VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2013

Částka 65 | **22. července 2013** | **Cena 48,- Kč**

OBSAH

ÚVOD

Šedesátá pátá částka Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací v období od 1. 2. 2013 do 21. 6. 2013.

Rubrika Stanoviska Úřadu přináší stanovisko č. 2/2013 „Pořizování obrazových a zvukových záznamů z jednání zastupitelstva“, které poskytuje veřejnosti ucelený postoj Úřadu k pořizování a zveřejňování zvukových nebo audiovizuálních záznamů z jednání zastupitelstev obcí a krajů.

V rubrice Sdělení Úřadu je publikován materiál „K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb“. Je zaměřen především na rizika spojená s využitím datových úložišť, respektive s předáváním osobních údajů do třetích zemí mimo EU/EHP, kde jsou datová úložiště umístěna. Materiál představuje obecně přijímané právní nástroje, které stanovují právní rámec pro předávání osobních údajů do třetích zemí nezajišťujících přiměřenou úroveň ochrany osobních údajů a upozorňuje na případná rizika vyplývající z jejich aplikace při využívání cloudových služeb.

Součástí rubriky Sdělení Úřadu je také oddíl Z rozhodovací činnosti Úřadu (rok 2012). Přináší přehled rozhodnutí Úřadu, k nimž dospěl na základě řešení případů porušení zákona o ochraně osobních údajů, nebo podezření z porušení zákona.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00002593/002	SVOBODA PETR	7.5.2013
00002593/001	SVOBODA PETR	7.5.2013
00002594/001	PELI - EKO s.r.o.	4.5.2013
00003904/001	BESTSPORT akciová společnost	21.5.2013
00004321/015	Statutární město Plzeň	20.2.2013
00004656/001	DuPont CZ s.r.o.	6.6.2013
00006614/004	SECURITAS ČR s.r.o.	7.2.2013
00009138/006	Občanské sdružení ADRA	26.4.2013
00009138/002	Občanské sdružení ADRA	26.4.2013
00009138/001	Občanské sdružení ADRA	26.4.2013
00013340/001	STŘEDNÍ POLICEJNÍ ŠKOLA MINISTERSTVA VNITRA V JIHLAVĚ	16.3.2013
00019116/065	Správa železniční dopravní cesty, státní organizace	15.6.2013
00024300/004	Mark2 Corporation Czech a.s.	15.3.2013
00024300/001	Mark2 Corporation Czech a.s.	15.3.2013
00024300/005	Mark2 Corporation Czech a.s.	7.2.2013
00024300/002	Mark2 Corporation Czech a.s.	15.3.2013
00026151/001	EDV s.r.o.	12.3.2013
00030434/001	MERIGLOBE ADVISORY HOUSE s.r.o.	23.2.2013
00031014/001	STŘEDNÍ ODBORNÁ ŠKOLA A STŘEDNÍ ODBORNÉ UČILIŠTĚ OBCHODNÍ, BRNO, JÁNSKÁ 22	28.3.2013
00031156/001	Optimal Finance, s.r.o.	3.5.2013
00031387/009	Heineken Česká republika, a.s.	7.2.2013
00032144/006	McDonald`s ČR spol. s r.o.	13.4.2013
00032144/007	McDonald`s ČR spol. s r.o.	13.4.2013
00033481/011	Family drogerie s.r.o.	11.4.2013
00033481/095	Family drogerie s.r.o.	21.3.2013
00033481/092	Family drogerie s.r.o.	13.4.2013
00033481/087	Family drogerie s.r.o.	13.4.2013
00033481/085	Family drogerie s.r.o.	18.4.2013
00033481/042	Family drogerie s.r.o.	7.6.2013
00033917/001	L.M.G. spol. s r.o.	14.3.2013
00034412/001	Mayfield Radlice East-group s.r.o.	15.2.2013
00038128/001	RWE Plynoprojekt, s.r.o.	5.3.2013
00038128/002	RWE Plynoprojekt, s.r.o.	5.3.2013
00038128/003	RWE Plynoprojekt, s.r.o.	5.3.2013
00038128/004	RWE Plynoprojekt, s.r.o.	5.3.2013
00038128/005	RWE Plynoprojekt, s.r.o.	5.3.2013
00038790/002	VISTEON - AUTOPAL, S.R.O.	21.2.2013
00038790/003	VISTEON - AUTOPAL, S.R.O.	21.2.2013
00040112/001	ZÁKLADNÍ UMĚLECKÁ ŠKOLA, MORAVSKÝ KRUMLOV, OKRES ZNOJMO	11.5.2013
00043165/001	DANIELA PALLOVÁ	22.3.2013
00045305/002	Kozí 3 s.r.o.	11.4.2013
00045305/001	Kozí 3 s.r.o.	11.4.2013

II. STANOVISKA ÚŘADU

Stanovisko č. 2/2013

červen 2013

Pořizování obrazových a zvukových záznamů z jednání zastupitelstva

Úvod

V návaznosti na dřívější stanoviska Úřadu pro ochranu osobních údajů (dále jen „Úřad"), stanoviska 2/2004[1] a 1/2007[2], a dále na základě výsledků dozorové činnosti[3] se Úřad rozhodl poskytnout veřejnosti ucelené stanovisko týkající se problematiky pořizování a zveřejňování zvukových nebo audiovizuálních záznamů z jednání zastupitelstev obcí a krajů. Závěry uvedené v předkládaném stanovisku jsou pro přehlednost uváděny z pohledu obce, ovšem uplatní se ve stejném rozsahu také pro jednání zastupitelstev krajů a hlavního města Prahy.

Základní právní posouzení

Pořizování záznamů

Na každém jednání zastupitelstva vystupují jednak konkrétní identifikovatelné fyzické osoby a také zde zaznějí osobní údaje dalších osob, a to především při projednávání jednotlivých bodů. Pořízení, uchování a zveřejnění záznamu (ať již pouze zvukového nebo audiovizuálního) lze považovat za zpracování osobních údajů tehdy, pokud obsahuje informace týkající se identifikované nebo identifikovatelné fyzické osoby. To znamená, že v případě záznamů z jednání zastupitelstva se o zpracování osobních údajů bude jednat vždy a je tedy potřeba se vypořádat s požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Proto pokud pořizuje sama obec záznam z jednání zastupitelstva, vystupuje tato obec v postavení správce osobních údajů.

Pro posouzení legálnosti a legitimnosti každého zpracování je základním kritériem účel zpracování osobních údajů. Z dosavadních poznatků z dozorové činnosti Úřadu lze konstatovat, že se jako účel zpracování v těchto případech objevují v zásadě dva důvody: pořízení záznamu jako podkladu pro pozdější vyhotovení zápisu ze zasedání zastupitelstva a pořízení záznamu za účelem informování veřejnosti o činnosti obce a zastupitelstva typicky prostřednictvím jeho zveřejnění na internetových stránkách obce. Oba tyto účely jsou dle Úřadu legální a legitimní a není důvod je jakkoliv omezovat. V některých případech popsaných dále může ovšem dojít k omezení rozsahu a způsobu zpracování, především zveřejnění osobních údajů.

Pořízení záznamu pro informování veřejnosti

Pro informování veřejnosti prostřednictvím záznamu (zvukového nebo audiovizuálního) se uplatní v zásadě stejná pravidla, která jsou vyjádřena ve stanovisku Úřadu 2/2004, které se týká zveřejňování zápisů z jednání obce. Na úvod lze tedy problematiku zjednodušit konstatováním, že obec může bez jakéhokoliv omezení informovat o své vlastní činnosti, pokud tato informace nesouvisí s konkrétní fyzickou osobou.

Otázkou, se kterou se bude muset správce (obec) vypořádat prvotně, je právní titul pro zpracování osobních údajů. U zastupitelů, úředníků obce a dalších úředních osob je tento právní titul obsažen v § 5 odst. 2 písm. f) zákona o ochraně osobních údajů, neboť lze předpokládat, že informace, které k těmto osobám zaznějí (stejně jako jejich samotná přítomnost) na zasedání zastupitelstva, mají přímou souvislost s jejich úřední činností. Proto v jejich případě není třeba získávat souhlas s pořízením a zveřejněním záznamu, ani není nutné jejich osobní údaje jakkoliv anonymizovat s výjimkou případů, kdy by se projednávané osobní údaje bezprostředně dotýkaly rovněž jejich osobního či rodinného života mimo veřejnou nebo úřední činnost.

U osob z řad veřejnosti, které budou přítomny na zasedání zastupitelstva, lze konstatovat, že z pohledu informačního účelu záznamu není třeba souhlas s jejich zaznamenáním, pokud budou tyto osoby na záznamu zachyceny přiměřeným způsobem, tedy např. pouze krátkým záběrem do prostoru pro veřejnost apod.[4] Naopak u osoby z veřejnosti, která aktivně na jednání zastupitelstva vystoupí k některému z bodů, lze její osobní údaje související s vystoupením zpracovávat bez jejího souhlasu, neboť takové vystoupení je

[1] Stanovisko č. 2/2004 – Zpřístupňování a zveřejňování osobních údajů z jednání zastupitelstev a rad obcí a krajů.

[2] Stanovisko č. 1/2007 – K aplikaci práva na ochranu osobních údajů při poskytování informací o činnosti orgánů veřejné správy.

[3] Výsledky kontrolní činnosti, jak jsou popsány ve Výroční zprávě za rok 2011 (str. 32-35), dále např. rozhodnutí zn. REG-0281/09-23 a kontrolní protokol zn. INSP2-4075/11-14 (obojí dostupné v archivu poskytnutých informací podle zákona č. 106/1999 Sb. na webových stránkách Úřadu www.uoou.cz).

[4] V takovém případě lze zpracování podřadit pod výjimku podle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, tedy jako zpracování nezbytné pro ochranu práva obce informovat o jednání zastupitelstva, které nepředstavuje nepřiměřený zásah do soukromí subjektu údajů.

projevem politického práva a aktivity konkrétního občana, která již z povahy věci není a nemůže být anonymní.[5] Je ovšem třeba rozlišovat příspěvek k diskusi na zastupitelstvu a vystoupení s konkrétní žádostí vůči obci zejména v sociální oblasti (zde bude třeba posuzovat situaci individuálně, takovéto případy by ovšem, zejména u větších obcí, neměly být časté).

Na základě výše uvedeného lze tedy doporučit, aby kamera byla umístěna tak, aby zaznamenávala prostor pro zastupitele a pro řečníky z řad veřejnosti, neměla by ovšem nepřetržitě zabírat prostor pro veřejnost.

Nejproblematičtější otázkou jsou osobní údaje třetích osob, které při jednání zastupitelstva zaznějí při projednávání jednotlivých bodů[6]. Pro tyto případy se uplatní právní názor vyjádřený již ve stanovisku 2/2004, tedy že neomezené zveřejnění těchto osobních údajů, typicky prostřednictvím internetu, ze strany obce není možné a tyto osobní údaje je třeba před zveřejněním záznamu anonymizovat. Proto v případě pořízeného záznamu pouze v těchto případech bude obec povinna osobní údaje vhodným způsobem anonymizovat.[7] Pro úplnost lze uvést, že v případě fyzických osob, na které se bude vztahovat § 8b zákona č. 106/1999 Sb., o svobodném přístupu k informacím, není potřeba anonymizaci osobních údajů v rozsahu[8] citovaného ustanovení provádět.

Zásadní význam pro zpracování osobních údajů výše uvedeným způsobem má splnění informační povinnosti dle § 11 zákona o ochraně osobních údajů. Prostor, kde probíhá jednání zastupitelstva, by měl být tedy označen informací o pořizování záznamu, jeho účelu atd., stejná informace může být součástí jednacího řádu zastupitelstva. Ze strany řídícího schůze zastupitelstva by ještě před zahájením vlastního pořizování záznamu měla také zaznít informace o tom, že bude pořizován záznam, za jakým účelem, jakým způsobem bude se záznamem dále zacházeno a o právu přítomných na námitku proti takovému zpracování ve smyslu § 21 zákona o ochraně osobních údajů. Jelikož nelze plně zobecnit veškeré možné situace, ke kterým při jednání zastupitelstva dojde, včetně osobních údajů, které na něm zaznějí, má právo na námitku význam v tom, že obec jako správce je poté povinna vyhodnotit, zda zveřejněním záznamu nedojde k nepřiměřenému zásahu do soukromí subjektu údajů nebo lidské důstojnosti, a zda není důvod záznam částečně upravit a nad rámec výše uvedeného dále anonymizovat.[9] Takové posouzení by měla na základě § 10 zákona o ochraně osobních údajů provádět ostatně automaticky u každého záznamu i bez výslovné námitky.

Z dalších povinností vztahujících se na obec jako na správce osobních údajů je třeba upozornit na stanovení doby uchování osobních údajů (resp. obecně dobu zveřejnění). Jako nejvhodnější se jeví stanovení doby zveřejnění záznamu po dobu cca jednoho funkčního období zastupitelstva, tj. čtyř let, ale vzhledem k účelu, kterým je informování veřejnosti, lze akceptovat i dobu delší. Povinnost dle § 13 zákona o ochraně osobních údajů se v daném případě zúží na zabezpečení záznamu před jeho neoprávněnou změnou či jiným zásahem do jeho obsahu. V případě tohoto zpracování je také správce povinen splnit oznamovací povinnost dle § 16 zákona o ochraně osobních údajů.

Pořízení záznamu pro potřeby vyhotovení zápisu

Z každého zasedání zastupitelstva obce je dle § 95 zákona o obcích[10] povinnost pořídit zápis, a to do 10 dnů po skončení zasedání. Jak bylo uvedeno výše, jedním z podkladů, na základě kterého bude zápis vyhotoven, může být také zvukový nebo audiovizuální záznam z jednání.

V případě zvukového záznamu lze podmínky pro postup

---

[5] Zpracování tedy bude možné podřadit pod § 5 odst. 2 písm. e) zákona o ochraně osobních údajů; lze také v některých případech uvažovat o omezené aplikaci § 5 odst. 2 písm. f) zákona o ochraně osobních údajů. Nejpřesněji uvedená možnost vyplývá z čl. 7 písm. f) směrnice 95/46/ES, který umožňuje zpracování osobních údajů bez souhlasu subjektu údajů, pokud je nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, pokud tyto zájmy převyšují právo na ochranu soukromí.

[6] Z dozorové činnosti Úřadu jsou známy případy řešení stížnosti na šikanu ve škole, kdy obec v zápise zveřejnila jméno a příjmení šikanované žačky a jejího otce, který stížnost podal, nebo otázka prominutí poplatku za odpad z důvodu umístění dívky do výchovného ústavu (zápis obsahoval jak jméno, příjmení dívky a její matky, jejich adresu trvalého pobytu, tak informaci o důvodech této žádosti, tj. umístění ve výchovném ústavu).

[7] Shodný závěr vyplývá také z rozsudku Městského soudu v Praze sp. zn. 9 Ca 261/2004 (dostupný na webových stránkách Úřadu www.uoou.cz v rubrice Judikatura) a z rozsudku Nejvyššího správního soudu sp. zn. 8 As 22/2009; opačný poté z rozsudku Městského soudu v Praze sp. zn. 10 A 54/2012.

[8] Dle § 8b odst. 3 zákona č. 106/1999 Sb. se poskytne o příjemci veřejných prostředků jméno, příjmení, rok narození, obec, kde má příjemce trvalý pobyt, výše, účel a podmínky poskytnutých veřejných prostředků.

[9] Dle § 21 zákona o ochraně osobních údajů:
(1) Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může
a) požádat správce nebo zpracovatele o vysvětlení,
b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.
(2) Je-li žádost subjektu údajů podle odstavce 1 shledána oprávněnou, správce nebo zpracovatel odstraní neprodleně závadný stav.

[10] Případně § 43 zákona o krajích, § 65 zákona o hlavním městě Praze.

obce shrnout tak, že záznam může být pořizován bez souhlasu přítomných osob (subjektů údajů), a to na základě výjimky dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů; takové zpracování slouží k ochraně práv obce při plnění její zákonné povinnosti, stejně jako k ochraně práv jednotlivých zastupitelů a práva na přesnost a správnost pořízeného zápisu. Současně neshledává Úřad existenci záznamu za zásadní zásah do soukromí účastníků jednání zastupitelstva (za podmínky, že se záznamem bude zacházeno dále popsaným způsobem). Stejně tak jako ve shora uvedeném případě, je povinností obce informovat ve smyslu § 11 odst. 1 zákona o ochraně osobních údajů přítomné o tom, že záznam bude pořizován, kým a za jakým účelem, komu mohou být osobní údaje zpřístupněny, a dále o právu přítomných na námitku proti zpracování osobních údajů (tj. proti existenci záznamu) ve smyslu § 21 zákona o ochraně osobních údajů.

Pro pořizování audiovizuálního záznamu pouze pro účely vyhotovení zápisu bude platit v zásadě výše uvedené. Obec jako správce bude muset pouze dbát na to, aby obrazový záznam byl pořizován pouze z prostor, kde se nacházejí zastupitelé, neboť pro potřeby zápisu není nutné zaznamenávat veřejnost, která aktivně na zastupitelstvu nevystupuje (tj. její přítomnost se v zápise nijak neprojeví).

Pro vlastní zacházení se záznamem, přístupu k němu atd. by obec měla v souladu s § 13 odst. 1 a 2 zákona o ochraně osobních údajů přijmout a dokumentovat pravidla, kterými se bude řídit. V souladu s § 5 odst. 1 písm. e) zákona o ochraně osobních údajů je povinností správce zlikvidovat osobní údaje, jakmile pomine účel jejich zpracování. Tím je v daném případě pořízení zápisu. Jelikož proti zápisu může vznést člen zastupitelstva námitku, o které by se rozhodovalo na nejbližší schůzi zastupitelstva, je v zásadě možné uchovávat záznam až do tohoto okamžiku, neboť právě záznam může být podkladem pro rozhodnutí zastupitele o námitce zastupitele proti zápisu. Poté je ovšem obec na základě § 20 odst. 1 zákona o ochraně osobních údajů[11] povinna osobní údaje zlikvidovat. V případě tohoto účelu zpracování osobních údajů nebude obec povinna plnit oznamovací povinnost vůči Úřadu a to na základě výjimky dle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů.

Závěr

Ačkoliv se problematika pořizování a zveřejňování záznamů z jednání zastupitelstva může na první pohled zdát složitá a nepřehledná, lze konstatovat, že se vždy uplatní následující pravidla, která by obec (kraj, hlavní město Praha či městská část) měla dodržet:

- stanovit účel takového zpracování osobních údajů;
- splnit informační povinnost vůči přítomným osobám;
- možnost zásahu do soukromí, a tedy otázku anonymizace, je třeba řešit shodně jako v případě písemných zápisů, tedy pouze u třetích osob, jejichž záležitosti jsou na zastupitelstvu projednávány. Není třeba anonymizovat ani členy zastupitelstva obce či jiné úřední osoby, ani osoby z řad veřejnosti, které aktivně na zastupitelstvu vystupují;
- je třeba umožnit subjektům údajů právo na námitku proti zpracování osobních údajů a každou námitku individuálně posoudit, zda nedochází k nedůvodnému a nepřiměřenému zásahu do soukromí.

Poznámka:
Publikované stanovisko je také k dispozici na internetové adrese Úřadu www.uoou.cz v rubrice Názory Úřadu/Stanoviska.

[11] Záznam plní stejnou roli jako rukou psané poznámky a další podklady, které teprve slouží pro vyhotovení zápisu, a proto by neměl být považován za písemnost ve smyslu zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.

III. SDĚLENÍ ÚŘADU

K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb

Úvod

Při provozování cloudových služeb bude téměř vždy docházet zároveň ke zpracování osobních údajů. Za zpracování osobních údajů je zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“) považována jakákoliv operace nebo soustava operací, kterou správce nebo zpracovatel systematicky provádí s osobními údaji, např. jejich shromažďování, zpřístupňování, zveřejňování či třídění, ale také ukládání na nosiče informací, uchovávání a předávání. Především tyto poslední operace budou předmětem tohoto materiálu. Zákazníci cloudových služeb se mohou dříve či později v rámci nabídky těchto služeb setkat s požadavkem jejich poskytovatele na přenos osobních údajů uložených v cloudu do jiných států, velmi často do tzv. třetích zemí[1] mimo EU/EHP. Je odpovědností zákazníka cloudových služeb, jako správce osobních údajů, aby si vybral takového poskytovatele, který je schopen zaručit soulad jim nabízených a realizovaných služeb se zákonem o ochraně osobních údajů. Materiál představuje některé právní instrumenty, jako jsou standardní smluvní doložky, institut „Safe Harbor“ nebo závazná podniková pravidla, tedy tradiční a obecně přijímané právní nástroje, které stanovují právní rámec pro předávání osobních údajů do třetích zemí nezajišťujících přiměřenou úroveň ochrany osobních údajů a upozorňuje na případná rizika vyplývající z jejich aplikace při využívání cloudových služeb. Ostatními aspekty a riziky týkajícími se zpracování údajů v cloudu se věnuje pouze okrajově a většinou pouze v souvislosti s předáváním údajů do jiných států.

Podstatnou vlastností cloud computingu je skutečnost, že nemusí existovat pevné umístění dat zákazníka v rámci sítě datových úložišť poskytovatele cloudových služeb a data mohou migrovat z jednoho datového úložiště do druhého, přičemž každé z nich se může nacházet v jiné zemi, včetně tzv. třetích zemí. Cloud computing v dnešní podobě představuje z pohledu ochrany osobních údajů poměrně velké riziko především pro samotného zákazníka/správce osobních údajů, který je primárně za zpracování osobních údajů odpovědný. Je tedy důležité, aby zákazník všechna rizika vždy pečlivě a předem analyzoval. Cílem tohoto materiálu není vyjmenovat všechna rizika související s poskytováním cloudových služeb,[2] ale zaměřuje se pouze na rizika spojená s využitím datových úložišť, resp. s předáváním osobních údajů do třetích zemí mimo EU/EHP, kde jsou datová úložiště umístěna.

Definice pojmu cloud computing

V současné době není obsah pojmu cloud computing ze strany odborné veřejnosti zcela přesně vymezen, resp. existuje několik obecných definic. Podobně bychom pro něj stěží hledali i vhodný český překlad[3]. Je tedy vhodnější vysvětlit samotnou podstatu cloud computingu, než uvádět jednotlivé definice, případně hledat tu nejvýstižnější. V případě poskytování služeb cloud computingu se v zásadě jedná o to, že některé zdroje, služby nebo aplikace, které uživatel využívá pro zajištění své činnosti, jsou umístěny mimo jeho počítač a práce s nimi probíhá na vzdálených zařízeních jejich poskytovatele, ke kterým uživatel přistupuje přes internet (často pomocí webového prohlížeče) a uživateli je umožněno zdroje, služby nebo aplikace pružně upravovat, měnit a používat dle svých potřeb. Jinými slovy, uživatel nemá svá data uložena ve svém lokálním počítači, ale kdesi „v cloudu“, a přistupuje k nim pomocí aplikací, které si opět neinstaluje do svého počítače, ale které běží „kdesi“. Uživatel pak pouze přistupuje k jejich uživatelskému rozhraní.

Řešení cloud computingu lze rozdělit do tří základních modelů podle druhu poskytovaných služeb:

IaaS (Infrastruktura jako služba) – poskytovatel pronajímá technologickou infrastrukturu, tj. většinou virtuální servery (včetně příslušných služeb). Uživatel může jednoduše, efektivně a ekonomicky nahradit stávající IT systémy nebo je používat v kombinaci s pronajímanou infrastrukturou. Poskytovatelé bývají specializované subjekty, které vytvářejí často komplexní řešení geograficky rozložené ve více oblastech.

SaaS (Software jako služba) – poskytovatel nabízí koncovým uživatelům prostřednictvím webu různé aplikační

[1] Za třetí zemi se považuje každá země, která není součástí Evropského hospodářského prostoru. Součástí EHP jsou kromě členských zemí EU rovněž Island, Lichtenštejnsko a Norsko. Každá ze zemí EHP, jako smluvní strana Smlouvy o EHP, je součástí vnitřního trhu EU.

[2] Podrobněji se všem aspektům cloud computingu věnuje Stanovisko Pracovní skupiny pro ochranu údajů zřízené podle čl. 29 směrnice 95/46/ES č. 5/2012 ke cloud computingu (dokument WP 196) přijaté dne 1. července 2012 a dostupné na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_cs.pdf#h2-2, kde jsou podrobněji uvedena všechna rizika s touto službou spojená, viz s. 5 tohoto stanoviska.

[3] Spojením dvou anglických slov cloud (mrak) a computing (práce s počítačem) bychom mohli do českého jazyka přeložit jako práce s počítačem na dálku nebo prostě jako kancelář v oblacích.

služby a stará se, aby byly pro uživatele dostupné. Tyto služby mohou nahradit běžné aplikace, které uživatelé instalují v rámci svých lokálních IT systémů. Tak je tomu například u kancelářských aplikací (textový editor, tvorba tabulek a databází, sdílené kalendáře atd.), ale i e-mailových aplikací založených na webových technologiích (Gmail pro firmy).

PaaS (Platforma jako služba) – poskytovatel nabízí řešení pro vývoj a hostování aplikací. Tyto služby jsou obvykle určeny pro subjekty na trhu, které je používají k rozvoji a umístění koncových aplikací určených pro vlastní potřebu nebo jako službu pro potřeby třetích stran.

Z hlediska vlastnictví lze jednotlivé modely rozdělit na:

Veřejný cloud (public cloud) – služby jsou nabízeny a zároveň sdíleny mezi navzájem nesouvisejícími uživateli.

Soukromý (privátní) – služby jsou poskytovány v rámci jedné organizace nebo pro přesně vymezenou množinu subjektů.

Hybridní cloud – je kombinace obou výše uvedených přístupů.

Zákazník/správce a poskytovatel/zpracovatel

Z pohledu zákona o ochraně osobních údajů je důležité vymezit role hlavních aktérů, zejména role správce[4] a zpracovatele[5] osobních údajů, aby byla jasně stanovena odpovědnost za dodržování pravidel pro ochranu osobních údajů. Dnes je zcela běžné, že správce deleguje některé úkoly související se zpracováním osobních údajů na smluvního partnera, který se tak ocitne v roli zpracovatele. Tento stav obecně souvisí s rozšířením outsourcovaných služeb. V běžných situacích je to správce, který rozhoduje, co by měl smluvní partner dělat a jak, nastavit podmínky, úroveň bezpečnosti dat a další důležité aspekty obchodního vztahu. V praxi to ovšem bude v mnoha případech právě poskytovatel cloudových služeb (zejména v případě větších společností), který bude mít předem nastaveny podmínky poskytované služby, které předloží zákazníkovi, a ten je buď akceptuje jako celek, či nikoliv. Nicméně i přesto je nutné vyjít z toho, že je to zákazník, který určuje účel zpracování, je za ně odpovědný a bez jeho vůle by žádný cloud nemohl existovat, což je také hlavní důvod, proč je zákazník obvykle považován za správce a jeho smluvní partner, tedy poskytovatel cloudových služeb, za zpracovatele.

Stanovisko (WP 196) č. 5/2012 ke cloud computingu k tomu uvádí:

„Zákazník cloudových služeb určuje konečný účel zpracování a rozhoduje o zadání tohoto zpracování nebo jeho části externí organizaci. Zákazník cloudových služeb tudíž vystupuje jako správce. Podle směrnice se správcem rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů". Zákazník cloudových služeb musí jako správce přijmout odpovědnost za dodržování právních předpisů na ochranu údajů a vztahují se na něj veškeré právní závazky stanovené ve směrnici 95/46/ES. Zákazník cloudových služeb může poskytovatele cloudových služeb pověřit výběrem postupů a technických či organizačních opatření, jež mají sloužit k naplnění účelu správce. Poskytovatel cloudových služeb je subjekt, který poskytuje výše popsané různé formy služeb cloud computingu. Pokud poskytovatel cloudových služeb zajišťuje prostředky a platformu a jedná jménem zákazníka cloudových služeb, pak se považuje za zpracovatele údajů, jímž se podle směrnice 95/46/ES rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje pro správce."

Zároveň ovšem uvedené stanovisko přiznává i možnost, kdy se i poskytovatel cloudových služeb může ocitnout za určitých okolností v roli správce, když dodává:

„…Mohou nastat situace, ve kterých může být poskytovatel cloudových služeb v závislosti na konkrétních okolnostech považován buď za společného správce, nebo správce v rámci vlastních pravomocí. Například k tomu může dojít v případě, kdy poskytovatel zpracovává údaje pro vlastní účely."

Pro úplnost je nutné dodat, že z uvedeného vztahu správce/zpracovatel vyplývá povinnost pro zákazníka/správce osobních údajů uzavřít zpracovatelskou smlouvu s poskytovatelem cloudových služeb/zpracovatelem osobních údajů podle § 6 zákona o ochraně osobních údajů, která musí obsahovat mj. i záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.[6] Správce bude tudíž vždy odpovědný za osobní údaje, ať jsou uloženy a zpracovávány kdekoliv.

Zákonná regulace předávání osobních údajů do jiných zemí

Zákazník cloudových služeb se může v praxi setkat s několika situacemi, kdy bude poskytovatel usazen v jiném státě a zároveň bude docházet ze strany poskytovatele cloudových

[4] Ustanovení § 4 písm. j) zákona o ochraně osobních údajů definuje správce takto: „správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak."

[5] Ustanovení § 4 písm. k) zákona o ochraně osobních údajů definuje zpracovatele takto: zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona."

[6] Podrobný obsah smluvních záruk je popsán ve Stanovisku (WP 196) č. 5/2012 ke cloud computingu přijatém dne 1. července 2012 na s. 12.

služeb k předávání a následnému ukládání svěřených osobních údajů do datových úložišť umístěných v různých státech světa. Ve spojitosti s tím je vždy nutné, aby poskytovatel cloudových služeb zákazníka předem informoval o tom, kde mohou být data umístěna, tj. ve kterých zemích a případně i komu konkrétně mohou být data dále předávána a v jaké zemi se příjemce údajů nachází. Jak již bylo uvedeno výše, jedním z hlavních rizik cloud computingu pro ochranu osobních údajů je riziko spojené s předáváním těchto údajů do třetích zemí mimo EU/EHP, které neposkytují osobním údajům dostatečnou úroveň ochrany. Podmínky, za kterých je možné takové předávání realizovat, upravuje zákon o ochraně osobních údajů, konkrétně ustanovení § 27. Účelem a smyslem tohoto ustanovení je zajištění ochrany osobních údajů subjektů údajů, které mají být předány a následně zpracovávány ve třetích zemích. V zásadě mohou být osobní údaje předávány do země mimo EU pouze, pokud tato země zaručuje odpovídající úroveň jejich ochrany. Předávat osobní údaje do třetích zemí nezajišťujících odpovídající úroveň ochrany lze rovněž na základě výjimek uvedených v § 27 odst. 3 písm. a) až g) zákona o ochraně osobních údajů.[7] Naplnění některého právem uznaného důvodu k předávání údajů do třetích zemí musí správce (vývozce) prokázat Úřadu pro ochranu osobních údajů (dále jen „Úřad“) v rámci povolovacího řízení vedeného na základě § 27 odst. 4 zákona o ochraně osobních údajů.

[7] „Není-li podmínka podle odstavců 1 a 2 splněna, může být předání osobních údajů uskutečněno, jestliže správce prokáže, že

a) předání údajů se děje se souhlasem nebo na základě pokynu subjektu údajů,

b) jsou v třetí zemi, kde mají být osobní údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření. Takové záruky mohou být upřesněny zejména smlouvou uzavřenou mezi správcem a příjemcem, pokud tato smlouva zajišťuje uplatnění těchto požadavků nebo pokud smlouva obsahuje smluvní doložky pro předání osobních údajů do třetích zemí zveřejněné ve Věstníku Úřadu,

c) jde o osobní údaje, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem; v takovém případě lze osobní údaje zpřístupnit jen v rozsahu a za podmínek stanovených zvláštním zákonem,

d) je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána,

e) je předání nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů,

f) je předání nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro uplatnění jiných právních nároků, nebo

g) je předání nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů, zejména pro záchranu života nebo pro poskytnutí zdravotních služeb.“

Odpovídající/přiměřená úroveň ochrany[8]

V souvislosti s přeshraničním tokem osobních údajů je velmi často zmiňován pojem přiměřená nebo odpovídající úroveň ochrany dat. Zajištění odpovídající úrovně ochrany při realizaci mezinárodních datových přenosů s využitím dostupných nástrojů je v současné době poměrně obtížné, což je způsobeno především rostoucím množstvím a složitostí mezinárodního předávání údajů. V zásadě existují dvě možnosti, jak dosáhnout toho, že třetí země bude označena za zemi s přiměřenou úrovní ochrany. První možností je, že odpovídající úroveň ochrany ve třetí zemi bude zajištěna prostřednictvím obecných právních předpisů dotyčné třetí země. Druhou možností je, že tuto ochranu bude garantovat sám správce (vývozce údajů), pokud přijme odpovídající ochranná opatření, která zajistí, že úroveň ochrany předávaných osobních údajů bude v zemi příjemce srovnatelná se standardy ochrany obsaženými v zákoně o ochraně osobních údajů. Taková opatření, resp. záruky mohou vyplývat např. ze smlouvy mezi vývozcem a příjemcem dat, jejíž nedílnou součástí budou standardní smluvní doložky podle příslušného rozhodnutí Komise, případně mohou být naplněna přijetím závazných podnikových pravidel. Pravomoc rozhodnout o tom, zda třetí země zajišťuje odpovídající úroveň ochrany na základě svých národních předpisů nebo svých mezinárodních závazků, má Evropská komise.[9] Úřad touto pravomocí nadán není. Nicméně ze zákona o ochraně osobních údajů vyplývá, že za země poskytující přiměřenou úroveň ochrany jsou považovány i ty, které ratifikovaly Úmluvu Rady Evropy 108, o ochraně osob se zřetelem na automatizované zpracování osobních údajů z roku 1981 (dále jen „Úmluva 108“).[10]

Modelové příklady předávání do jiných států

V praxi se mohou zákazníci cloudových služeb v postavení správců osobních údajů setkat s případy, kdy budou osobní údaje v rámci poskytování cloudových služeb předá-

[8] Odpovídající úroveň ochrany je hlavní zásadou, která se aplikuje při přeshraničních přenosech osobních údajů, a jejímž smyslem je zabránit předávání osobních údajů do třetích zemí, pokud nezaručí přiměřenou úroveň ochrany těmto údajům. Tato zásada vyplývá konkrétně z článku 25 směrnice 95/46/ES a § 27 odst. 1 a 2 zákona o ochraně osobních údajů.

[9] Komise v minulosti analyzovala národní předpisy týkající se ochrany osobních údajů v několika zemích a doposud rozhodla o přiměřené úrovni ochrany Andorrského knížectví, Argentiny, Faerských ostrovů, Guernsey, Izraele, Jersey, Kanady, ostrova Man, Nového Zélandu, Švýcarska a Uruguayské východní republiky. Dále Komise rozhodla, že úroveň ochrany je přiměřená za určitých podmínek v USA – případy „Safe Harbor“.

[10] Vedle členských států Evropské unie ratifikovaly Úmluvu 108 tyto státy: Andorra, Arménie, Albánie, Azerbajdžán, Bosna a Hercegovina, Černá Hora, Gruzie, Chorvatsko, Island, Lichtenštejnsko, Makedonie, Moldavsko, Monako, Norsko, Srbsko, Švýcarsko a Ukrajina.

vány do jiných zemí. Přitom přicházejí v úvahu následující možnosti:

1. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nacházejí v zemích EU a údaje budou předávány a uchovávány pouze v jejich rámci

   V tomto případě není nutné, aby správce/zákazník přijal dodatečné zvláštní záruky pro přenos údajů,[11] jelikož pro předávání v rámci členských států EU platí zásada volného pohybu osobních údajů, a proto předávání osobních údajů v rámci EU je možné bez povolení Úřadu. Jedná se o předávání v režimu § 27 odst. 1 zákona o ochraně osobních údajů. Správce a zpracovatel jsou povinni mezi sebou uzavřít smlouvu o zpracování osobních údajů ve smyslu § 6 zákona o ochraně osobních údajů[12], přičemž tato smlouva musí obsahovat všechny podstatné náležitosti podle tohoto ustanovení zákona.

2. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nacházejí ve třetích zemích, které ratifikovaly Úmluvu 108 nebo ve třetích zemích, o kterých Komise rozhodla, že poskytují přiměřenou úroveň ochrany, a údaje budou předávány a uchovávány pouze v rámci těchto zemí

   V těchto případech platí, že všechny tyto země poskytují odpovídající úroveň ochrany. Předávání probíhá v režimu § 27 odst. 2 zákona o ochraně osobních údajů. Dále platí obdobně to, co je uvedeno v bodě prvním.

3. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nacházejí ve zbývajících zemích světa, které nelze podřadit pod bod 1 ani bod 2, tzn. v zemích neposkytujících přiměřenou úroveň ochrany, a údaje budou předávány a uchovávány v rámci těchto zemí

   V tomto případě musí sám správce (zákazník cloudových služeb) zajistit, aby předávaným osobním údajům byla poskytnuta odpovídající ochrana srovnatelná s ochranou, kterou osobním údajům poskytuje zákon o ochraně osobních údajů. Nejvhodnějšími nástroji jsou standardní smluvní doložky a závazná podniková pravidla (BCR).

   a) **Standardní smluvní doložky**
   Jedním z nejčastěji využívaných nástrojů pro předávání osobních údajů do třetích zemí jsou standardní smluvní doložky.[13] V případě cloud computingu je v zásadě relevantní použití standardních (nebo také vzorových) smluvních doložek, které jsou přílohou rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES. Jak ze samotného názvu vyplývá, jedná se o doložky, které jsou určené pro předávání údajů mezi správcem/zákazníkem na jedné a zpracovatelem/poskytovatelem na druhé straně. Výhodou předávání realizovaných na základě aplikace standardních smluvních doložek je skutečnost, že pokud se stanou součástí smlouvy o poskytování (cloudových) služeb, není nutné žádat Úřad o povolení k předávání do třetích zemí, přičemž je zároveň splněn požadavek zákona o ochraně osobních údajů a předávaným osobním údajům je tímto (z hlediska právní úpravy) zajištěna dostatečná ochrana. Podle tohoto rozhodnutí Komise může zpracovatel osobních údajů (poskytovatel cloudových služeb) v rámci konkrétního zpracování využít rovněž služeb dílčích zpracovatelů.

Doložka č. 11 rozhodnutí Komise 2010/87/EU zavádí nový pojem „dílčí zpracovatel“, kterým se rozumí „*zpracovatel najatý dovozcem údajů nebo jiným dílčím zpracovatelem dovozce údajů, který se zavazuje přijímat od dovozce údajů nebo od jiného dílčího zpracovatele dovozce údajů osobní údaje určené výhradně pro činnosti spojené se zpracováním jménem vývozce údajů po předání v souladu s pokyny vývozce údajů, standardními smluvními doložkami stanovenými v příloze a podmínkami písemné smlouvy o dílčím zpracování.*“

Základním východiskem při využití institutu dílčích zpracovatelů zůstává, že správce je odpovědný za vše, co se stane s osobními údaji, jinými slovy osobní údaje mohou být zpracovány dílčím zpracovatelem pouze s výslovným souhlasem správce. Pokud by ve smlouvě o zpracování dat bylo výslovně stanoveno, že zpracovatel může delegovat celé nebo část zpracování na další subjekt, aniž by se zbavoval své odpovědnosti za dodržování smlouvy se správcem, může zpracovatel outsourcovat části zpracování na jednoho nebo více dílčích zpracovatelů. Pokud tak učiní, musí zpracovatel podniknout kroky k zajištění smluvních záruk, že dílčí zpracovatel se bude také řídit a dodržovat pokyny správce, a přijme nezbytná ochranná opatření k zajištění bezpečnosti zpracovávaných dat.

---

[11] Je důležité nezaměňovat se zárukami, které musí zpracovatel poskytnout v rámci zpracovatelské smlouvy podle § 6 zákona o ochraně osobních údajů. Zde se hovoří pouze o zárukách ve smyslu § 27 tohoto zákona.

[12] „Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.“

[13] Čl. 26 odst. 2 směrnice Evropského parlamentu a Rady 95/46/ES stanoví, že členské státy mohou předání nebo předávání osobních údajů do třetích zemí, které nezajišťují odpovídající úroveň ochrany, povolit za předpokladu, že existují určitá ochranná opatření. Tato ochranná opatření mohou zejména vyplývat z příslušných smluvních doložek.

Pokud zpracovatelé externě zadávají služby dílčím zpracovatelům, jsou rovněž povinni informovat o tom zákazníka, konkrétně popsat typ delegované služby, charakterizovat stávající a potenciální subdodavatele, seznámit zákazníka se zárukami, jež tyto subjekty nabízejí poskytovateli služeb cloud computingu.[14]

b) **Závazná podniková pravidla (Binding Corporate rules, dále jen „BCR“)**

BCR jsou interním aktem nadnárodní korporace, přičemž někteří z členů mohou mít sídlo mimo EU, ve třetích zemích, které nezajišťují osobním údajům odpovídající úroveň ochrany. Interní akt obsahuje komplexní politiku v oblasti ochrany osobních údajů s ohledem na jejich mezinárodní předávání pouze v rámci této korporace. V zásadě rozeznáváme BCR pro správce a BCR pro zpracovatele. Zatímco první z nich byla upravena řadou pracovních dokumentů Pracovní skupiny podle čl. 29 směrnice 95/46/ES a v praxi se již osvědčila, druhá na uvedení do praxe teprve čekají.[15] BCR pro správce stanovují společná a závazná pravidla pro předávání osobních údajů, která jsou původně zpracovaná korporací vystupující v roli správce (např. údajů vztahujících se k zákazníkům nebo zaměstnancům). Naproti tomu BCR pro zpracovatele jsou určena k témuž s tím rozdílem, že osobní údaje jsou původně zpracovávány korporací vystupující v roli zpracovatele. Jedná se o nový právní nástroj, který přináší nové možnosti v oblasti externího zpracování dat. Měl by být efektivní především tam, kde dochází k masivnímu předávání údajů zpracovatelem dílčím zpracovatelům v rámci téže korporace a na základě pokynů správce, aniž by bylo zapotřebí uzavřít s každým novým dílčím zpracovatelem zvlášť smlouvu o zpracování. Tím se zásadně liší od standardních smluvních doložek. Cílem nového právního nástroje není přesunout povinnosti správce na zpracovatele. Povinnosti správce a zpracovatele v kontextu mezinárodního předávání zůstávají nezměněny (analogicky jako u standardních smluvních doložek 2010/87/EU), nicméně některé nástroje jsou přizpůsobené zvláštnostem předávání v rámci jedné nadnárodní korporace (např. jeden globální závazek namísto několika smluv, určení odpovědnosti, audit, vzdělávací programy, role inspektora ochrany údajů apod.). Podobně jako v případě BCR pro správce i zde platí, že zpracovatel musí BCR předložit ke schválení vedoucímu dozorovému úřadu v EU, který řídí celý schvalovací proces a následně garantuje, že BCR mohou být považována za nástroj poskytující odpovídající ochranu. Následně ještě musí daný správce osobních údajů, který hodlá nechat zpracovat osobní údaje zpracovatelem se schválenými BCR pro zpracovatele, požádat o povolení k předávání příslušný národní dozorový orgán, pokud je to legislativou vyžadováno. Podle zákona o ochraně osobních údajů je tak nutné učinit podle § 27 na základě splnění požadavku podle odst. 3 písm. b) tohoto ustanovení zákona. Určitou nevýhodou oproti standardním smluvním doložkám zůstává délka schvalovacího procesu na úrovni EU, která se v praxi pohybuje okolo 8 měsíců, i skutečnost, že předávání údajů na základě BCR musí projít povolovacím řízením ještě na národní úrovni. Nicméně pro velké nadnárodní korporace poskytující cloudové služby a nacházející se v roli zpracovatelů může být zavedení BCR pro zpracovatele přínosem, neboť řeší tuto problematiku v globálním měřítku.

4. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nachází v USA (případy „Safe Harbor“ neboli „bezpečný přístav“)

Speciální postavení v rámci tzv. třetích zemí mají Spojené státy americké.[16] Pro bezpečné předání byl smlouvou mezi USA a EU zaveden tzv. program „Safe Harbor“ („bezpečný přístav“). Předmětem smlouvy je závazek EU umožnit volné předávání osobních údajů ze zemí EU do USA,[17] pokud se na straně příjemce jedná o společnosti, které jsou zařazeny na tzv. „Safe Harbor List.“[18] Z pohledu zákona o ochraně osobních údajů se jedná o předávání v režimu § 27 odst. 2 tohoto zákona, podle kterého mohou být do třetích zemí předány osobní údaje, pokud je tato třetí země označena na základě rozhodnutí orgánu EU za zemi, která poskytuje odpovídající úroveň ochrany. I přes právní zakotvení institutu „bezpečného přístavu“ v rozhodnutí Komise, je na místě otázka, zda certifikace „Safe Harbor“ je skutečně dostatečnou zárukou pro bezpečnost osobních údajů předávaných do USA, resp. zda společnosti na seznamu „Safe Harbor“ nabízejí dostatečné záruky pro předávání osobních údajů

[14] Stanovisko (WP 196) č. 5/2012 ke cloud computingu přijaté dne 1. července 2012, s. 9.

[15] Pracovní skupina podle čl. 29 směrnice 95/46/ES přijala 6. června 2012 pracovní dokument (WP 195) týkající se zásad, které jsou obsahem BCR pro zpracovatele a formulář žádosti o předložení závazných korporátních pravidel pro zpracovatele dostupné na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf .

[16] Z hlediska ochrany osobních údajů jsou USA považovány za třetí zemi nezajišťující přiměřenou úroveň ochrany.

[17] Rozhodnutí Komise č. 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států.

[18] Jedná se o seznam společností, které oznámily Ministerstvu obchodu Spojených států, že budou dodržovat zásady „bezpečného přístavu“. Seznam je k dispozici na www.export.gov/safeharbor

do USA. Odpověď na tuto otázku můžeme nalézt ve stanovisku WP29 ke cloud computingu:

„Pracovní skupina se domnívá, že společnosti vyvážející údaje by se neměly opírat pouze o prohlášení dovozce údajů o tom, že má osvědčení „bezpečného přístavu“. Společnost vyvážející údaje by naopak měla získat důkazy o tom, že existují vlastní osvědčení o přijetí zásad „bezpečného přístavu“, a požadovat důkazy o dodržování těchto zásad, což je důležité zejména s ohledem na informace poskytované subjektům údajů, jichž se zpracování údajů týká.“[19]

Správce/zákazník odpovědný za předávání údajů by se tedy neměl spokojit s konstatováním poskytovatele cloudu, že má certifikaci „Safe Harbor“, ale ověřit, zda tato certifikace skutečně existuje a je platná a dále požadovat důkazy, že zásady „bezpečného přístavu“ jsou také v praxi dodržovány.

V souvislosti s ochranou zpracovávaných osobních údajů uvádí stanovisko WP29 ke cloud computingu následující:

„V neposlední řadě zastává pracovní skupina názor, že zásady „bezpečného přístavu“ samy o sobě nemusejí vývozci údajů zaručovat prostředky nezbytné k zajištění toho, že poskytovatel cloudových služeb v USA přijal vhodná bezpečnostní opatření tak, jak mohou vyžadovat vnitrostátní právní předpisy na základě směrnice 95/46/ES. Pokud jde o bezpečnost údajů, jsou s cloud computingem spojena specifická rizika (např. ztráta kontroly, nezabezpečený nebo neúplný výmaz údajů, nedostatečné auditní stopy a selhání izolovanosti), která nejsou dostatečně ošetřena stávajícími zásadami „bezpečného přístavu“ k bezpečnosti údajů. Proto je možné zavést dodatečná ochranná opatření. Například lze využít odbornosti a zdrojů třetích stran, jež jsou schopny posoudit odpovídající úroveň poskytovatelů cloudových služeb na základě různých auditních, standardizačních a certifikačních systémů. Z těchto důvodů může být žádoucí doplnit závazek dovozce údajů k dodržování zásad „bezpečného přístavu“ o dodatečná ochranná opatření, jež by přihlížela ke zvláštní povaze cloud computingu.“[20]

Přihlášení se k dodržování zásad „bezpečného přístavu“ tedy především legalizuje samotný přenos těchto údajů do USA příslušné certifikované společnosti, nicméně ještě automaticky nezaručuje, že osobní údaje zpracovávané v cloudu jsou dostatečným způsobem chráněny. Stejně tak neexistuje žádná záruka, že zpracování v USA splňuje všechny požadavky podle platného českého práva regulující oblast ochrany osobních údajů. Podobně jako v případě zpracování, prováděném zpracovatelem na základě pokynu správce, tak i v případě zpracování v cloudu, zůstává správce primárně odpovědný za dodržování zákona. Proto bude nutné v tomto ohledu smluvně zavázat zpracovatele ve smyslu garance vhodných bezpečnostních záruk. Jestliže bude docházet k předávání osobních údajů mezi správcem/zákazníkem usazeným v ČR a zpracovatelem/poskytovatelem v USA, je nutné uzavřít smlouvu ve smyslu § 6 zákona o ochraně osobních údajů bez ohledu na účast zpracovatele na zásadách „bezpečného přístavu“.

„Cílem smlouvy je ochrana zájmů správce údajů, tedy fyzické či právnické osoby, která určuje účel a prostředky zpracování a která nese plnou odpovědnost za údaje vůči dotčené fyzické osobě (osobám). Smlouva tedy blíže určuje zpracování, které má být prováděno, a veškerá opatření nezbytná k zajištění bezpečnosti údajů.“[21]

Závěr

Závěrem tohoto materiálu je doporučení správcům/zákazníkům cloudových služeb, aby provedli komplexní a důkladnou analýzu rizik v souvislosti s využíváním cloudových služeb včetně přeshraničního předávání osobních údajů, a to zejména do třetích zemí nezajišťujících přiměřenou úroveň ochrany. Všichni poskytovatelé cloudových služeb by měli svým zákazníkům podávat veškeré informace týkající se přenosu a umístění datových úložišť, aby zákazník mohl správně posoudit všechny výhody a nevýhody poskytované služby. Zákazník by měl zhodnotit i rizika, která mohou vzniknout v případě, že právní předpisy třetí země nebo mezinárodní smlouva obsahují požadavky na příjemce údajů (poskytovatele cloudových služeb), aby zpřístupnil za určitých okolností osobní údaje orgánům veřejné moci (policii, soudu apod.).

Poznámka:
Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v rubrice Názory Úřadu/Na aktuální téma a v rubrice Předávání osobních údajů do zahraničí.

---

[19] Stanovisko (WP 196) č. 5/2012 ke cloud computingu přijaté dne 1. července 2012, s. 17.

[20] Stanovisko (WP 196) č. 5/2012 ke cloud computingu přijaté dne 1. července 2012, s. 18.

[21] Rozhodnutí Komise č. 2000/520/ES, (FAQ 10).

Z rozhodovací činnosti Úřadu

(rok 2012)

Sdělení úvodem:

Úřad pro ochranu osobních údajů se prostřednictvím následující stručné charakteristiky vyjadřuje k některým problematickým okruhům případů porušování povinností při zpracování osobních údajů, které projednává v rámci své rozhodovací činnosti.

1. K rozsahu osobních údajů shromažďovaných subjektem veřejné správy

Jednou ze základních povinností správce osobních údajů je dle § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Toto ustanovení zákona je přitom dle názoru správního orgánu nutno vykládat tak, že je-li z hlediska stanoveného účelu (zde vyřízení žádosti o poskytnutí stipendia) příslušný osobní údaj nadbytečný, dochází vždy k porušení této povinnosti. U povinnosti stanovené v § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. totiž zákon nepředpokládá, že by její porušení bylo možno zhojit, resp. mu předejít, souhlasem [srovnej s § 5 odst. 1 písm. f) zákona č. 101/2000 Sb., který umožňuje zpracovávat osobní údaje k jinému účelu, než pro který byly shromážděny, pokud k tomu dal subjekt údajů předem souhlas]. Plnění povinnosti podle § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. je závislé na objektivních kritériích týkajících se daného zpracování, tedy na tom, jaké konkrétní kategorie, resp. skupiny osobních údajů jsou ještě nezbytné pro daný účel, a které již nikoliv. V daném případě, vzhledem ke stanovenému účelu, považuje správní orgán za prokázané, že vyřízení žádosti o stipendium bylo nepochybně možné i bez rodného čísla žadatele a jeho zákonného zástupce a bez údaje o místu narození žadatele o toto stipendium, tedy že tyto osobní údaje nebyly nezbytné pro stanovený účel zpracování.

Účastník řízení je územní samosprávný celek, který podle § 1 odst. 4 krajského zřízení pečuje o všestranný rozvoj svého území a o potřeby svých občanů. Z hlediska zásady rovnosti je vyloučeno, aby bylo o potřeby občanů (ve smyslu výše uvedeného ustanovení) pečováno rozdílně podle toho, zda poskytnou účastníku řízení svá rodná čísla, resp. údaj o místu narození, či nikoli. Jinak řečeno účastník řízení není oprávněn podmiňovat poskytnutí stipendia poskytnutím souhlasu se zpracováním osobních údajů, které jsou z hlediska účelu takového zpracování nadbytečné. Proto má správní orgán za to, že účastníkem řízení získávaný souhlas nelze z hlediska posouzení porušení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. považovat za relevantní.

Ze stejných důvodů nepovažuje ve vztahu ke shromažďování rodných čísel správní orgán za relevantní ani právní úpravu obsaženou v zákoně o evidenci obyvatel, neboť ten nijak neřeší otázku toho, zda je, či není z hlediska stanoveného účelu rodné číslo nezbytné.

K tvrzení účastníka řízení, že rodné číslo bylo nezbytné pro zamezení duplicity žádostí, je třeba konstatovat, že se jedná zcela zjevně o účelové tvrzení, jelikož k přesné identifikaci žadatele měl účastník řízení dostatek jiných osobních údajů (např. datum narození, adresu bydliště, informace o návštěvě školy, atd.).

(čj. SPR-7763/11)

2. Ke zveřejnění fotografie pořízené kamerovým systémem v souvislosti s vyšetřováním trestného činu

Informace zachycené a zaznamenané kamerovým systémem jsou osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. tehdy, lze-li ze záběru identifikovat jednotlivé osoby a tedy tyto informace přiřadit k byť potenciálně identifikovatelné osobě. Dle správního orgánu k tomu v daném případě došlo, jak vyplývá z fotografie uveřejněné na sociální síti účastníkem řízení, která je dostatečná pro to, aby bylo možné osobu na ní zachycenou identifikovat, tj. ztotožnit. Ostatně i výzva, kterou účastník řízení zveřejnil s touto fotografií, žádá o pomoc při zjištění totožnosti této osoby.

Pořizování obrazového záznamu zachycujícího jednotlivé fyzické osoby v provozovně účastníka řízení, uchovávání těchto záznamů a jejich případné další použití (jako tomu bylo např. v tomto případě) jsou dle správního orgánu operacemi, které lze podřadit pod definici pojmu zpracování osobních údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. Účastník řízení je tedy správcem osobních údajů [§ 4 písm. j) zákona č. 101/2000 Sb.] zaznamenaných kamerou, kterou umístil ve své provozovně, a je tedy povinen dodržovat povinnosti stanovené zákonem č. 101/2000 Sb. Pro závěr ve smyslu, že se jedná o zpracování osobních údajů a že účastník řízení je správcem, přitom není nijak významná ani skutečnost, že kamerový systém je tvořen pouze jedinou kamerou.

Zpracování osobních údajů, tedy provoz kamerového systému se záznamem, musí mít podle zákona č. 101/2000 Sb. svůj právní titul. Tím může být souhlas subjektu údajů, nebo některá z výjimek dle § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. V dané věci je nutné konstatovat, že souhlas účastník řízení neměl. Souhlasem přitom není a nemůže být pouhý vstup zákazníka do provozovny, a to ani tehdy, pokud je předtím na existenci kamerového systému upozorněn. Takový právní úkon (tj. vstup do sledovaného prostoru) totiž není jednoznačný, svobodný, vědomý a prokazatelný projev vůle ve smyslu § 4 písm. n) zákona č. 101/2000 Sb. spočívající v souhlasu se shromažďováním osobních údajů;

současně nejsou splněny ani podmínky souhlasu ve smyslu § 5 odst. 4 zákona č. 101/2000 Sb. V daném případě ovšem může účastník řízení zpracovávat osobní údaje bez souhlasu subjektu údajů na základě výjimky dle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., neboť je to nezbytné pro ochranu jeho práv (ochrana majetku) a nejedná se s ohledem na záběr kamery o nepřiměřený zásah do soukromí sledovaných osob.

Správní orgán současně zdůrazňuje, že právě posouzení a vyvážení dvou kritérií (tedy práva na ochranu majetku a práva na soukromí) jsou zásadní pro posouzení legálnosti většiny kamerových systémů. Jednou ze základních vlastností kamerového systému přitom je, že shromažďuje a uchovává osobní údaje, tj. informace o soukromém životě, v naprosté většině běžných osob, které se žádného protiprávního jednání nedopouštějí.

Je-li účelem kamerového systému (zpracování osobních údajů) ochrana majetku, znamená to, že v případě odcizení majetku nebo způsobení jiné škody může kamerový systém, resp. záznam z něj, napomoci zjištění pachatele. Vyhledávání pachatelů trestných činů a shromažďování důkazů o jejich vině je ovšem v demokratickém právním státě rolí orgánů činných v trestním řízení (tj. orgánu státu, Policie České republiky) a nikoliv účastníka řízení. Proto je každý správce osobních údajů z kamerového systému v souladu s účelem ochrany majetku oprávněn pouze k předání záznamu orgánům činným v trestním řízení, ale již v žádném případě nesmí sám tyto záznamy zveřejnit. Uvedené souvisí i s tím, že dalším z prvků právního státu je presumpce neviny. Orgány činné v trestním řízení jsou za zákonem stanovených podmínek, na základě svých znalostí a zkušeností a po vyhodnocení všech jim dostupných důkazů a informací oprávněny zahájit proti konkrétní osobě trestní řízení, které je výrazem toho, že je daná osoba důvodně podezřelá z trestného činu, případně vyhlásit po takové osobě pátrání. V případě pátrání po pachateli trestného činu je poté Policie České republiky v souladu s § 81 písm. a) bodu 2. zákona č. 273/2008 Sb. oprávněna zveřejnit osobní údaje (tedy např. i fotografii podezřelé osoby) v rozsahu nezbytném k plnění úkolů policie v souvislosti s pátráním po osobách. Pokud tedy účastník řízení sám zveřejnil na svých stránkách na sociální síti fotografii podezřelé osoby pocházející z jím provozované kamery, jednalo se o zpracování osobních údajů k jinému účelu, než ke kterému byly osobní údaje shromážděny, a tedy o porušení § 5 odst. 1 písm. f) zákona č. 101/2000 Sb.
(čj. SPR-8505/11)

3. K předání osobních údajů zaměstnanců jinému subjektu za účelem vypracování návrhů smluv

Podle § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. je správce povinen zpracovávat osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny. K jinému účelu je může zpracovávat pouze v mezích ustanovení § 3 odst. 6 zákona č. 101/2000 Sb. (což v dané věci nepřipadá v úvahu) anebo s předchozím souhlasem subjektu údajů. Předání osobních údajů zaměstnanců za účelem jejich použití pro přípravu návrhů smluv konkrétních finančních produktů třetího subjektu je nepochybně jiným účelem zpracování, než ke kterému je účastník řízení jako zaměstnavatel shromáždil. K tomuto postupu mohl tedy přistoupit pouze se souhlasem svých zaměstnanců, který by splňoval náležitosti § 4 písm. n) zákona č. 101/2000 Sb. (svobodný a vědomý projev vůle) a § 5 odst. 4 zákona č. 101/2000 Sb. (tzv. informovaný souhlas).
(čj. SPR-0285/12)

4. K posouzení otázky liberace v případě zveřejnění osobních údajů prostřednictvím internetu

Správní orgán tedy na základě shora uvedeného posuzoval jednání účastníka řízení z hlediska ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. Správní orgán v této souvislosti uvádí, že vynaložení veškerého úsilí, které bylo možno požadovat, neznamená jakékoliv úsilí, které správce vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit (zákon používá kritérium veškeré úsilí, které bylo možno požadovat, a nikoliv např. spravedlivě požadovat, požadovat s ohledem na poměry atp.). V případě účastníka řízení je zřejmé, že sám nepřijal a neprovedl opatření pro zabezpečení osobních údajů, v následku čehož došlo k jejich zpřístupnění prostřednictvím internetu.

Z vyjádření účastníka je také zřejmé, že tabulka obsahující předmětné osobní údaje byla i spolu s informací, že bude zveřejněna, k dispozici minimálně dalším 3 zaměstnancům účastníka řízení (včetně přímé nadřízené paní X. Y.), aniž by kterýkoli z nich neoprávněnému zpracování, které je předmětem tohoto správního řízení, zabránil. Je tedy zcela vyloučené, aby bylo toto jednání přičítáno paní X. Y. a posuzováno jako její exces, za který by účastník řízení nenesl zodpovědnost.

Účastník řízení pouze ve svém vyjádření citoval některá z ustanovení týkajících se práce s informačními a komunikačními technologiemi. V tomto ohledu je třeba konstatovat, že žádné z těchto ustanovení z hlediska jeho obsahu není možné považovat za opatření, které by mělo upravovat nakládání s osobními údaji při výkonu zaměstnání a plnění úkolů, které jednotlivým zaměstnancům vyplývají z agendy, kterou zpracovávají. Z vyjádření účastníka řízení tak vyplývá, že žádným způsobem ve vnitřních předpisech nedefinoval požadavky na ochranu osobních údajů, nezavedl žádné kontrolní mechanismy a ani jiným způsobem neseznámil zaměstnance s pravidly pro zpracování osobních údajů. Správní orgán má proto za prokázané, že účastník řízení zcela jasně nevynaložil veškeré úsilí, které bylo možné požadovat, a že nepochybně existovaly další možnosti, jak mohl

postupovat, aby zveřejnění předmětných osobních údajů zabránil. (čj. SPR-7796/11)

5. K principu proporcionality při zpracování osobních údajů na základě zákona o svobodném přístupu k informacím

Zákon č. 106/1999 Sb. předpokládá poskytnutí informace na žádost konkrétní osoby a nezakazuje poskytnutí této informace jejím zveřejněním, přičemž účastníkem řízení nebyla doložena žádná žádost konkrétní osoby o poskytnutí informace týkající se některého z žadatelů dle zákona č. 106/1999 Sb. Při zveřejňování informace je obecně nezbytné rozlišovat dvě situace, a to na jedné straně zveřejnění informace určené pro oprávněné osoby (tj. v tomto případě žadatele) a na druhé straně zveřejnění prostřednictvím webových stránek, kdy dochází ke zpřístupnění informací včetně osobních údajů nejen uvedeným (oprávněným) osobám, ale neomezenému počtu příjemců. Podle § 5 odst. 7 zákona č. 106/1999 Sb. může povinný subjekt za podmínek stanovených tímto zákonem zveřejnit i další informace (než informace povinně zveřejňované podle tohoto zákona, resp. informace poskytované na základě žádostí jednotlivců). Protože však zákon č. 106/1999 Sb. pro poskytování osobních údajů odkazuje v § 8a na podmínky plynoucí ze zákona č. 101/2000 Sb., je nutné i v tomto případě uplatnit test proporcionality, jenž je ve vztahu k osobním údajům vyjádřen především v § 5 odst. 3 a § 10 zákona č. 101/2000 Sb. Zveřejňování osobních údajů způsobem umožňujícím dálkový přístup (prostřednictvím internetu) pro předem neurčený okruh osob z vlastní iniciativy povinného subjektu přitom zjevně zasahuje do osobní sféry jednotlivce daleko podstatnějším způsobem, než jejich zpřístupnění na základě individuální žádosti konkrétní fyzické nebo právnické osoby.

Princip proporcionality, resp. nutnost aplikace třístupňového testu (zákonný podklad – legitimní cíl – nezbytnost/přiměřenost), používají při své rozhodovací činnosti Evropský soud pro lidská práva, Soudní dvůr Evropské unie (resp. Evropský soudní dvůr), např. rozsudek ze dne 20. května 2003 ve spojených věcech Österreichischer Rundfunk a další (C-465/00, C-38/01 a C-139/01) nebo rozsudek ze dne 9. listopadu 2010 Volker a Markus Schecke GbR (C-92/09) a Hartmut Eifert (C-93/09) vs. spolková země Hessensko, ale i Ústavní soud, např. nález zn. Pl. ÚS 4/94 ze dne 12. října 1994, zn. Pl. ÚS 15/96 ze dne 9. října 1996, či zn. Pl. ÚS 40/08 ze dne 26. května 2009 a Nejvyšší správní soud (např. rozsudek čj. 1 Afs 60/2009-119). Správní orgán tak odkazuje například na bod 85 a 86 rozsudku ve věci Österreichischer Rundfunk, podle kterých mají daňoví poplatníci a veřejné mínění právo být obecně v demokratické společnosti informováni o používání veřejných příjmů; vyvstává však otázka, zda je uvádění jmen dotčených osob ve vztahu k probíraným příjmům přiměřené ve vztahu k legitimnímu cíli a zda se důvody takového zveřejnění jeví jako právně významné a dostatečné.

Omezení základních práv a svobod je podle testu proporcionality možné pouze tehdy, jedná-li se o zásah, který je pro dosažení sledovaného cíle vhodný, nutný a přiměřený. Kritériem pro nutný zásah je skutečnost, že není možné ze strany daného subjektu užití jiného, objektivně srovnatelného prostředku, jímž by docházelo k menšímu zásahu do chráněných zájmů na straně dotčených subjektů údajů. Za přiměřený je považován takový zásah, kdy je možno očekávat, že dosažený prospěch realizací dané činnosti bude větší, nežli nepříznivý následek jí způsobený – v tomto případě zejména v podobě míry zásahu do osobnosti dotčených subjektů údajů.

V případě žadatelů, jejichž žádosti byly vráceny, tito zjevně nebyli v danou chvíli příjemci veřejných prostředků, tudíž nebyl žádný právní důvod ke zveřejnění jejich osobních údajů. V případech úspěšných žadatelů pak správní orgán uvážil, že účastník řízení svou povinnost informovat o vynaložení veřejných prostředků mohl splnit tak, že by prostřednictvím svých webových stránek poskytl informaci o celkovém počtu příjemců, kterým byl dar poskytnut, a o celkové výši finančních prostředků takto vynaložených, struktuře těchto veřejných prostředků apod.

Výše uvedené tak vede k jednoznačnému závěru, že ani právo na přístup k informacím není neomezené; i pokud by bylo možné považovat za zákonný podklad jednání účastníka řízení zákon č. 106/1999 Sb. a legitimním cílem jeho jednání by bylo zvýšení transparentnosti, resp. veřejná kontrola použitých veřejných prostředků, nelze zveřejnění osobních údajů žadatelů prostřednictvím internetu v rozsahu vymezeném ve výroku tohoto rozhodnutí považovat za přiměřené resp. nezbytné, neboť způsobuje nepřiměřený zásah do práva na ochranu soukromého a osobního života. Lze tedy učinit závěr, že zveřejnění osobních údajů způsobem, který zvolil účastník řízení, by nebylo v souladu se zákonem č. 101/2000 Sb. ani v případě, že by skutečný účel zpracování směřoval k plnění práv a povinností vyplývajících mu ze zákona č. 106/1999 Sb. *(čj. SPR-5137/12)*

6. K souhlasu se zveřejněním osobních údajů u nezletilých, se kterými je vedeno trestní řízení

K předmětu tohoto řízení lze uvést následující: Na účastníka řízení se při nakládání s osobními údaji nezletilých v rámci vedeného trestního řízení vztahuje § 53 odst. 1 zákona č. 218/2003 Sb., tj. zákaz jakýmkoli způsobem zveřejnit informaci, ve které je uvedeno jméno, popřípadě jména, a příjmení mladistvého, nebo která obsahuje informace, které by umožnily tohoto mladistvého identifikovat.

V případě zveřejnění osobních údajů nezletilého je zřejmé, že k tomuto zveřejnění byl udělen písemný souhlas matky nezletilého, jako jeho zákonného zástupce. Zákon

č. 218/2003 Sb. neobsahuje výjimky ze zákazu zveřejnění informací o osobě nezletilého, a to ani souhlas dotčené osoby. Správní orgán však subsidiárně aplikoval ustanovení zákona č. 141/1961 Sb., trestní řád, jako obecné ustanovení týkající se zveřejňování informací o trestním řízení, kde podle § 8b odst. 5 písm. c) zákaz zveřejnění informací neplatí, dá-li poškozený předchozí písemný souhlas. Je-li poškozený mladší 18 let nebo je zbaven způsobilosti k právním úkonům anebo je jeho způsobilost k právním úkonům omezena, musí dát takový souhlas jeho právní zástupce, což bylo v projednávaném případě splněno. Současně je zřejmé, že jelikož je smyslem zákona č. 218/2003 Sb. chránit právní zájmy mladistvých, proti kterým je vedeno trestní řízení, nemůže být jeho cílem znemožnit, aby se v rámci jejich obhajoby postupovalo v souladu s jejich vůlí, resp. vůlí zákonného zástupce, která může zahrnovat též zveřejnění informací o probíhajícím trestním stíhání.
(čj. SPR-4266/12)

Poznámky:

[1)] Za jednotlivými texty, které jsou rozděleny do tematických okruhů, jsou vždy kurzívou uvedena interní čj., pod kterými jsou jednotlivé případy v Úřadu evidovány.

[2)] Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v sekci Dozorová činnost v rubrice Správní delikty/Z rozhodovací činnosti.

Věstník Úřadu pro ochranu osobních údajů

Vydavatel: Úřad pro ochranu osobních údajů
Adresa redakce: Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7
Redakce: Miluše Nejedlá, tel.: 234 665 232, fax: 234 665 505
e-mail: posta@uoou.cz
internetová adresa: www.uoou.cz

Administrace: Písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422, www.sevt.cz, e-mail: predplatne@sevt.cz. – **Předpokládané roční předplatné** se stanovuje za dodávku kompletního ročníku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Věstníku a pro tento rok činí 300 Kč – Vychází podle potřeby – **Tiskne**: Sprint servis, Lovosická 31, Praha 9.

Distribuce: Předplatné, jednotlivé částky na objednávku i za hotové – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422; drobný prodej v prodejnách SEVT, a. s. – Praha 4, Jihlavská 405, tel.: 261 260 414 – Brno, Česká 14, tel.: 542 213 962– České Budějovice, Česká 3, tel.: 387 319 045 a ve vybraných knihkupectvích. Distribuční podmínky předplatného: Jednotlivé částky jsou expedovány předplatitelům neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného, nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. Lhůta pro uplatnění reklamací je stanovena na 15 dnů od data rozeslání, po této lhůtě jsou reklamace vyřizovány jako běžné objednávky za úhradu. V písemném styku vždy uvádějte IČ (právnická osoba) a kmenové číslo předplatitele. Podávání novinových zásilek povoleno ŘPP Praha.

ISSN 1213-3442

62013002