osobními údaji provádějí. Lze doporučit připravit si na to formulář s kolonkami a do nich zapsat informace požadované v článku 30 GDPR (záznam o evidenci smluv,

o evidenci zaměstnanců, případně o slevovém programu pro zákazníky aj.). Takový zápis by pak neměl trvat déle než 10 - 15 minut.

Ohlašování případů porušení zabezpečení–všichn

Druhou obecně platnou povinností je ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů podle článku 33 GDPR (do 72 hodin od zjištění takového incidentu). Hlásit je třeba závažné incidenty s předpokládanými závažnými důsledky, ne když se z papírově vedené evidence omylem založí jeden papír do jiného šuplíku, kde se za hodinu najde. Pokud dojde k úniku dat, např. v bance, kde máte uloženy peníze, a hrozilo by, že o ně můžete v důsledku toho přijít, bude mít banka povinnost oznámit to i vám, v krajním případě i veřejným oznámením takového závažného incidentu.

Kodexy a osvědčení – dobrovolně

Pokud v některých odvětvích, např. při podnikání, dochází ke stejným nebo velmi podobným činnostem s osobními údaji, může pro to být, např. profesním sdružením, vypracován kodex chování. Přihlášení se k takovému kodexu dokládá snahu být v souladu s obecným nařízením, není však povinné, stejně jako osvědčení o ochraně osobních údajů, o které bude možné požádat, ale povinné rovněž nebude.

Pověřenec pro ochranu osobních údajů – jen někdo
Úřady a jiné orgány, které rozhodují o právech občanů, a patří k nim i školy, budou muset jmenovat pověřence pro ochranu osobních údajů, osobu, která se bude této problematice věnovat a upozorňovat na případné nedostatky. Předpokládá se, že bude problematice ochrany osobních údajů v příslušném odvětví rozumět. Pověřencem může být jak vlastní zaměstnanec, tak externista. Poměrně široce tak lze využít možnosti, že jeden pověřenec bude moci takovou činnost vykonávat pro více úřadů, škol, ale i nemocnic, protože ty také budou mít povinnost pověřence jmenovat z hlediska velkého množství údajů o zdravotním stavu pacientů v informačním systému nemocnice. Pověřencem ale nemůže být šéf organizace nebo oddělení informatiky, protože by byl ve střetu zájmů.

Posouzení vlivu a konzultace s Úřadem – jen někdo

Stejně jako jmenování pověřence není ani posouzení vlivu na ochranu osobních údajů a předchozí konzultace s Úřadem pro ochranu osobních údajů povinností obecně platnou, týká se těch, kdo hodlají provádět s osobními údaji rozsáhlé rizikové operace, spočívající například v rozsáhlém profilování lidí prostřednictvím internetu, při kterém jsou pro marketingové účely získávány podrobné informace o jejich soukromém životě, nebo rizikovost spočívá ve využití nových technologií používaných, např. na velké množství údajů o zdravotním stavu pacientů. Seznam těchto operací bude Úřadem pro ochranu osobních údajů zveřejněn.

Sankce – vždy přiměřené

Flagrantního porušení obecným nařízením stanovených povinností při takových rizikových operacích prováděných ve velkém objemu dat, zpravidla velkými nadnárodními společnosti, se mohou týkat maximální, obecným nařízením stanovené sankce, dosahující značných částek. Strašit takovými sankcemi menší firmu nebo školu je nesmysl, stejně jako vydávání horentních částek, podstatně převyšujících výši pokut Úřadem pro ochranu osobních údajů ukládaných za externí audity soulad s nařízením nezaručujícími. Případné sankce za porušení povinností obecného nařízení budou jako dosud přiměřené a v žádném případě nemohou být likvidační.