VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2012

Částka 62 | **29. června 2012** | **Cena 124,- Kč**

OBSAH

ÚVOD

Šedesátá druhá částka Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací v období od 16. 3. 2012 do 15. 6. 2012.

V rubrice Sdělení Úřadu je poprvé začleněn oddíl Z kontrolní činnosti Úřadu (rok 2011), který uvádí výběr případů, které byly v roce 2011 řešeny v rámci jeho kontrolní činnosti.

Součástí rubriky Sdělení Úřadu je také oddíl Z rozhodovací činnosti Úřadu (rok 2010–2011). Přináší přehled rozhodnutí Úřadu, k nimž dospěl na základě řešení případů porušení zákona o ochraně osobních údajů, nebo podezření z porušení zákona.

Rubriku Sdělení Úřadu uzavírá dokument Pracovní skupiny pro ochranu dat podle článku 29 (WP29), kterým je „Stanovisko č. 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení“. Cílem tohoto stanoviska je objasnit právní rámec použitelný u geolokalizačních služeb dostupných a/nebo generovaných prostřednictvím inteligentních mobilních zařízení, která se mohou připojit na internet a jsou vybavena lokalizačními detektory, jako je GPS. K takovým službám patří například mapy a navigace, ukládání geolokalizačních odkazů u obsahu na internetu („geotagging“), sledování míst pobytu přátel, kontrola dětí a reklama vycházející z lokalizace. Vzhledem k tomu, že inteligentní telefony a tabletové počítače jsou neoddělitelně spjaty se svými majiteli, poskytují velmi podrobný pohled do soukromého života majitelů. Jedním z velkých rizik je to, že majitelé nemají povědomí o tom, že přenášejí svoji lokalizaci, ani o tom, komu. V souvislosti s rychlým technologickým rozvojem, zejména s ohledem na mapování bezdrátových přístupových míst a skutečností, že subjekty, které nově vstupují na trh, jsou připraveny vyvíjet nové lokalizační služby na základě kombinace údajů základnové stanice a GPS a WiFi, se pracovní skupina rozhodla konkrétně objasnit právní požadavky na tyto služby podle směrnice o ochraně údajů.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00000038/001	ČESKÝ SVAZ OCHRANCŮ PŘÍRODY SDRUŽENÍ MLADÝCH OCHRÁNCŮ PŘÍRODY	11.5.2012
00000065/001	ČESKÝ SVAZ OCHRÁNCŮ PŘÍRODY 01/51 ZÁKLADNÍ ORGANIZACE	15.6.2012
00002244/001	TESTCOM - TECHNICKÝ A ZKUŠEBNÍ ÚSTAV TELEKOMUNIKACÍ A POŠT PRAHA	7.4.2012
00002244/002	TESTCOM - TECHNICKÝ A ZKUŠEBNÍ ÚSTAV TELEKOMUNIKACÍ A POŠT PRAHA	7.4.2012
00006199/001	BUSINESS CENTRE SERVICE A.S.	9.6.2012
00006199/002	BUSINESS CENTRE SERVICE A.S.	9.6.2012
00006199/003	BUSINESS CENTRE SERVICE A.S.	9.6.2012
00026415/001	KORN/FERRY INTERNATIONAL S.R.O. V LIKVIDACI	12.4.2012
00033997/001	HOPR GROUP, A.S.	7.6.2012
00035018/004	KRAJSKÉ STÁTNÍ ZASTUPITELSTVÍ V OSTRAVĚ	7.6.2012
00035051/002	HROCH GROUP S.R.O.	12.6.2012
00039210/001	BSC CONSULTING S.R.O.	10.5.2012
00039955/001	1. LÉKAŘSKÁ POJIŠŤOVACÍ A.S.	10.4.2012
00040222/002	TO & MI VDF. SPOL. S R.O.	11.4.2012
00040833/001	ALADIN ANTIK S.R.O.	21.3.2012
00043143/001	CEERM, S.R.O.	2.6.2012

II. SDĚLENÍ ÚŘADU

Z kontrolní činnosti Úřadu

(rok 2011)

Sdělení úvodem:
Úřad pro ochranu osobních údajů (dále jen „Úřad") prostřednictvím následujících popisů uvádí případy, které byly v roce 2011 řešeny v rámci kontrolní činnosti Úřadu. Níže uvedené stručné charakteristiky jsou pouze výběrem široce řešeného spektra problematiky, týkající se podezření na porušování zákona o ochraně osobních údajů.

Inspektoři Úřadu ukončili v roce 2011 celkem 281 kontrol; z toho kontrol zaměřených na dodržování povinností osob odpovědných za zpracování osobních údajů podle zákona č. 101/2000 Sb., o ochraně osobních údajů, v platném znění bylo ukončeno 144. Kontroly byly zahájeny jednak na základě podnětů, které Úřad obdržel, dále na pokyn předsedy Úřadu a v neposlední řadě na základě Kontrolního plánu Úřadu pro rok 2011.

Kontroly probíhaly jak ve státním, tak v soukromém sektoru, velkou část z nich tvořily kontroly shromažďování a zpracovávání osobních údajů prostřednictvím kamerových systémů. Tato problematika se objevuje v kontrolní činnosti Úřadu stále častěji. Nejedná se pouze o kamerové systémy v bytových domech, ale také kamerové systémy v prostorách různých společností, či státních úřadů.

1. Zprostředkování půjčky prostřednictvím webové stránky

Úřad obdržel v roce 2011 podnět k prošetření porušení zákona č. 101/2000 Sb., v němž bylo uvedeno, že *„Společnost při shromažďování osobních údajů zájemců o zprostředkování půjčky prostřednictvím webové stránky ve svém souhlasu se zpracováním osobních údajů neuvádí přesný účel zpracování, neuvádí identifikaci správce osobních údajů a neuvádí, na jaké období je souhlas dáván"*.

Kontrolou bylo zjištěno, že společnost při inzerci půjček na webu, v souvislosti s nezávazným posouzením možnosti půjčky, zpracovává osobní údaje zájemců v rozsahu jméno, příjmení, telefonní spojení, rodné číslo, údaj o prokazatelném čistém měsíčním příjmu, bydliště. Podle § 5 odst. 2 zákona č. 101/2000 Sb. správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat pouze z důvodů taxativně uvedených v § 5 odst. 2 písm. a) – g) tohoto zákona. V daném případě by připadalo v úvahu pouze ustanovení § 5 odst. 2 písm. b) zákona č. 101/2000 Sb., podle kterého je správce bez souhlasu oprávněn zpracovávat osobní údaje, jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření smlouvy nebo změně smlouvy uskutečněné na návrh subjektu údajů. V posuzovaném případě se nejednalo o jednání o uzavření smlouvy na návrh subjektu údajů, ale o nabídku (reklamu) správce, ještě před uzavřením samotné zprostředkovatelské smlouvy. Proto nebylo možné uplatnit některé z liberačních ustanovení § 5 odst. 2 písm. a) – g) zákona č. 101/2000 Sb., a bylo nezbytné posoudit, zda společnost informovala subjekt údajů při udělení souhlasu podle § 5 odst. 4 téhož zákona.

Podle § 5 odst. 4 zákona č. 101/2000 Sb. subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období.

Ze znění prohlášení zájemce v souvislosti s ochranou osobních údajů, uvedeného na předmětných webových stránkách, a z informací na těchto stránkách uvedených vyplynulo, že subjekt údajů před udělením souhlasu nebyl úplně informován o účelu zpracování, zájemce nevěděl, kterému správci souhlas dává a na jakou dobu. Pokud subjekt údajů není konkrétním správcem informován podle § 5 odst. 4 zákona č. 101/2000 Sb., není uvedené prohlášení zájemce platným souhlasem subjektu údajů konkrétnímu správci se shromažďováním osobních údajů ve smyslu § 5 odst. 2 věta první zákona č. 101/2000 Sb.

Podle § 11 odst. 1 a 2 zákona č. 101/2000 Sb. je správce při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech podle § 21. V případě, kdy správce zpracovává osobní údaje získané od subjektu údajů, musí subjekt údajů poučit o tom, zda je poskytnutí osobních údajů povinné či dobrovolné.

Skutečnost, že správce údajů shromažďuje osobní údaje bez toho, aby subjektu údajů bylo vůbec známo, kdo je správcem osobních údajů, a doba uchování dat, vylučuje možnost platně (určitě) informovat subjekt údajů dle § 11 odst. 1 a 2 zákona č. 101/2000 Sb., neboť musí být subjektu údajů známé, který správce osobních údajů tuto zákonnou povinnost ve vztahu k subjektu údajů vůbec plní. Rovněž musí být subjekt údajů přesně informován o účelu, pro jaký budou osobní údaje zpracovány, o právu přístupu k osobním

údajům, právu na opravu osobních údajů, jakož i o dalších právech podle § 21 zákona. Nesplnění informační povinnosti vůči subjektu údajů je porušením ustanovení § 11 odst. 1 a 2 zákona č. 101/2000 Sb. Zpracování rodných čísel zájemců o zprostředkování půjčky bylo shledáno v rozporu s ustanovením § 13c zákona o evidenci obyvatel, neboť platný souhlas podle § 5 odst. 4 zákona č. 101/2000 Sb. nebyl subjekty údajů dán.

Společnost tak při zpracování osobních údajů zájemců o půjčku porušila zákon č. 101/2000 Sb., neboť shromažďovala osobní údaje subjektů údajů bez toho, aby jim sdělila, kdo je správcem těchto údajů, platně informovala subjekty údajů dle § 11 odst. 1 a 2 zákona č. 101/2000 Sb. a měla od subjektů údajů platný souhlas se zpracováním osobních údajů. Společnosti byla ve správním řízení udělena pokuta.

2. Kamery na finančním úřadě

Úřad obdržel žádost o provedení kontroly nevhodného umístění kamer na finančním úřadě, ve které bylo uvedeno, že *„Kamery jsou umístěné čelně proti všem schodištím uvnitř budovy. Zabírají tak pohyb všech osob na schodištích, včetně velice detailních záběrů jejich obličeje. Dále je jedna z kamer namířena z prostoru vstupní haly směrem na vstup do budovy tak, že detailně zabírá jak obličeje všech návštěvníků objektu, tak i osob ve frontě, která se u vchodu do budovy často tvoří. Kamerový systém nechrání žádný majetek ani bezpečnost osob. Množství kamer rozmístěných v budově je silně nadbytečný (každé schodiště čelně do obličeje) a nemá žádný smysluplný účel. Domnívám se, že takové umístění kamerového systému pošlapává soukromí všech návštěvníků objektu. Kamerový systém, tak jak je realizován, neplní žádný veřejný zájem (mimo monitorování pohybu všech osob po objektu) a jejich umístění je v příkrém rozporu se zákonem. Žádám vás tímto o kontrolu kamerového systému a odstranění kamer na schodištích a u vstupu do budovy“*.

Finanční úřad stanovil účel a prostředky zpracování osobních údajů kamerovým systémem se záznamem a je tedy správcem osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb. Podle § 5 odst. 2 tohoto zákona může správce zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat jen z důvodů taxativně uvedených v § 5 odst. 2 písm. a) – g) zákona. V daném případě byly osobní údaje zpracovávány bez souhlasu subjektů údajů, neboť se jednalo o zpracování 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 na ochranu jeho soukromého a osobního života [§ 5 odst. 2 písm. e) zákona č. 101/2000 Sb.].

K přiměřenosti použití kamerového systému ve vnitřních prostorách budovy bylo třeba uvést, že finanční úřady, které sídlí v budově s předmětným kamerovým systémem, přijímají hotovost, která může činit denně až několik desítek milionů korun, a je tedy třeba provést takové opatření, které jednak preventivně působí k tomu, aby v budově nedocházelo k majetkové trestné činnosti, jednak je schopno případnou majetkovou trestnou činnost dokumentovat. Uvedené opatření tak obdobně platí i pro konflikty (protiprávní jednání), ke kterým dochází v souvislosti se specifikou činností finančních úřadů. Kamerový systém tak slouží k ochraně majetku správce a klientů finančních úřadů a zajištění bezpečnosti zaměstnanců a klientů finančních úřadů. Takový účel však nebylo možné dovodit u některých kamer umístěných v učebně, a to bez ohledu na skutečnost, zda je učebna používána pouze pro zaměstnance, či i pro osoby, které nejsou zaměstnanci úřadu, a dále také u kamer na schodišti. U venkovních kamer pak bylo možné za odpovídající stanovenému účelu hodnotit monitorování vlastního majetku včetně pláště budovy a nejbližšího okolí (travnaté plochy před budovou, ze kterých by mohlo dojít k vniknutí do budovy), nikoliv však monitorování veřejných prostor používaných občany (chodníky, komunikace). Z uvedených důvodů u venkovních kamer, které snímaly výhradně veřejné prostory, se jednalo o shromažďování osobních údajů bez právního důvodu.

Kontrolou bylo zjištěno, že finanční úřad prostřednictvím některých kamer zpracovával osobní údaje fyzických osob z důvodu uvedeného v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Nad rámec tohoto zákonného důvodu byly bez souhlasu subjektů údajů zpracovávány osobní údaje fyzických osob tím, že bylo částečně monitorováno okolí budovy (veřejné prostory – komunikace, chodníky), které užívá veřejnost, a to některými venkovními kamerami. Zcela bez právního důvodu jedna kamera snímala výhradně veřejný prostor (křižovatka komunikace). Tím došlo k porušení právní povinnosti správce osobních údajů podle § 5 odst. 2 věta první zákona č. 101/2000 Sb. U vnitřních kamer nebylo stanoveným účelem odůvodněno zpracování osobních údajů kamerovým systémem se záznamem v učebně. Za uvedené porušení zákona č. 101/2000 Sb. byla finančnímu úřadu uložena pokuta.

3. Zneužití důvěry klienta

Inspektor Úřadu pro ochranu osobních údajů na základě stížnosti provedl kontrolu ve společnosti, jejímž předmětem podnikání je zprostředkování půjček a zpracovávání návrhu na oddlužení. Tato činnost zahrnuje předávání osobních údajů zájemců/klientů o nabízené služby nejen kontrolovanému, ale i dalším subjektům.

Stížnost směřovala na předání osobních údajů stěžovateli za provizi, s poukázáním na neoprávněně zaslané osobní údaje třetí osobě, tj. samému stěžovateli.

Kontrolou byla potvrzena oprávněnost stížnosti. V konečném závěru však bylo prokázáno individuální pochybení zaměstnance, nikoli společnosti, tedy porušení § 15 zákona

č. 101/2000 Sb. Zaměstnanec kontrolované společnosti porušil vnitřní postupy společnosti, zákon o ochraně osobních údajů a jeho chování bylo hrubým porušením důvěry klienta, který ve své obtížné životní situaci vyhledal profesionální pomoc. Snaha využít problému klienta k obohacení je nepřípustná nejen z právního, ale i morálního hlediska. Pokuta za porušení zákona č. 101/2000 Sb. byla vyměřena ve správním řízení zaměstnanci společnosti.

4. Pořizování a zveřejňování videozáznamů z jednání zastupitelstva

Předmětem kontroly bylo plnění povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů prostřednictvím videozáznamu z průběhu jednání zastupitelstva, zpřístupněného prostřednictvím webových stránek města.

Kontrolou bylo zjištěno, že kontrolované město porušilo, v souvislosti se zpracováním osobních údajů prostřednictvím videozáznamu z průběhu jednání zastupitelstva, ustanovení § 5 odst. 2 a § 11 odst. 1 zákona č. 101/2000 Sb. Kontrolující inspektor se rovněž zabýval otázkou dopadů zjištěného protiprávního jednání kontrolovaného do soukromí dotčených fyzických osob, které se účastnily jednání zastupitelstva, které bylo natáčeno videotechnikou, a následně byl záznam zpřístupněn na webu města a dále mírou společenské nebezpečnosti tohoto jednání tím, že jako správce při zpracovávání osobních údajů porušilo § 5 odst. 2 a § 11 odst. 1 zákona č. 101/2000 Sb. a dospěl k následujícímu závěru: S ohledem na skutečnost, že z jednání zastupitelstva byl uskutečněn on-line přenos do internetové sítě a tudíž z tohoto jednání si mohl kdokoliv pořizovat záznam, byla míra společenské nebezpečnosti následného zpřístupnění tohoto záznamu na webových stránkách města, shledána jako sporná. Jinými slovy, kontrolující inspektor dospěl k závěru, aby mohlo být konstatované protiprávní jednání kvalifikováno jako správní delikt, musela by být kromě formálních znaků deliktního jednání naplněna i materiální stránka deliktu. Z toho důvodu nebylo ve věci Úřadem zahájeno správní řízení.

S ohledem na oprávněný zájem občanů o dění v obecních zastupitelstvech a s odkazem na § 97 zákona o obcích, který říká, že „obec informuje občany o činnosti orgánů obce na zasedání zastupitelstva obce a dále jiným způsobem v místě obvyklým“, konstatoval kontrolující inspektor, že při absenci příslušné právní úpravy, která by jednoznačně řešila provádění audio nebo video záznamu z jednání zastupitelstva pro účely následného informování veřejnosti, a s ohledem na skutečnost, že platná právní úprava zákona o obcích byla koncipována v roce 1991, tedy v době neznalosti možností a vlastností internetu, a s ohledem na změnu společenského vývoje od doby vydání tohoto zákona, lze tento § 97 použít přiměřeně při respektování ochrany osobnosti podle § 12 zákona č. 40/1964 Sb., Občanský zákoník.

5. Používání vzdáleného přístupu k počítači obecního úřadu starostou obce

Předmětem kontroly bylo dodržování povinností správcem osobních údajů stanovených zákonem č. 101/2000 Sb. se zaměřením na shromažďování a zpracování osobních údajů prostřednictvím systémů informačních technologií nainstalováním aplikace programu Team Viewer 6.

Kontrola byla zahájena na základě podnětu bývalého zaměstnance obecního úřadu.

V podnětu stěžovatel uvedl, že starosta obce nechal do PC, jehož byl stěžovatel uživatelem a denně na něm prováděl účetnictví obce, spisovou službu, evidenci obyvatel, elektronické bankovnictví atd., nainstalovat aplikaci programu Team Viewer 6 – vzdálený přístup (dále jen „aplikace“). Dle názoru stěžovatele ohrožovala uvedená aplikace osobní i obchodní údaje uložené v PC obce a byla v rozporu se zákony.

Obec určila účel zpracování osobních údajů, kterým bylo vedení agend v programech umístěných na PC obce souvisejících s evidencí majetku, evidencí obecních smluv, evidencí obyvatel, evidencí zaměstnanců obce a vedení dalších agend za účelem výkonu státní správy. Z kontrolních zjištění vyplynulo, že stěžovatel měl určena samostatně jména a přístupová hesla k programu Helios-Fenix s dálkovým přístupem do účetního software SUCÚIS, ke mzdovému programu, programu elektronická úřední deska a elektronické bankovnictví obce. Další programy nebyly chráněny samostatným přístupovým heslem. Jednalo se o spisovou službu, evidenci písemností, evidenci majetku, inventarizaci, evidenci obecních smluv, evidenci obyvatel, program Office a program Outlook pro elektronickou poštu. V daném případě měl starosta obce možnost připojit se vzdáleným přístupem pouze k programům, u nichž neměl stěžovatel určená vlastní hesla a s nimiž mohl pracovat pomocí vzdáleného připojení tak, jako na PC v prostorách obecního úřadu, v souladu s výkonem funkce starosty. Kontrolou nebylo zjištěno, že by byly zaznamenány pokusy o narušení přístupu k programům, k nimž měl stěžovatel určena vlastní přístupová hesla. V daném případě se také nejednalo o skryté napojení do PC stěžovatele, který měl informaci, že se někdo vzdáleně do PC připojil, a měl možnost jeho připojení odmítnout nebo v případě již probíhajících připojení tato připojení přerušit a ukončit. Využití aplikace vzdáleného přístupu Team Viewer 6 na PC obce starostou obce jako statutárního zástupce obce, bylo dle názoru kontrolujících možné, nikoliv však zcela standardní. Starosta obce vzdálený přístup na PC obce využíval v souvislosti s výkonem svojí funkce. Vzdáleným připojením starosty k PC stěžovatele se neprokázalo, že by došlo ke zneužití osobních údajů, které byly v PC uloženy.

Na základě shromážděných důkazů vyhodnotili kontrolující zjištěné skutečnosti tak, že dospěli k závěru, že obec neporušila ustanovení zákona č. 101/2000 Sb. v souvislosti

s využitím aplikace vzdáleného přístupu Team Viewer 6 na PC obce.

6. Kamerový systém v provozovně společnosti

Úřad obdržel stížnost, jež byla podána více stěžovateli, kteří ve svém podnětu uvedli, že ve společnosti je nainstalována kamera, a to na střeše přístřešku provozovny společnosti monitorující pozemky ve vlastnictví stěžovatele a dalších osob, kteří na žádost stěžovatele o vysvětlení způsobu fungování kamerového systému nereagovali. Inspektor Úřadu provedl kontrolu, jejímž předmětem bylo dodržování povinností stanovených zákonem č. 101/2000 Sb. se zaměřením na ochranu osobních údajů zpracovávaných prostřednictvím kamerového systému, instalovaného v provozovně kontrolované společnosti.

V průběhu kontroly bylo zjištěno, že kamery snímají pouze venkovní prostor. Nahrávání probíhá na jednotlivých kamerách pouze při pohybu. Videonahrávky jsou uchovávány po dobu tří dnů, aby mohl správce kontrolovat detekci pohybu přes víkend. Poté jsou nahrávky automaticky smazány. Zóny detekce pohybu jsou nastaveny tak, aby striktně dodržovaly hranice pozemku. Kamera snímající vjezd do areálu a příjezdovou cestu s bránou na sousední pozemek má nastavenu oblast detekce pohybu na hranici pozemku správce, tudíž při vstupu na sousední pozemek není aktivován záznam. Tato tvrzení byla kontrolujícímu při ústním jednání předvedena a též doložena prostřednictvím záznamů z jednotlivých kamer.

V průběhu kontroly si kontrolovaný doplnil registraci zpracování osobních údajů v registru vedeném Úřadem.

Inspektor konstatoval, že kamerový systém kontrolovaného je nastaven v souladu s povinnostmi správce údajů uvedenými v § 5 a násl. zákona č. 101/2000 Sb.

Kontrolovaný stanovil účel zpracování „ochrana a kontrola jeho majetku“ s tím, že záznam je pořizován pouze v zóně detekce pohybu, která je omezena na nemovitosti v majetku kontrolovaného, což je v souladu se zněním § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.; záznamy jsou automaticky mazány po uplynutí tří dnů, což je v souladu se zněním § 5 odst. 1 písm. e) téhož zákona; zaměstnanci kontrolovaného vyjádřili souhlas s použitím kamer k ochraně majetku, tj. právem chráněného zájmu správce; klienti a návštěvy kontrolovaného jsou upozorněni na pořizování záznamu tabulkou s textem „Objekt je střežen kamerovým systémem“, což odpovídá povinnosti správce, jak ji stanoví § 11 zákona č. 101/2000 Sb., případným dalším příjemcem zpracovávaných osobních údajů je pouze Policie České republiky; správce v průběhu kontroly též splnil oznamovací povinnost ve smyslu § 16 zákona č. 101/2000 Sb.

Kontrolovaný provádí zpracování osobních údajů v souladu s povinnostmi správce stanovenými zákonem č. 101/2000 Sb.

Vzhledem k tomu, že kontrolovaný si v průběhu kontroly doplnil registraci zpracování osobních údajů, neuložil inspektor Úřadu v souladu s ustanovením § 40 odst. 1 zákona č. 101/2000 Sb. opatření, ani pokutu ve správním řízení.

7. Kontrola zaměřená na bezpečnost provozovaných webových stránek

Inspektor Úřadu provedl kontrolu společnosti, jejímž podnětem byla stížnost, ve které stěžovatel uvedl, že je registrovaným uživatelem webu www.xxx.cz. Po přihlášení k jeho účtu a následném obnovení stránky docházelo k přihlášení k náhodným účtům jiných registrovaných uživatelů tohoto webu. Tudíž stěžovatel mohl vidět objednávky a kontaktní informace těchto uživatelů. A stejně tak mohli jiní vidět jeho údaje a objednávky.

Kontrolovaný k danému případu uvedl, že došlo k softwarové chybě, ale nedošlo k úniku dat z databáze. Dále sdělil, že po přihlášení k uživatelskému účtu se vytvoří virtuální prostor, který není shodný s databází. Každý uživatel má vytvořený svůj vlastní virtuální prostor. V inkriminovanou dobu se stalo, že aplikace odpovědná za vytváření virtuálních prostorů přestala pracovat a nebyl každému vytvořen jeho vlastní nový virtuální prostor, ale byl použit již předešlý virtuální prostor vytvořený pro jiného uživatele. Z tohoto důvodu mohli uživatelé vidět účty jiných uživatelů. V uvedené době nebylo možné si nic objednávat. Objednávka byla v systému vidět, ale nedala se dokončit. Problém trval v určitý den od 12:15 do 13:30. Byl proveden restart systému, ten však problém nevyřešil, a proto byla činnost stránky v tento den ve 13:30 zastavena. V současné době je součást systému, která způsobila daný problém, ze systému odstraněna.

Kontrolovaný prostřednictvím webového rozhraní a svých webových stránek shromažďuje a zpracovává osobní údaje svých klientů. Účet klienta (uživatele) obsahuje kontaktní údaje – zejména jméno, příjmení, poštovní adresa, e-mailová adresa, dále informace o posledních objednávkách, slevách apod., tedy osobní údaje ve smyslu ustanovení § 4 písm. a) zákona č. 101/2000 Sb.

Z podané stížnosti, z vyjádření uživatelů v rámci diskuse mezi provozovatelem www.xxx.cz a uživateli na http://www.facebook.com/pages/xxx a z vyjádření kontrolovaného je zřejmé, že dne 1. října 2010 od 12:15 do 13:30 bylo možné, aby přihlášení uživatelé viděli účty jiných uživatelů.

Kontrolovaný subjekt tak jednoznačně porušil ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. tím, že nepřijal taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, a to nezjištěnému počtu třetích osob (minimálně však stěžovateli).

Kontrolovaný tím spáchal správní delikt podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., neboť nepřijal nebo neprovedl opatření pro zajištění bezpečnosti zpracování

osobních údajů, za což mu v souladu s § 45 odst. 3 zákona č. 101/2000 Sb. byla uložena pokuta.

8. Kontrola obchodního rejstříku (elektronické podoby obchodního rejstříku dostupné přes webový portál www.justice.cz)

Webový portál obchodního rejstříku je významným veřejným informačním systémem, jehož závažnost je potvrzena důležitostí pro e-Government. Prostřednictvím tohoto portálu dochází ke zpracovávání osobních údajů na internetu, kde je přítomné vyšší riziko zneužití osobních údajů. Kontrolující při této kontrole vycházeli kromě zákona č. 101/2000 Sb. zejména z čl. 2 odst. 3 Ústavy ČR, podle kterého *„státní moc slouží všem občanům a lze ji uplatňovat jen v případech, mezích a způsoby, které stanoví zákon“*.

Kontrola předně upozornila na to, že každé zpracování osobních údajů musí mít svého správce, který je za toto zpracování zodpovědný, a této odpovědnosti se nelze zříci. Správcem je v tomto případně Ministerstvo spravedlnosti. Ministerstvo tudíž zodpovídá za to, že rozsah zveřejňovaných údajů a doba, po kterou jsou zveřejňovány, odpovídá účelu zpracování. Webový portál www.justice.cz má sloužit jako informace o obchodních společnostech a řídí se Směrnicí Evropského parlamentu a Rady 2009/101/ES ze dne 16. září 2009, *o koordinaci ochranných opatření, která jsou na ochranu zájmů společníků a třetích osob vyžadována v členských státech od společností ve smyslu čl. 48 druhého pododstavce Smlouvy, za účelem dosažení rovnocennosti těchto opatření*. U všech ostatních dokumentů, které obsahují osobní údaje, je třeba zvažovat, zda jsou nezbytné k výše danému účelu z hlediska zákona č. 101/2000 Sb. Podobně doba jejich uchovávání na webovém portálu musí být nezbytná k účelu, tj. informovanosti třetích osob.

Dále kontrola poukázala na problematiku zveřejňování rodného čísla na webovém portálu. V této souvislosti je možno uvést, že se podařilo do připravované novely zákona č. 513/1991 Sb., obchodní zákoník, doplnit ustanovení k § 28 odst. 1, a to tak, že se doplňuje věta *„Rodné číslo se zapisuje do obchodního rejstříku, neuvádí se však ve výpisu z obchodního rejstříku ani se nezveřejňuje v Obchodním věstníku“*.

Dále kontrola připomněla problematiku „personálního indexu“, neboť účelem obchodního rejstříku je poskytnutí informací o obchodních společnostech k ochraně zájmů společníků a třetích osob v souvislosti s obchodováním, resp. podnikáním. Vyhledávání podle jména a příjmení fyzické osoby, a to nejen v obchodním rejstříku, ale zároveň i např. v nadačním rejstříku a rejstříku bytových družstev, je zpracování osobních údajů k jinému účelu. Personální index v současné době již není na webovém portálu obchodního rejstříku dostupný.

Zkvalitnění právní úpravy ve výše uvedených ustanoveních bylo kontrolou shledáno jako zásadní vzhledem k ustanovení § 5 odst. 3 zákona č. 101/2000 Sb., které ukládá, že *„provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů“*.

Zpracování osobních údajů z obchodního rejstříku formou webového portálu si tudíž zaslouží jasná pravidla včetně odpovědnosti Ministerstva spravedlnosti, která jsou v souladu s principy ochrany osobních údajů. Současný stav právní úpravy, kdy dochází ke zpracování osobních údajů pouze na základě obecných ustanovení § 27 a 28 obchodního zákoníku a ustanovení § 5 odst. 5 zákona o svobodném přístupu k informacím, nezohledňuje principy ochrany osobních údajů.

9. Vymahačská společnost působící přes internet

V roce 2011 přišlo několik stížností na činnost Společnosti, která se snažila vyvolat dojem seriózní firmy zajišťující vymožení dluhu bez zbytečných formalit. Jako hlavní nástroj pro vymožení dluhu používala Společnost veřejný „registr dlužníků“ přístupný prostřednictvím internetu.

Na základě dotazníku, který vyplnil věřitel a uvedl v něm svého údajného dlužníka, se Společnost pokoušela dluh vymoci – často pouze zasláním dopisu, případně se skrytou výhružkou. Hlavním nástrojem byl však „registr dlužníků“. V mandátní smlouvě, automatizovaně vystavené na základě vyplněného dotazníku, byl generován určitý kód, který měl identifikovat smluvní strany a měl nahradit právoplatný podpis.

Z hlediska ochrany osobních údajů je ale třeba se ptát, na základě jakého právního titulu byly zpracovávány osobní údaje dlužníků.

Relevantní ustanovení zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, umožňuje postoupení pohledávky někomu jinému bez vědomí dlužníka. Podmínkou ovšem je, že postupitel musí dlužníkovi postoupení pohledávky oznámit nebo postupník postoupení pohledávky musí dlužníkovi prokázat, neboť dle § 526 odst. 1 občanského zákoníku platí, že *postoupení pohledávky je povinen postupitel bez zbytečného odkladu oznámit dlužníkovi. Dokud postoupení pohledávky není oznámeno dlužníkovi nebo dokud postupník (nový věřitel) postoupení pohledávky dlužníkovi neprokáže, zprostí se dlužník závazku plněním postupiteli.*

Další možností by bylo uzavřít mandátní smlouvu mezi věřitelem a Společností o vymožení dluhu. Při uzavření této smlouvy ovšem, jako při každé jiné smlouvě, musí být obě strany jednoznačně identifikovány. Uzavíraní smlouvy prostřednictvím pouhého „zakliknutí“ v počítačovém programu, kdy není věřitel nepochybně identifikován, a tudíž Společnost nemá možnost si ověřit, že se jedná o skutečnou osobu věřitele a o skutečný dluh, je právně problematické.

Tento způsob uzavírání právního vztahu v sobě totiž nese velkou míru právní nejistoty do budoucna, je tedy problematickým právním základem pro zpracování osobních údajů. Lze tudíž jen doporučit, aby smlouvy v obdobných případech v prostředí internetu byly elektronicky podepsané.

V případě Společnosti dospěli kontrolující ke zjištění, že ke zpracování osobních údajů dlužníků neexistuje žádný právní titul, neboť souhlas dlužníka evidentně chybí (srov. ustanovení § 5 odst. 2 zákona č. 101/2000 Sb.).

Navíc bylo zasahováno do osobnostních práv osob, které byly prostřednictvím registru dlužníků označeny za dlužníky, aniž by o jejich případném dluhu měla Společnost relevantní důkazy.

Společnost následně ukončila svou činnost.

10. Kamery v obchodním centru

Na základě stížnosti Stálé komise Senátu pro ochranu soukromí, ze které vyplývalo podezření na porušování zákona č. 101/2000 Sb., a to v souvislosti se zneužíváním kamerových záznamů k propouštění některých zaměstnanců z pracovního poměru a dále neplnění informační a oznamovací povinnosti správce kamerového systému, byla provedena kontrola v jednom obchodním centru (dále jen „OC“).

Šetřením byly zjištěny tyto skutečnosti: Účelem pořizování kamerového záznamu (zpracovávání osobních údajů) je bezpečnost osob a ochrana majetku. Záznamy z kamerového systému se uchovávají po dobu 14 dnů. Areál OC je rozlehlý, OC se nachází ve čtyřpatrové budově.

V OC je umístěno 111 kamer. Informace o pořizování kamerového záznamu je umístěna na vchodech do objektu (někde je i obrazovka, na které běží on-line záběry z kamery). Kontrolující se seznámili s chodem tzv. velína, kde jsou sledovány jednotlivé kamery. Bylo zjištěno, že ke kamerovému záznamu je možný přístup pouze po zadání hesla. Přístup k záznamu má pouze „velínář“, vedoucí útvaru G4S v OC a ředitel centra OC. Každá z těchto osob má upraveno oprávnění vzhledem k rozsahu pravomocí své pracovní pozice. V případě mimořádné události se pořizuje výpis ze záznamu z kamerového systému, a to na základě požadavku na vytvoření/zhlédnutí obrazového záznamu z uzavřeného kamerového systému. Zde se uvádějí údaje o osobě, která o záznam požádala, dále jaké věci (případně jakého trestného činu) se záznam týká, služební číslo policisty, důvod požadavku, doba a místo, ze kterého je obrazový záznam požadován. O pořízení kamerového výpisu se dále sepisuje protokol o převzetí výpisu z obrazového záznamu z uzavřeného kamerového systému.

V tomto protokolu se uvádějí následující údaje: jméno a příjmení žadatele (pokud jde o policistu, jeho služební číslo), kdy byl požadavek na záznam doručen, kdo požadavek schválil, kdo výpis provedl, na jaké médium byl uložen, počet kamerových záznamů, z kterého dne je záznam pořizován a jeho délka a dále kdo záznam převzal. Jednotlivé vstupy v souvislosti s nahlížením a pořizováním kamerového výpisu jsou logovány, avšak záznam o tomto je uchováván jen po dobu 14 dnů, seznam přístupů se pak maže společně se záznamem.

Právním titulem pro zpracovávání osobních údajů je souhlas subjektu údajů anebo právní důvod přímo citovaný v zákoně. V posuzovaném případě se jedná o zpracovávání osobních údajů bez souhlasu, proto musí dané zpracovávání osobních údajů vyhovět podmínkám ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. „*Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat, 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*.“

Z výše uvedeného vyplývá, že právě hlediska:

a) zda daný prostředek zasahuje do základních práv a svobod,
b) zda v konkrétním případě jiný právem chráněný zájem převáží nad právem na ochranu soukromí,
c) zda právě záznam z kamerového systému je jediný a nejvhodnější prostředek pro ochranu takového zájmu,
d) zda záznam z kamerového systému je schopen naplnit deklarovaný účel,

jsou při kontrole Úřadem rozhodující pro posouzení legálnosti použití kamerového systému. Účelem, pro který v daném případě dochází ke zpracování osobních údajů, je ochrana osob a majetku. Jak bylo předesláno, OC je rozsáhlý komplex, který se rozprostírá ve čtyřpodlažní budově. Společnost je odpovědná za zajištění bezpečnosti osob a ochranu majetku v tomto komplexu. Dle slov zástupců kontrolovaného docházelo k občasnému poškození majetku a ohrožení osob (nehody v garážích, krádeže, poškozování vstupních dveří). Rozsah zpracovávaných osobních údajů musí být dle ustanovení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. minimální vzhledem k danému účelu. Tudíž je nutné ověřit, zda je opravdu každá kamera nezbytná a zda uchovávané záběry z ní nezasahují v míře neúměrné sledovanému účelu do soukromí osob. Určité pochybnosti nastávají v případě otočné kamery, která sleduje také restaurační prostory a lze při využití zoomu velmi dobře sledovat jednotlivé návštěvníky, nicméně i zde je možno přihlížet k tomu, že se tu občas zdržují osoby bez domova a dochází k obtěžování hostů a ke krádežím. Vzhledem ke zmíněnému je tedy účel zpracovávání osobních údajů legitimní a v souladu s ustanovením § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Správce musí plnit všechny povinnosti uvedené v ustanovení § 5 odst. 1 zákona č. 101/2000 Sb., včetně stanovení

doby nezbytné pro uchovávání záznamů z kamer. Ta je obecně Úřadem doporučena maximálně jako týdenní.

Záznamy nesmějí být použity k žádnému jinému účelu, než ke kterému byly pořízeny – ochraně majetku společnosti a bezpečnosti zákazníků. S tím úzce souvisí bezpečnost uchovávaných záběrů z kamer. Oprávnění vstupovat do záznamů z kamer je možné pouze v případě porušení právem chráněného zájmu, např. dojde ke krádeži, rozbití dveří, ohrožení zákazníků. Stejně tak je možno záznamy z kamer předávat v těchto případech Policii ČR, avšak na základě písemné žádosti včetně odůvodnění této žádosti, jímž je vyšetřování konkrétního protiprávního jednání. Dokonce ani správce objektu nemá právo nahlížet do záznamů bez důvodu, spočívajícím v nahlášeném protiprávním jednání.

Při automatizovaném zpracovávání vyplývá správci nebo zpracovateli navíc povinnost *pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány* – tzv. logování [§ 13 odst. 4 písm. c) zákona č. 101/2000 Sb]. S ohledem na ochranu osobních údajů není dokumentace, kdy jsou logy po 14 dnech mazány, odpovídající, neboť společnost v případě porušení zákona č. 101/2000 Sb. v souvislosti s neoprávněným nakládáním se záznamy z kamerového systému nebude schopna po 14 dnech identifikovat, resp. ověřit, kdy, kdo a z jakého důvodu se záznamem pracoval, což je proti smyslu uvedeného ustanovení, a tudíž nejsou dostatečně splněna opatření k ochraně osobních údajů. Dobu logování vstupů ke kamerovým záznamům je tedy nezbytné prodloužit, a to minimálně na dobu 3 měsíců.

Základní informační povinnost v souladu s ustanovením § 11 zákona č. 101/2000 Sb. byla splněna, neboť vstupující zákazníci jsou informováni o kamerovém systému se záznamem prostřednictvím informačních tabulí. Informační tabulky je však třeba doplnit o odkaz, kde se mohou lidé dozvědět všechny informace, které má správce povinnost sdělit, např. prostřednictvím odkazu na www stránky.

Zneužívání kamerového záznamu za účelem rozvázání pracovního poměru se zaměstnanci nebylo zjištěno.

11. Poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím stavebním úřadem

Úřad obdržel stížnosti týkající se poskytnutí osobních údajů žadatelů o poskytnutí informací dle zákona č. 106/1999 Sb. vedoucím stavebního úřadu starostovi obce, který je následně zveřejnil v místním zpravodaji. Vedoucí stavebního úřadu, při vyřizování žádostí žadatelů o poskytnutí informací dle zákona č. 106/1999 Sb., zaslal starostovi obce na vědomí odpovědi, společně s kopií žádostí, v mylném domnění, že se jedná o účastníka řízení. Osobním údajem je podle ustanovení § 4 písm. a) zákona č. 101/2000 Sb. *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů“,* tudíž i obsah dopisu, který určitý subjekt napsal. Podle ustanovení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. smí správce shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění tohoto účelu. V tomto případě se jedná o zpracování výhradně pro evidenci žadatelů o informace dle zákona o svobodném přístupu k informacím a dále pro odpověď žadateli. Podle ustanovení § 13 zákona č. 101/2000 Sb. je *„správce povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům“*. Kontrolou bylo zjištěno, *že* vedoucí stavebního úřadu postupoval v rozporu s tímto ustanovením, neboť osobní údaje žadatelů o informace (jméno, příjmení, bydliště a text žádosti) poskytl třetí osobě, konkrétně starostovi obce, který nebyl oprávněn k přístupu k těmto datům. Ustanovení § 5 odst. 3 zákona č. 106/1999 Sb., ukládá sice povinnému subjektu zveřejnit do 15 dní formou dálkového přístupu odpověď na žádost, ovšem bez osobních údajů a pouze odpověď, nikoli samotnou žádost či jakékoli osobní údaje žadatele.

Správní delikt podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. byl řešen pokutou.

12. Uzavírání pracovních smluv

Inspektor Úřadu provedl kontrolu potravinářské společnosti, zaměřenou na shromažďování a zpracovávání osobních údajů v rámci jednání o uzavření pracovního poměru. Společnost při výběrovém řízení na pozice řezník nebo prodavačka požadovala poskytnutí takových osobních údajů, jako jsou např. informace o pracovní neschopnosti v posledním roce, rodinný stav nebo počet dětí, zda je adept kuřák či nikoli, aniž by subjektu údajů poskytl informace o zpracování osobních údajů v souvislosti s výběrem a přijímáním nových zaměstnanců podle ustanovení § 11 odst. 1 a odst. 2 zákona č. 101/2000 Sb.

Především je pak ale takovéto vyžadování osobních údajů v závažném konfliktu se zákoníkem práce. Lze totiž poukázat na § 4 odst. 2 zákona č. 435/2004 Sb., podle kterého *„při uplatňování práva na zaměstnání je zakázána přímá i nepřímá diskriminace z důvodu pohlaví, sexuální orientace, rasového nebo etnického původu, národnosti, státního občanství, sociálního původu, rodu, jazyka, zdravotního stavu, věku, náboženství či víry, majetku, manželského a rodinného stavu nebo povinností k rodině, politického nebo jiného smýšlení, členství a činnosti v politických stranách nebo politických hnutích, v odborových organizacích nebo organizacích zaměstnavatelů…,“ atd.*

Dle § 12 stejného zákona, a to odst. 1 *„Účastníkům právních vztahů vznikajících podle tohoto zákona je zakázáno činit nabídky zaměstnání, dále informace, které odporují dobrým mravům, a také osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených zvláštním právním předpisem. Na žádost uchazeče o zaměstnání je zaměstna-*

vatel povinen prokázat potřebnost požadovaného osobního údaje. Hlediska pro výběr zaměstnanců musí zaručovat rovné příležitosti všem fyzickým osobám ucházejícím se o zaměstnání. Ustanovení § 4 odst. 3 platí i zde."

Konečně je pak třeba poukázat na § 30 odst. 2 zákoníku práce, dle kterého *„Zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy."*

Při provedené kontrole tak informace o poslední pracovní neschopnosti uchazeče (zájemce o zaměstnání) ani výše uvedené další požadované údaje nebyly vyhodnoceny jako nezbytné pro naplnění stanoveného účelu. Inspektorem bylo tedy zjištěno porušení povinnosti porušení § 5 odst. 2 zákona č. 101/2000 Sb., navíc s přihlédnutím k dikci § 5 odst. 4 zákona č. 101/2000 Sb. je jasné, že kontrolovaná společnost souhlas se zpracováním předmětných údajů neprokázala.

13. Identifikační náramky pacientů v nemocnici

Inspektorka Úřadu provedla v souladu s plánem kontrolní činnosti na rok 2011 kontrolu dodržování povinností správce osobních údajů v souvislosti s používáním pasivních identifikačních náramků v jedné z pražských nemocnic. Předmět kontroly byl rozšířen v průběhu kontroly na základě stížnosti, kterou Úřad obdržel, v níž stěžovatel doložil záznam z internetu, na kterém byl zveřejněn záznam ze zákroku, a na kterém je zobrazeno rodné číslo pacienta, včetně části jeho jména i příjmení.

V průběhu kontroly bylo zjištěno, že pasivní identifikační prvky (identifikační náramky) obsahují informace, které jsou na nich umístěné, ve formě samolepky vytištěné z informačního systému nemocnice. Při příjmu pacienta k hospitalizaci je pacient vybaven identifikačním štítkem s údaji: jméno pacienta, datum narození, čárový kód obsahující číslo pacienta z registru pacientů nemocnice, potřebnými pro jeho identifikaci. Sestra na oddělení, na které je pacient přijat, nalepí tento štítek na identifikační náramek, umístěný na zápěstí pacienta. Standardně se v nemocnici používá náramek modré barvy, pro pacienty s vyšším rizikem upadnutí náramek žluté barvy. Údaje na náramku jsou jeden ze základních prostředků zajištění kvality a bezpečnosti pacienta při jeho pobytu v nemocnici. Kontrolou údajů na identifikačním náramku se zajistí, aby nedošlo k záměně pacientů nebo přiřazení výsledků vyšetření k dokumentaci jiného pacienta. Mají zcela zásadní funkci při provádění diagnostických nebo léčebných výkonů, a to zejména mimo příslušné oddělení, na kterém je pacient hospitalizován (zobrazovací vyšetřovací metody, laboratorní vyšetření, operační zákrok atp.). Nezastupitelnou úlohu mají při identifikaci dezorientovaných či zmatených pacientů a pacientů pod vlivem léčiv (celková anestézie apod). Všechny údaje uvedené na náramku jsou automaticky i součástí každého listu zdravotnické dokumentace. Čárový kód na náramku je možno snímat pouze na vzdálenost cca 10–20 cm při přímé viditelnosti, což vylučuje možnost sledování pohybu pacienta v areálu nemocnice.

Kontrolovaná nemocnice byla od roku 2005 držitelem certifikátu kvality, který uděluje mezinárodní organizace a certifikát je platný po dobu 3 let. V roce 2011 proběhl v nemocnici druhý certifikační audit s vynikajícím výsledkem. Nemocnice musela prokázat naplnění kapitoly Mezinárodní bezpečnostní cíle. Jedním z těchto cílů je právě bezpečná identifikace pacienta, aby byla vyloučena jeho záměna s jiným pacientem, což je také požadavek zřizovatele nemocnice, kterým je Ministerstvo zdravotnictví ČR.

Nemocnice má vypracovány vnitřní předpisy (zdravotnické a organizační směrnice) upravující ochranu osobních údajů a pacientských dat. Vnitřní předpisy obsahují postupy, jejichž dodržování je povinné pro všechny zaměstnance nemocnice, povinnost řídit se vnitřními předpisy a zachovávat mlčenlivost je ukotvená v Pracovním řádu.

Systém identifikace pacientů včetně identifikace prostřednictvím pasivních náramků je vytvořen a spravován vlastním IT oddělením nemocnice, nikoliv třetím subjektem. Nemocniční informační systém (dále jen „NIS") včetně jeho databází obsahujících osobní údaje je spravován z technického hlediska oddělením informatiky nemocnice nikoliv třetím subjektem. Ve vztahu k přístupu třetích subjektů do NISu za účelem údržby NISu a řešení komplikovaných provozních problémů NISu, mohou mít některé třetí subjekty, resp. jejich oprávnění zaměstnanci, přístupová oprávnění do aplikačního prostředí, avšak tyto třetí osoby nejsou oprávněny nahlížet či zapisovat do datového skladu, v němž se osobní údaje nachází. Pouze IT oddělení je správcem a administrátorem databází s pacientskými daty.

Administrátorská oprávnění k přístupu do databází NISu obsahující osobní údaje pacientů mají někteří zaměstnanci oddělení informačních technologií nemocnice. Tito pracovníci mohou nakládat s databázemi jen pomocí programového vybavení k tomu určenému a v rozsahu svých oprávnění, která jsou omezená. Nemocnice v přijaté vnitřní směrnici popisuje organizační strukturu oddělení informatiky, včetně zabezpečení prostor elektronickým zabezpečovacím systémem a přístupu osob do kancelářských prostor oddělení informatiky.

Řízení informací je popsáno organizační směrnicí, která definuje procesy tvorby, správy, ochrany a zabezpečení a využití informací vznikajících nebo využívaných v nemocnici. Stanoveno je zároveň předávání a uchovávání informací týkajících se vzdělávání a školení personálu, včetně příslušných zásad a postupů a dostupnost těchto informací pro všechny zaměstnance, uchovávání audio/video materiálů, zabezpečení přístupu k datům – definování přístupových práv, zásady a postupy vymezující mechanismy přijaté k ochraně a auto-

matickému zabezpečení dat a informací proti ztrátě, zničení a neoprávněným zásahům, monitorování užívání informací v elektronické podobě tak, aby bylo vždy možné dohledat, kdo a kdy k chráněné informaci přistupoval, tzv. logování.

K záznamu z lékařského zákroku uveřejněnému na internetu a zároveň zveřejněným údajům v rozsahu rodné číslo a části jména a příjmení pacienta kontrolovaný v průběhu kontroly předložil pacientem podepsaný „Souhlas pacienta k mediálnímu použití provedeného diagnostického/léčebného výkonu“, jehož součástí byl i výslovný souhlas s použitím jména, příjmení, data narození, rodného čísla, textové informace, obrazových a zvukových záznamů konkrétní podoby či podoby částí těla a dále projevu či jiných prvků osobní povahy. Kontrolovaný dále uvedl, že tento záznam byl již z internetových stránek odstraněn, jelikož nemocnice fakticky neměla v úmyslu rodné číslo příslušného pacienta zveřejňovat, a to navzdory tomu, že měla od příslušného pacienta udělen písemný souhlas.

Kontrolou bylo zjištěno, že nemocnice neporušila povinnosti správce osobních údajů při zpracování osobních údajů dle zákona č. 101/2000 Sb., v souvislosti s identifikací pacientů prostřednictvím pasivních identifikačních náramků, ani v souvislosti se zveřejněním osobních a citlivých údajů pacienta na internetu.

14. Změna registrace pacientů ke zdravotní pojišťovně

Změna registrace pacientů k jiné zdravotní pojišťovně, a to bez jejich vědomí, byla náplní několika kontrol, podobně jako v roce 2010. V rámci kontroly jedné ze zdravotních pojišťoven bylo zjištěno, že zdravotní pojišťovna pro získávání nových pojištěnců uzavírala mandátní či zprostředkovatelské smlouvy s externími subjekty. Ze smluv vyplývalo, že zprostředkovatelé budou přihlášky předávat fyzicky přímo zástupcům zdravotní pojišťovny, zprostředkovatelé však měli také přístup do pomocného softwaru, do kterého zadávali pod svým přihlašovacím jménem a přístupovým heslem údaje o pojištěncích, které byly uvedeny v přihláškách. Zdravotní pojišťovna v době kontroly vedla aktuální evidenci o podvodných jednáních v souvislosti s falešnými přihláškami zdravotního pojištění a měla zaregistrováno celkem 100 případů podvodných jednání, které vyšetřovala Policie ČR. Zdravotní pojišťovna sama však podávala trestní oznámení pouze v jednom případě, o ostatních případech podvodného jednání se zdravotní pojišťovna dozvěděla od orgánů činných v trestním řízení. Dle vyjádření Policie ČR spočívala podvodná činnost jednoho z konkrétních zprostředkovatelů v tom, že si patrně vymyslel, nebo si z volně dostupných zdrojů opsal jméno a příjmení osoby, dále patrně vymyslel, nebo z volně přístupných zdrojů opsal adresu, která neměla žádný vztah ke jménu a příjmení osoby, z obchodního rejstříku opsal náhodně rodná čísla existujících osob a náhodně, na základě zkušeností, si vymyslel číslo občanského průkazu. Následně takto upravené přihlášky byly odevzdány Pojišťovně. Další případ podvodů s přihláškami zdravotního pojištění evidovala Policie ČR v souvislosti s dalším zprostředkovatelem. Ten osobní údaje pojištěnců využil pravděpodobně ze smluv, které pojištěnci uzavírali např. s telekomunikačními společnostmi, u kterých byl přítomen nebo ze smluv se kterými se setkal ve svém zaměstnání. Takto zfalšoval přihlášky zdravotního pojištění celkem ve 47 případech.

Stěžovatelka v případě této zdravotní pojišťovny žádala o prošetření ve věci neoprávněné evidence její přihlášky. Kontrolou bylo zjištěno, že v jejím případě došlo ke zneužití osobních údajů ze strany dalšího zprostředkovatele. Zprostředkovatel využil informace o stěžovatelce v rozsahu jméno, příjmení a rodné číslo, padělal její podpis, uvedl nesprávné bydliště a takto upravenou přihlášku zdravotního pojištění předal k evidenci zdravotní pojišťovně. Zdravotní pojišťovna přihlášku převzala a dále osobní údaje zpracovávala v dobré víře, že tak činí se souhlasem osoby uvedené v přihlášce, který byl vyjádřen podpisem na přihlášce zdravotního pojištění. Jelikož zdravotní pojišťovna v daném případě zprostředkovateli zcela důvěřovala a spoléhala na to, že zprostředkovatel bude postupovat v souladu s uzavřenou mandátní smlouvou a platnými právními předpisy, přihlášku převzala, aniž by dále zkoumala její pravost. V tomto případě sama stěžovatelka podala ke zdravotní pojišťovně žádost o zrušení přihlášky, v níž uvedla, že nikdy žádnou přihlášku o převodu zdravotního pojištění k této zdravotní pojišťovně nepodepsala a ani adresa jejího bydliště uvedená na přihlášce neodpovídá skutečnosti. Zdravotní pojišťovna zpětně zjistila, který ze zprostředkovatelů neoprávněně za stěžovatelku přihlášku vyplnil a předložil. Žádost o zrušení přihlášky zdravotní pojišťovna vyhodnotila jako oprávněnou a vyjednala její zpětnou přeregistraci k původní zdravotní pojišťovně.

Kontrola byla ukončena se závěrem, že sama zdravotní pojišťovna zákon č. 101/2000 Sb. neporušila, ale v kontrolním protokolu inspektorka Úřadu konstatovala, že problematiku trestné činnosti související se zajišťováním nových pojištěnců by měla zdravotní pojišťovna řešit zejména preventivními opatřeními, a to zvolením účinných kontrolních mechanismů. Pojišťovna by měla před vložením nového pojištěnce do databáze prověřit, zda osobní údaje pojištěnce, včetně jeho podpisu, na přihlášce odpovídají skutečnosti. Účinné kontrolní mechanismy je zapotřebí vytvořit zejména s ohledem na objem trestné činnosti páchané vyhotovením falešných přihlášek pojištěnců. Tomu, že kontrolní mechanismy zdravotní pojišťovny zprostředkovatelů selhaly, odpovídá i počet evidovaných trestných činů, které byly spáchány v souvislosti s neoprávněně vyplněnými přihláškami zdravotního pojištění. Kontrolující si jsou vědomi, že pojišťovna nemůže trestnou činnost podvodů v souvislosti s falešnými přihláškami zdravotního pojištění odhalit v celém rozsahu, musí však vyvinout maximální možné úsilí, aby tomuto druhu trestné činnosti preventivně a účinně zabránila.

15. Kamerový systém v bytovém domě

Jako typický příklad řešení problematiky kamerových systémů v bytových domech lze uvést kontrolu, kterou prováděla inspektorka Úřadu na základě stížnosti ve dvou činžovních domech, jejichž vlastníkem bylo společenství vlastníků. V obou domech byl instalován kamerový systém se záznamem, který se skládal ze čtyř kamer a digitálního videorekordéru. Dvě kamery byly instalovány do suterénních prostor (po jedné v každém domě) a 2 kamery do prostor schodiště do 1. patra (v době kontroly byly vypnuté). Účelem, dle sdělení kontrolovaných, bylo zamezit nepořádku na chodbě domu, u poštovních schránek, snaha o zamezení používání osobních výtahů popeláři, v důsledku kterého docházelo k poškozování výtahu – záznamy chtěli kontrolovaní použít pro následné jednání s popeláři, dále k ochraně majetku obecně, včetně získání informací o osobách, které nemají oprávnění vstupu do sledovaných prostor. Digitální videorekordér typu AVC785 se záznamem na pevný disk byl instalován v kanceláři společenství, k ovládání videorekordéru sloužil notebook, instalovaný v kanceláři společenství vlastníků. Kamerový systém byl v nepřetržitém provozu 24 hodin denně. Doba uchovávání pořízených záznamů byla cca 10 dnů, tato doba nebyla určena nastavením parametrů kamerového systému, ale kapacitou pevného disku videorekordéru, kdy po jeho zaplnění se automaticky mazaly nejstarší uložené záznamy. Doba uchování tak mohla kolísat dle četnosti pořizování nových záznamů. Společenství neprokázalo, že disponuje souhlasem všech obyvatel domů se zpracováním jejich osobních údajů prostřednictvím kamerového systému se záznamem.

Inspektorka Úřadu v kontrolním protokolu konstatovala, že kamerový systém se záznamem, tak jak byl v domech instalován a nastaven, sleduje a zaznamenává neustále činnost osob ve sklepních prostorách Domů, dále pak je zamýšleno shromažďovat a zpracovávat záznamy o aktivitách každého, kdo do Domů vstupuje, nebo z Domů odchází (kamery na podestách do 1. patra). Vzhledem k tomu, že se jedná o dva rozdílné prostory, zvážila kontrolující inspektorka míru zásahu do soukromého a osobního života sledovaných osob v daných prostorách a jeho proporcionalitu vzhledem ke stanovenému účelu pro každý prostor zvlášť. Zároveň konstatovala, že vlastní shromažďování osobních údajů kamerovým systémem se záznamem uvedeným způsobem přitom zcela postrádá preventivní funkci ve smyslu přímého zabránění či odvrácení nežádoucích aktivit, jeho funkce je omezena pouze na odstrašení potencionálního pachatele. Osobní údaje, resp. záznamy z kamerového systému, shromážděné v prostorách domu v rozsahu zjištěném v průběhu kontroly, tak mohou sloužit pouze jako podpůrný prostředek pro následné objasnění či vyšetření incidentů, nemohou však samy o sobě zajistit žádoucí ochranu ve smyslu účelů, které byly určené společenstvím, tedy zabránit nežádoucímu jednání. Vlastností kamerového systému, vyplývající z jeho podstaty, je to, že nepřetržitě shromažďuje záznamy o všech aktivitách veškerých osob, které jsou právě v dosahu jednotlivých kamer, nezávisle na tom, zda se jedná o aktivity v souladu, či rozporu s určeným účelem. Důsledkem této vlastnosti pak je to, že pouze nepatrný zlomek shromážděných a uchovávaných kamerových záznamů obsahuje údaje, které mohou být využity k naplnění určeného účelu, zbytek je shromážděn a uchováván nadbytečně, a to za cenu více než nepřiměřeného zásahu do soukromí dotčených osob. V případě pořizování záznamu ve sklepních prostorách konstatovala, že zásah do soukromého a osobního života není značný, protože do uvedených prostor vstupují dotčené osoby pouze nepravidelně a málo často, přičemž jejich aktivita se zpravidla omezuje pouze na vyhození odpadu do popelnic. Tyto prostory nejsou průchozí, tj. neslouží pro vstup do dalších částí domů, kam by dotčené osoby musely nezbytně vstupovat. Z hlediska stanoveného účelu, tedy kontroly vstupu a pobytu neoprávněných osob a jejich nežádoucích aktivit, je možno dané prostory posoudit jako mírně rizikové, neboť společenství již dříve realizovalo účinné opatření pro zabránění vstupu neoprávněných osob do Domů (uzamykatelné mříže u vstupu). Na základě tohoto zvážení lze na předmětné zpracování aplikovat výjimku dle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Současně je však nezbytné posuzovat aplikaci této výjimky jako hraniční případ, neboť i při běžné činnosti, jako je vynášení odpadu, může dojít k situaci, jejíž zveřejnění by mohlo dotčenou osobu značně poškodit. V případě zamýšleného pořizování záznamů z kamer, instalovaných na podestách schodišť do prvního patra Domů, uvedla, že je nezbytné nejprve konstatovat, že oblast ochrany soukromí každého jednotlivce není vázána pouze na vnitřní prostory jeho bytu, ale i na prostory, kterými daný jedinec musí nezbytně procházet, aby mohl vstoupit do vlastního obydlí nebo ho opustit. Dotčené osoby přitom nemají možnost volby, jak vstoupit do svého bytu nebo ho opustit, aniž by o tom byl pořízen záznam. Kamery by sledovaly dotčenou osobu v prostoru mezi vstupem do chodby Domů a vstupem do výtahu nebo na schodiště do obytné části Domů, přičemž pro vstup do obytné části Domů neexistuje alternativní cesta. Současně je nutno zdůraznit, že sledování by bylo až na výjimky soustavné a dlouhodobé, nikoliv nahodilé či jednorázové, a proto by bylo možné ze shromážděných záznamů snadno získat informace, zneužitelné k poškození některého ze sledovaných subjektů údajů, k čemuž značně přispívá i to, že záznamy jsou automaticky opatřovány údajem o datu a čase. Pořizování záznamů prostřednictvím kamerového systému za uvedených podmínek a uvedeným způsobem je nutno posuzovat jako zasahující vysokou měrou do osobního a soukromého života obyvatel domu, tedy jako velmi invazivní. Z hlediska dosažení stanoveného účelu, tedy ochrany majetku společenství, majetku obyvatel domů a jejich zdraví a bezpečnosti je nutno konstatovat, že při daném nastavení kamer by byl sledován pouze omezený prostor a vybavení domů. Jak již bylo uvedeno výše, funkce by se omezila pouze na odstrašení případného

pachatele a následné zdokumentování nežádoucího jednání pro účely vyšetřování, v žádném případě by však toto jednání nebylo možno přímo odvrátit.

Dle inspektorky Úřadu by bylo zpracování osobních údajů společenstvím prostřednictvím kamerového systému se záznamem v popsaném rozsahu a popsaným způsobem prostřednictvím kamer na podestách natolik významným a hrubým zásahem do soukromého a osobního života subjektů údajů, přičemž tento zásah by byl neúměrný dosaženému účinku, že na něj nelze aplikovat ustanovení výjimky uvedené v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Zpracováním osobních údajů bez souhlasu subjektů údajů prostřednictvím záznamů z kamer na podestách by společenství porušilo povinnost uloženou v § 5 odst. 2 zákona č. 101/2000 Sb.

16. Postup Policie ČR při dodržování § 8a – 8c zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen „trestní řád“) – tzv. „náhubkový zákon“

Úřad obdržel stížnost subjektu údajů na zveřejnění jména stěžovatele ve sdělovacích prostředcích v souvislosti s šetřením Policie ČR, zveřejněny byly i informace o jeho obvinění. Osoba stěžovatele byla v daném městě veřejně známa, zároveň byla zveřejněna fotografie této osoby, pořízená v okamžiku, kdy byla tato osoba předváděna k podání vysvětlení na Policii ČR.

V § 8a odst. 1 trestního řádu je uvedeno, že *„Při poskytování informací o své činnosti veřejnosti orgány činné v trestním řízení dbají na to, aby neohrozily objasnění skutečností důležitých pro trestní řízení, nezveřejnily o osobách zúčastněných na trestním řízení údaje, které přímo nesouvisejí s trestnou činností, a aby neporušily zásadu, že dokud pravomocným odsuzujícím rozsudkem není vina vyslovena, nelze na toho, proti němuž se vede trestní řízení, hledět, jako by byl vinen (§ 2 odst. 2). V přípravném řízení nesmějí zveřejnit informace umožňující zjištění totožnosti osoby, proti které se vede trestní řízení, poškozeného, zúčastněné osoby a svědka“*.

V průběhu kontroly nebylo prokázáno, že by Policie ČR poskytla před zahájením domovní prohlídky nebo v průběhu telefonicky, ani jinak informace, jež by vedly k identifikaci stěžovatele. Policie ČR na tiskové konferenci konané následující den po domovní prohlídce jméno a příjmení konkludentně potvrdila. Je zapotřebí konstatovat, že jméno a příjmení bylo již v souvislosti s podezřením ze spáchání přečinu veřejnosti známo, jelikož bylo zveřejněno před tiskovou konferencí na webových stránkách deníku, který v daném městě vychází. Kontrolující na místě zjistili, že jméno a příjmení stěžovatele věděli před tiskovou konferencí i další novináři, kteří následně po Policii ČR tiskovou konferenci požadovali. Kontrolující akceptovali vyjádření Policie ČR, že ve snaze zabránit dezinformacím a spekulacím, které by mohly stěžovatele ještě více poškodit, tiskovou konferenci urychleně uspořádala.

V průběhu tiskové konference Policie ČR opakovaně zdůraznila zásadu presumpce neviny v přípravném řízení a na tiskové konferenci používala pouze označení podezřelá osoba.

Kontrolující konstatovali, že stěžovatel byl dle sdělení zástupců Policie ČR osobou, která je ve městě veřejně známa, jednalo se o osobu, která se zúčastňovala veřejného života, což vyplývalo i z textu stížnosti, kterou na Úřad stěžovatel zaslal. Ze zkušeností policistů příslušného územního odboru také vyplynulo, že je běžné, že se informace o tom, že policie někde zasahuje, rychle rozšíří. Tedy není nic zvláštního na tom, že o průběhu domovní prohlídky se dozvěděl i novinář deníku, který jako první ještě v den domovní prohlídky osobní údaje stěžovatele zveřejnil.

Osoba stěžovatele tak byla v souvislosti s podezřením ze spáchání přečinu ztotožněna veřejností ještě před zahájením tiskové konference. Policie ČR tedy na tiskové konferenci informovala novináře o okolnostech, které již byly veřejnosti známé.

Kontrolovaná součást Policie ČR neporušila v souvislosti s poskytováním informací o fyzické osobě sdělovacím prostředkům na tiskové konferenci ani ustanovení zákona č. 101/2000 Sb.

V druhém případě se jednalo o podobnou kontrolu. Prověřováno bylo dodržování ustanovení § 8b odst. 2 trestního řádu. Stěžovatelka uvedla ve své stížnosti, že v souvislosti s šetřením podezření na spáchání trestného činu pro trestný čin týrání svěřené osoby došlo k uvedenému porušení zákona s tím, že reportérům televize byly poskytnuty jedním ze svědků či dalších osob informace, které mohly vést ke zjištění totožnosti její nezletilé dcery. Televize odvysílala reportáž, ve které svědkyně uváděla některé informace, které se týkaly trestního stíhání, a i když v reportáži nebylo zmíněno jméno poškozené nezletilé, z údajů, které zazněly, bylo dle stěžovatelky zřejmé, že pro ty, kdo znají její dceru a ji, byla jejich totožnost zřejmá. Stěžovatelka byla toho názoru, že údaje reportérům poskytla vědomě a úmyslně svědkyně. Stěžovatelka také uvedla, že po odvysílání reportáže se její dcera obává chodit do školy. Odvysílání reportáže způsobilo její dceři také zhoršení zdraví, což v příloze podnětu doložila lékařskou zprávou. Ze shromážděného důkazového materiálu vyplynulo, že Policie ČR poskytla sdělovacímu prostředku pouze informace, které nebyly v rozporu s ustanovením § 8a trestního řádu. Policie ČR ve zveřejněné reportáži pouze uvedla, že vyšetřovatelka sdělila obvinění pro podezření ze spáchání trestného činu týrání svěření osoby. Informace o věku obviněné není dostatečným identifikátorem, podle kterého by se dal určit konkrétní subjekt údajů. Kontrolou nebylo prokázáno, že by Policie ČR reportérům sdělila dílčí informace, které by vedly ke zjištění totožnosti stěžovatelky

pro účely reportáže. Inspektorka konstatovala, že Policie ČR neporušila § 8a trestního řádu, ani ustanovení zákona č. 101/2000 Sb. Žádné konkrétní informace, na základě kterých by se dala identifikovat nezletilá dcera stěžovatelky nebo stěžovatelka sama, nebyly v reportáži televize uvedeny. Zda údaje, které vedly televizi k identifikaci nezletilé, poskytla svědkyně, nebylo kontrolujícími provedeným šetřením prokázáno. Svědkyně byla spolu se svojí dcerou Policií ČR řádně poučena dle § 8b trestního řádu, zákona č. 218/2003 Sb. a zákona č. 101/200 Sb. o povinnosti mlčenlivosti o všech skutečnostech, které se v souvislosti s vyšetřováním dozvěděla. Svědkyně zaslala Úřadu vyjádření, ve kterém uvedla, že ona ani její dcera neposkytly nikomu žádné osobní údaje v případě šetření stěžovatelky. Zdroje, od kterých získává televize osobní údaje subjektů údajů, a které následně využije za účelem realizace reportáže, nikomu nesděluje. Pokud se informace o konkrétním subjektu údajů shromáždí v reportáži z více zdrojů, je pak v souvislosti s jejím odvysíláním možné, že se subjekt údajů stane identifikovatelným pouze pro určitý, ohraničený okruh osob. Těmto osobám jsou většinou odvysílané skutečnosti již částečně známy. Televize ve zveřejněné reportáži žádné konkrétní identifikační údaje o dceři stěžovatelky ani o stěžovatelce samotné neuvedla. Kontrolujícím se provedeným šetřením a dokazováním nepodařilo zjistit žádné skutečnosti, které by vedly ke zjištění konkrétního subjektu, který televizi poskytl informace, na základě kterých mohli reportéři identifikovat stěžovatelku nebo její nezletilou dceru za účelem natočení reportáže.

Poznámka: Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v sekci Dozorová činnost v rubrice Kontrolní činnost inspektorů.

Z rozhodovací činnosti Úřadu

(rok 2010–2011)

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. Zpracování osobních údajů při ukončení smluvního vztahu pro vyplacení zbývajícího telefonního kreditu (dále jen „kredit“)

Zpracování osobních údajů bez souhlasu subjektu údajů, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby, umožňuje ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Pro účely identifikace osoby, které má být vyplacen zbývající kredit (což bylo hlavním důvodem, proč účastník řízení požadoval osobní údaje od stěžovatele), je nepochybně dostačující, pokud tato osoba předloží originál SIM karty spolu s průvodním dopisem obsahujícím kódy PIN a PUK a číslo bankovního účtu, podle kterého je Policie České republiky schopná v případě trestního činu vyhledat jeho majitele. Další osobní údaje jsou požadovány již nadbytečně a v rozporu s principem aktivované služby X, která je anonymní, SIM karta je přenosná a v důsledku toho tedy může být konečný majitel karty odlišný od toho, kdo ji aktivoval. Z toho vyplývá také oprávnění žádat vrácení kreditu držitele karty bez ohledu na jeho identifikaci. Navíc musí správní orgán konstatovat, že zaslání kopie občanského průkazu prostřednictvím elektronické pošty není žádným relevantním důkazem v případě podvodu, a účastník řízení nemůže mít žádnou jistotu, že se bude jednat o občanský průkaz skutečného žadatele. I z tohoto důvodu nelze považovat požadování kopie občanského průkazu a osobních údajů na ní uvedených za nezbytné pro identifikaci osoby žadatele o vyplacení zbývajícího kreditu. (čj. *SPR-2837/10)*

2. Porušení zákazu zveřejnit informace o mladistvých osobách v souvislosti s trestním řízením, které je proti nim vedeno

Podle § 53 odst. 1 a § 54 odst. 2 zákona č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), nikdo nesmí jakýmkoli způsobem zveřejnit žádnou informaci, ve které je uvedeno jméno, popřípadě jména, a příjmení mladistvého, nebo která obsahuje informace, které by umožnily tohoto mladistvého identifikovat, a dále je zakázáno publikování informací o průběhu hlavního líčení nebo veřejného zasedání, které by vedly ke ztotožnění mladistvého, ve veřejných sdělovacích prostředcích nebo jiným způsobem; stejně tak je zakázáno publikování každého textu nebo každého vyobrazení týkajícího se totožnosti mladistvého. D. D., D. K. a M. K. v době spáchání provinění nepřekročili osmnáctý rok svého věku, byli tedy v souladu s § 2 písm. d) zákona č. 218/2003 Sb. mladistvými osobami, proti kterým bylo vedeno trestní řízení, tudíž se jednalo o osoby ve smyslu § 53 a 54 tohoto zákona. V daném případě prokazatelně došlo ke zveřejnění takových informací, podle nichž bylo možné mladistvé identifikovat, a je tedy zřejmé, že obviněný svým jednáním porušil zákaz uvedený v § 53 odst. 1 a § 54 odst. 2 zákona č. 218/2003 Sb., a naplnil tedy skutkovou podstatu přestupku podle § 44a odst. 1 zákona č. 101/2000 Sb. Obviněný tuto skutečnost sám potvrdil na ústním jednání a uvedl, že se tak stalo z důvodu omylu na jeho straně, když se domníval, že to, zda jsou dané osoby považovány za mladistvé, se posuzuje vždy v aktuální okamžik, a nikoli zpětně ke dni spáchání trestného činu.

Přestupku podle § 44a odst. 3 zákona č. 101/2000 Sb. se dopustí ten, kdo poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem, a spáchá jej tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem. Obviněný z přestupku umístil svůj článek obsahující informace, jejichž zveřejnění je zakázáno, na internet, tedy na veřejně přístupnou počítačovou síť, a výše citované ustanovení tak naplnil. *(čj. SPR-3872/11)*

3. Zpracování údajů z registru o činnostech, oznámení o majetku a oznámení o příjmech, darech a závazcích vedeného podle zákona č. 159/2006 Sb., o střetu zájmů

Podle § 13 odst. 9 zákona č. 159/2006 Sb. mohou být veškeré údaje vedené v registru oznámení o činnostech, oznámení o majetku a oznámení o příjmech, darech a závazcích použity a dále zpracovávány, s výjimkou uvedenou v § 13 odst. 5 zákona č. 159/2006 Sb., pouze za účelem zjištění případného střetu zájmů při výkonu funkce veřejného funkcionáře. Zpracováním osobních údajů v registru nesmí být dotčena ochrana osobních údajů podle zvláštních právních předpisů. Podle § 13 odst. 5 zákona č. 159/2006 Sb. lze dále zveřejnit pouze údaje uvedené v registru, které se týkají poslance, senátora, člena vlády a veřejného funkcionáře uvedeného v § 2 odst. 1 písm. j) až l) zákona č. 159/2006 Sb. (těmi jsou člen Rady pro rozhlasové a televizní vysílání, člen zastupitelstva kraje, hlavního města Prahy, obce, městské části nebo městského obvodu územně členěného statutárního města a městské části hlavního města Prahy, který je pro výkon funkce dlouhodobě uvolněn, a nebo ten, který před svým zvolením do funkce člena zastupitelstva

nebyl v pracovním poměru, ale vykonává funkce ve stejném rozsahu jako člen zastupitelstva, který je pro výkon funkce dlouhodobě uvolněn).

Přestože ustanovení § 23 odst. 2 písm. a) zákona č. 159/2006 Sb. obsahuje i po novelizaci provedené zákonem č. 216/2008 Sb. opět ve vymezení skutkové podstaty přestupku nesprávný odkaz na odpovídající právní povinnost (§ 13 odst. 7 namísto § 13 odst. 9), je ustanovení zákona v této části natolik určité a náležitě slovně definuje skutkovou podstatu přestupku, že tato chyba nebrání posuzovat jednání obviněného právě z hlediska možného naplnění této skutkové podstaty (viz též rozsudek Nejvyššího správního soudu 5 A 65/2001, SJS 124/2004, Sb. NSS 2004; 3: 197).

Jak vyplývá z výše uvedeného, obviněný použil údaje z registru v článku publikovaném v deníku X. Z obsahu tohoto článku přitom nijak nevyplývá, že by se věnoval konkrétnímu střetu zájmů pánů P. Ž., J. R., M. T., J. M., M. R., M. K., K. T. nebo I. H. Článek pouze shrnuje obsah údajů o majetku a závazcích, tak jak je uvedli ve svém oznámení podaném podle zákona č. 159/2006 Sb. Správní orgán se přitom domnívá, že samotné zveřejnění údajů z registru, bez toho, aby bylo dáno do souvislosti s jinou skutečností nebo informací, která by mohla nebo měla vést ke zjištění případného střetu zájmů (tak jak je definuje § 3 zákona č. 159/2006 Sb.), nesplňuje podmínku oprávněného použití údajů ve smyslu § 13 odst. 9 zákona č. 159/2006 Sb. Na základě toho dospěl správní orgán k závěru, že obviněný svým jednáním naplnil znaky skutkové podstaty přestupku podle § 23 odst. 2 písm. a) zákona č. 159/2006 Sb., neboť údaje použil k jinému účelu, než ke zjištění případného střetu zájmů.

S námitkou obviněného, dle které jeho čin není společensky nebezpečný (neporušuje ani neohrožuje zájem společnosti), se správní orgán neztotožnil. Správní orgán konstatuje, že ze zákona č. 159/2006 Sb. sice vyplývá, že údaje vedené v registru jsou za splnění podmínky podání písemné žádosti přístupné každému (§ 13 odst. 2), to ale neznamená, že bylo možno s těmito údaji nakládat libovolně. Naopak, dle správního orgánu je zjevné, že zákonodárce při vědomí si ústavního práva vyplývajícího z čl. 10 odst. 2 a 3 Listiny základních práv a svobod (právo na ochranu soukromí) a v souladu s čl. 17 odst. 4 Listiny základních práv a svobod omezil v § 13 odst. 9 zákona č. 159/2006 Sb. další využití takto získaných údajů pouze pro konkrétní účel. Ze znění § 13 odst. 5 zákona č. 159/2000 Sb. poté dle správního orgánu vyplývá jednoznačný účel daného omezení, a s ním souvisejícího vymezení skutkové podstaty přestupku, kterým je zamezení zveřejňování informací vedených v registru u přesně vymezené skupiny veřejných funkcionářů (v daném případě negativním vymezením, tj. vymezením těch funkcionářů, o nichž informace z registru zveřejnit lze). Oproti právní úpravě platné před novelou provedenou zákonem č. 216/2008 Sb. rozlišuje nyní platná právní úprava právě v § 13 odst. 5 zákona č. 159/2006 Sb. mezi jednotlivými funkcionáři z hlediska jejich postavení v rámci správy věcí veřejných, tj. jejich podílu na rozhodování o veřejných věcech, a požadavku veřejnosti (tedy i médií) na jejich kontrole z hlediska možného vzniku střetu zájmů. Toto vymezení je dle správního orgánu rozumné a plně v souladu se shora uvedenými ústavními principy (ochrana soukromí a právo na svobodu projevu) a správní orgán je jím při svém rozhodování vázán. Pokud tedy obviněný zveřejnil informace v celostátním deníku, resp. jeho regionální příloze, považuje správní orgán takové jednání za současného naplnění formálního znaku přestupku za jednání, které porušuje a ohrožuje zájem společnosti. *(čj. SPR-4989/11)*

4. Posouzení otázky liberace v případě nezabezpečení listin s osobními údaji jejich ponecháním ve vozidle

Správní orgán proto na základě shora uvedeného posuzoval jednání účastníka řízení (tj. uzamčení vozidla, zaparkování vozidla ve frekventované části města, vědomost o kamerovém systému města) 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 sice došlo k uzamčení vozidla, to ovšem nemění nic na skutečnosti, že vozidlo (jeho zadní sedadlo) není běžným místem pro uložení dokumentů s osobními údaji. Navíc v případě dokumentace obsahující i údaje o zdravotním stavu nebo informace týkající se trestního řízení se správní orgán domnívá, že jednoznačně nelze hovořit o vynaložení veškerého úsilí, aby nedošlo k neoprávněnému přístupu k těmto údajům. Instalace kamerového systému ve městě a tvrzení účastníka řízení, že jeho existenci vyhodnocoval při svém rozhodování o zaparkování automobilu ve městě a případném ponechání předmětné dokumentace uvnitř auta, zcela jasně odporuje logice a správní orgán je přesvědčen, že se jedná skutečně o účelové tvrzení, které má dodatečně liberovat jednání účastníka řízení. Dle správního orgánu je zcela rozhodující v tomto směru také skutečnost, že auto bylo na zaparkovaném místě ponecháno po dobu skoro 4 hodin, tudíž se nejednalo zcela zjevně o snahu v co nejkratší době zavést dokumentaci do místa jiného výkonu pracovní činnosti účastníka řízení, a to, že dokumenty byly odcizeny po 15 minutách od zaparkování vozidla, na tom nic nemění. Také uložení dokumentů v plátěné tašce na místo na zadním sedadle, které je volně viditelné z venku všem kolemjdoucím, lze chápat jako nedostatečnou snahu k přijetí a provedení vůbec jakýchkoliv (pomineme-li běžné uzamčení vozidla) opatření k zajištění bezpečnosti před neoprávněným přístupem. *(čj. SPR-0447/19)*

5. Postup obce při nakládání s listinou zaslanou exekutorem, aniž je obec jejím oprávněným příjemcem

Účastník řízení je podle zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, povinen v souvislosti s výkonem spisové služby zajistit odbornou správu dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností. Přijetím uvedeného exekučního příkazu řádným způsobem tak účastník řízení postupoval v souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., jelikož se jednalo o řádné zpracování nezbytné pro plnění právní povinnosti správce. Následným zveřejněním uvedeného dokumentu, které účastníkovi řízení neukládá žádný právní předpis, však došlo k jednání, které je mimo účel, kterým je vedení spisové služby.

Jelikož zákon o obcích, exekuční řád, občanský soudní řád a ani žádný jiný právní předpis, neobsahuje povinnost zveřejnit předmětný exekuční příkaz, je nutno dojít k závěru, že se na daný postup bude vztahovat obecná úprava nakládání s osobními údaji, obsažená v zákoně č. 101/2000 Sb. Účastník řízení je tedy jako správce osobních údajů podle § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. povinen nakládat s osobními údaji pouze v souladu s účelem, pro který byly shromážděny; zpracovávat osobní údaje k jinému účelu lze, jen pokud k tomu dal subjekt údajů předem souhlas, případně pokud se na takové zpracování vztahuje některá z výjimek dle § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. Současně je také správce povinen dbát práva na ochranu soukromého a osobního života subjektů údajů. Vzhledem k tomu, že byly osobní údaje osob zveřejněny bez jejich souhlasu prostřednictvím internetových stránek účastníka řízení a účastník řízení nedisponoval ani žádným jiným právním titulem pro tento postup, je nutno dojít k závěru, že stanovený účel zpracování byl zveřejněním exekučního příkazu zjevně překročen.

Podle § 49 odst. 4 exekučního řádu se exekuční příkaz doručí oprávněnému, povinnému a dalším osobám, kterým se podle zvoleného způsobu exekuce doručuje usnesení o nařízení výkonu rozhodnutí podle občanského soudního řádu. V uvedeném případě není účastník řízení označen jako další z adresátů tohoto příkazu. Dále je účastník řízení povinen zveřejňovat písemnosti zaslané v rámci exekučního řízení pouze na základě § 336c odst. 3 a § 338p odst. 3 občanského soudního řádu ve vztahu k nemovitostem a podnikům nacházejícím se v jeho obvodu.

K předmětu řízení správní orgán dále uvádí, že je nepochybné, že v daném případě došlo také k pochybení na straně příslušného exekutorského úřadu, který zaslal písemnost s uvedenými osobními údaji účastníkovi řízení, aniž by byl jedním z oprávněných adresátů tohoto příkazu. To ovšem nezbavuje účastníka řízení odpovědnosti za další nakládání s osobními údaji v tomto exekučním příkazu obsaženými, zejména za jejich zveřejnění na úřední desce města přístupné prostřednictvím internetu také široké veřejnosti. Na dané skutečnosti nemění nic ani fakt, že jsou účastníkem řízení běžně zveřejňovány písemnosti, které obdrží od soudního exekutora, přičemž žádným způsobem nezkoumá, zda je k tomu oprávněn nebo povinen. Účastník řízení je naopak povinen došlou písemnost posoudit a vyhodnotit, zda se jedná o některý z případů, kdy se má tato písemnost zveřejnit odpovídajícím způsobem prostřednictvím úřední desky města (tedy zda se jedná o dražební vyhlášku podle § 336c odst. 3, resp. § 338p odst. 3 občanského soudního řádu).

Správní orgán tedy shrnuje, že účastník řízení je povinen došlou písemnost od soudního exekutora, případně jiného orgánu veřejné moci, nejprve posoudit podle jejího obsahu, a poté učinit závěr, zda je povinen v souladu s příslušným procesním předpisem (např. občanský soudní řád, zákon č. 337/1992 Sb., o správě daní a poplatků) doručený dokument na své úřední desce zveřejnit. Pokud dospěje k závěru, že ano, poté je povinen tento dokument zveřejnit, aniž by jakkoliv zasahoval do jeho obsahu, neboť odpovědnost ve vztahu k zákonu č. 101/2000 Sb. je poté na tom, kdo zveřejnění požaduje. Pokud ovšem žádný právní předpis zveřejnit došlý dokument neukládá, nese odpovědnost za zveřejněné osobní údaje přímo účastník řízení, a to bez ohledu na to, zda mu byla písemnost doručena omylem (jako v projednávaném případě), nebo cíleně (např. proto, že byla soudním exekutorem nařízena exekuce srážkami ze mzdy zaměstnance účastníka řízení, což musí být samozřejmě zaměstnavateli oznámeno, viz § 282 odst. 2 občanského soudního řádu). *(čj. SPR-5089/10)*

6. Zveřejňování osobních údajů poškozených v trestním řízení

Správní orgán vychází ze skutečnosti, že A. B. je v trestním řízení vedeném Policií České republiky poškozenou, kdy vůči ní měl být spáchán trestný čin (zločin) pohlavního zneužití. Postavení poškozeného přitom není vázáno na pravomocné rozhodnutí o trestném činu, ale mimo jiné na skutečnost, že se o určitém skutku vede jako o trestném činu trestní řízení bez ohledu na výsledek tohoto trestního řízení. Jinými slovy, pokud se v dané věci vedlo trestní řízení a byly zahájeny úkony trestního řízení podle § 158 odst. 3 trestního řádu, pro skutek, ve kterém je Policií České republiky spatřován trestný čin pohlavního zneužití vůči A. B., je nutné na A. B. od této doby nahlížet jako na poškozenou. Proto se také na poskytování informací a zejména jejich zveřejňování vztahuje omezení podle § 8b odst. 2 trestního řádu, neboť dle správního orgánu není pochyb, že A. B. je vzhledem ke svému věku (rok narození 2003) nezletilou.

Správní orgán doplňuje, že ačkoliv to není v § 8b odst. 2 trestního řádu výslovně uvedeno, zákaz poskytování in-

formací se v zásadě vztahuje na dobu od spáchání trestného činu, přinejmenším však na dobu od počátku trestního řízení. Trestním řízením je přitom dle § 12 odst. 10 trestního řádu řízení podle trestního řádu, tedy i postup před zahájením trestního stíhání včetně přijímání a prověřování oznámení a jiných podnětů podle § 158 odst. 1 a 2 trestního řádu.

V této souvislosti je třeba zdůraznit, že ochrana poškozeného podle § 8b odst. 2 trestního řádu není vázána na to, zda bude konkrétní pachatel uznán vinným z trestného činu, kde vystupuje poškozený; ostatně v některých případech ani konkrétní pachatel trestného činu nemusí být odhalen a usvědčen, přičemž není pochyb o tom, že se trestný čin stal, a že poškozeným z tohoto trestného činu je např. nezletilá osoba. I v tomto případě jí ovšem svědčí ochrana před neoprávněným zveřejněním informací ve smyslu § 8b odst. 2 trestního řádu.

Lze tedy shrnout, že zákaz zveřejňování informací o poškozeném v trestním řízení není zásadně vázán na rozsudek o vině, ale postačí, že se o určitém skutku vede trestní řízení. Opačný výklad by naprosto popíral smysl ochrany práva na soukromí poškozeného trestným činem, kdy do právní moci odsuzujícího rozsudku by nebylo jeho soukromí nijak chráněno, a tedy mohly by být o něm zveřejňovány jakékoliv informace, a teprve po právní moci rozsudku by začal být chráněn podle § 8b odst. 2 trestního řádu. *(čj. SPR-3927/11)*

7. Zpracování osobních údajů žadatelů o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

K předmětu tohoto řízení lze uvést, že účastníci řízení jsou jako povinné subjekty ve smyslu zákona č. 106/1999 Sb. nepochybně správci osobních údajů osob, které je požádaly o poskytnutí informací, ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., přičemž nezbytné osobní údaje dotčených subjektů údajů zpracovávají ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. za účelem vyřízení příslušné žádosti, neboť je shromažďují, třídí, používají, uchovávají, tedy s nimi provádějí operace tímto zákonem předpokládané. Jako správci osobních údajů jsou proto povinni dodržovat veškeré povinnosti stanovené zákonem č. 101/2000 Sb.

Osobním údajem je přitom podle § 4 písm. a) zákona č. 101/2000 Sb. jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže jej lze 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.

Jsou-li osobní údaje uvedeny v rozsahu: jméno, příjmení, případně titul před jménem, datum narození, adresa bydliště, telefonní číslo, e-mailová adresa; jméno, příjmení, datum a místo narození, adresa bydliště a údaj o studiu na konkrétní vysoké škole; titul před jménem, jméno, příjmení, datum narození, adresa bydliště, celkový počet písemných podání týkajících se konkrétně specifikovaného domu; tituly před jménem, jméno, příjmení, titul za jménem, datum narození, adresa bydliště, ID datové schránky; titul před jménem, jméno, příjmení, datum narození, e-mailová adresa a údaj o vztahu ke konkrétní vysoké škole; jméno, příjmení, datum narození, adresa bydliště; jméno, příjmení, adresa bydliště, e-mailová adresa; titul před jménem, jméno, příjmení, datum narození, adresa bydliště; jméno příjmení, datum narození, rodné číslo, adresa bydliště, další údaje o vlastnickém či jiném právu fyzické osoby k nemovitostem vyplývající z výpisu z katastru nemovitostí včetně rodného čísla vlastníka a identifikačního údaje právního zástupce této osoby; titul před jménem, jméno, příjmení, e-mailová adresa, jsou dle názoru správního orgánu jednotlivé fyzické osoby identifikovatelné vždy.

Subjekt údajů je však dle názoru správního orgánu identifikovatelný i tehdy, dojde-li ke zveřejnění informací v rozsahu jméno, příjmení, případně titul/y před jménem a za jménem, a označení pracovní pozice či funkce fyzické osoby v právnické osobě, za kterou podávala tato osoba žádost, nebo pracovní spojení tazatele s touto právnickou osobou vyplývá z kontextu žádosti; jméno a příjmení, případně titul před jménem, a další údaje identifikující tuto osobu spojením s informacemi vyplývajícími z kontextu zveřejněného obsahu odpovědi na žádost; příjmení, případně i jméno, a adresa bydliště vyplývající z kontextu obsahu zveřejněné odpovědi na žádost, neboť je zjevné, že i v těchto případech je žadatel o informace na základě zveřejněných údajů určitelný.

Za zvláštní skupinu je pak dle názoru správního orgánu nutno považovat případy, kdy dochází ke zpracování (v tomto případě zveřejnění) příjmení, případně jména a titulu nebo titulů před jménem anebo za jménem, jsou-li tyto údaje ve svém spojení dostatečně specifické, přičemž tato specifičnost vyplývá z neobvyklosti příjmení, množství titulů atd.

Dále je k předmětu řízení nutné uvést, že podle ustanovení § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. je správce povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje v mezích § 3 odst. 6 zákona č. 101/2000 Sb., nebo pokud k tomu dal subjekt údajů předem souhlas.

Účel zpracování osobních údajů žadatelů o informaci, k němuž byly tyto údaje shromážděny, tj. přijetí, zaevidování žádosti o informaci a její vyřízení, byl přitom následným zveřejněním osobních údajů prostřednictvím webových stránek účastníků řízení zjevně překročen; současně na jednání účastníků řízení není možné aplikovat žádnou z výjimek stanovených v § 3 odst. 6 zákona č. 101/2000 Sb. ani účastníci řízení nedisponovali souhlasem dotčených subjektů údajů se zveřejněním jejich osobních údajů.

Pokud tedy všichni účastníci řízení osobní údaje žadatelů zveřejnili na svých webových stránkách, jedná se o další (jiný účel) zpracování osobních údajů ve smyslu ustanovení § 4 písm. e) zákona č. 101/2000 Sb., aniž k tomu daly sub-

jekty údajů předem souhlas. Na takovéto zpracování nelze vztáhnout ani žádnou z výjimek uvedených v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. *(čj. SPR-5205/11)*

8. Zpracování nepřesného rodného čísla (tj. rodného čísla jiné osoby) a jeho předání do registru dlužníků

Podle § 5 odst. 1 písm. c) zákona č. 101/2000 Sb. je každý správce povinen zpracovávat pouze přesné osobní údaje, které získal v souladu se zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracovávané osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům.

Pokud vznikne ze smluvního vztahu na straně zákazníka prodlení s plněním (dluh) a správce osobních údajů v postavení věřitele musí přistoupit k vymáhání své pohledávky, je třeba, aby pohledávku vymáhal po skutečném dlužníkovi a nikoliv po osobě, jejíž osobní údaje mu někdo v souvislosti s uzavřením smlouvy poskytl, ale jako správce si přesnost (správnost) těchto údajů nijak neověřil. V případě smluv uzavíraných prostředky na dálku je přitom riziko uvedení nesprávných osobních údajů ze strany zákazníka nepochybně vyšší právě s ohledem na zvolený komunikační prostředek a s vědomím tohoto rizika proto musí správce k osobním údajům a jejich přesnosti přistupovat.

Dle správního orgánu je nepochybné, že účastník řízení je oprávněn shromažďovat a dále zpracovávat rodná čísla svých zákazníků [§ 63 odst. 3 písm. b) bod 3. zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)].

V dané věci účastník řízení ověřil prostřednictvím České pošty správnost údaje o jménu, příjmení, adrese a číslu občanského průkazu svého zákazníka M. H. U rodného čísla, které je svou povahou jedinečným identifikátorem fyzické osoby (občana České republiky) a tedy samo o sobě slouží ke ztotožnění osoby, ovšem účastník řízení jeho správnost žádným způsobem neověřil. Přesto s tímto údajem pracoval jako s přesným osobním údajem a v okamžiku, kdy mu vznikla vůči M. H. pohledávka z nezaplacené faktury, předal (zpracovával) do registru dlužníků SOLUS mimo jiné jako identifikační údaj M. H. rodné číslo, které ovšem nebylo jeho. Tento postup je přitom dle správního orgánu porušením povinnosti dle § 5 odst. 1 písm. c) zákona č. 101/2000 Sb. V daném případě je třeba přihlížet právě ke shora uvedenému charakteru rodného čísla – jedinečného, státem garantovaného, identifikátoru fyzické osoby. Zpracování nepřesného rodného čísla může mít za následek značný zásah do soukromí a práv nositele tohoto rodného čísla. V případě účastníka řízení je proto dle názoru správního orgánu porušením jeho povinností zpracovávat přesné osobní údaje, pokud předává neověřená rodná čísla do registru dlužníků. V tomto konkrétním případě dochází s ohledem na účel dlužnických registrů a v nich zapojené subjekty k vážnému zásahu do práv skutečných nositelů rodného čísla (v daném případě pana J. K.), kteří nemusí být k účastníkovi řízení v žádném smluvním vztahu, resp. kteří nemají vůči účastníkovi řízení žádný dluh. Tento zásah je poté násoben skutečností, že to je právě nositel rodného čísla, který musí následně (mnohdy komplikovaně a po delší dobu) prokazovat, že předmětný záznam je v registru dlužníků uveden neoprávněně.

Správní orgán je tedy toho názoru, že v případě neověřených rodných čísel by účastník řízení v souladu s § 5 odst. 1 písm. c) zákona č. 101/2000 Sb. neměl přinejmenším tento údaj zpracovávat způsobem, který by mohl znamenat zásah do práv nositele rodného čísla; účastník řízení by proto do registru dlužníků měl v těchto případech předávat pouze identifikační údaje bez rodného čísla, a rodné číslo pouze tam, kde ověřil, že se jedná o přesný osobní údaj (např. při osobní návštěvě klienta v prodejně účastníka řízení).

Porušení povinnosti podle § 5 odst. 1 písm. c) zákona č. 101/2000 Sb. poté správní orgán spatřuje i v postupu účastníka řízení při řešení stížnosti pana J. K. Skutečnost, že zaměstnanci účastníka řízení neodeslali stížnost pana J. K. na zneužití jeho rodného čísla na příslušné oddělení, je nepochybně třeba přičítat účastníkovi řízení. Jako nesprávný ovšem správní orgán považuje i požadavek účastníka řízení na podání trestního oznámení ze strany J. K., se kterým účastník řízení spojuje nápravu a řešení vzniklého stavu. Je nepochybné, že ke zjištění, že u M. H. je účastníkem řízení evidováno nesprávné rodné číslo, postačí ověření totožnosti pana J. K. z jím předložených dokladů; tedy, pokud účastník řízení z občanského průkazu ověří, jaké je rodné číslo J. K., a následně ve svém systému zjistí, že stejné rodné číslo má evidováno u úplně jiné osoby, jedná se o dostatečné zjištění pro to, aby u něj vznikla pochybnost o přesnosti tohoto osobního údaje. Tato pochybnost poté musí vést vždy k blokování tohoto osobního údaje a ke sdělení této skutečnosti všem příjemcům nepřesného osobního údaje (v daném případě registru dlužníků SOLUS). Takto ovšem účastník řízení nepostupoval, když požadoval po J. K. podání trestního oznámení, a teprve na jeho základě provedl opravu nepřesného rodného čísla, resp. jeho vymazání. To ve svém důsledku vedlo k prodloužení doby, po kterou účastník řízení zpracovával nepřesný osobní údaj a zasahoval tím do práv pana J. K. *(čj. SPR-5265/11)*

Poznámka:

[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.

Pracovní skupina pro ochranu údajů zřízená podle článku 29

881/11/CS
WP 185

Stanovisko 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení

Přijaté dne 16. května 2011

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán ve věci ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytlo ředitelství C (Základní práva a občanství Unie) Generálního ředitelství pro spravedlnost Evropské komise, B-1049 Brusel, Belgie, kancelář č. MO59 02/013.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

OBSAH

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ
zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na ustanovení článku 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice,

s ohledem na svůj jednací řád,

PŘIJALA TENTO DOKUMENT:

1. Úvod

Zeměpisné informace hrají v naší společnosti významnou úlohu. Téměř všechny lidské činnosti a rozhodnutí mají zeměpisnou složku. Hodnota informací se obecně zvyšuje, jsou-li informace spojené s lokalizací. Se zeměpisnou lokalizací lze spojit všechny typy informací, jako jsou finanční údaje, zdravotní údaje a další údaje o chování spotřebitelů. V souvislosti s rychlým technologickým rozvojem a rozsáhlým využitím inteligentních mobilních zařízení vzniká úplně nová kategorie služeb založených na lokalizaci.

Cílem tohoto stanoviska je objasnit právní rámec použitelný u geolokalizačních služeb dostupných a/nebo generovaných prostřednictvím inteligentních mobilních zařízení, která se mohou připojit na internet a jsou vybavena lokalizačními detektory, jako je GPS. K takovým službám patří: mapy a navigace, zeměpisné personalizované služby (včetně zajímavých míst v blízkém okolí), rozšířená realita, ukládání geolokalizačních odkazů u obsahu na internetu („geotagging“), sledování míst pobytu přátel, kontrola dětí a reklama vycházející z lokalizace.

Toto stanovisko také pojednává o třech hlavních typech infrastruktury používané pro poskytování geolokalizačních služeb, a to o GPS, základnových stanicích GSM a WiFi. Zvláštní pozornost je věnována nové infrastruktuře založené na lokalizaci přístupových míst WiFi.

Pracovní skupina si je dobře vědoma skutečnosti, že existuje mnoho dalších služeb, které zpracovávají lokalizační údaje, které by také mohly vzbuzovat obavy týkající se ochrany údajů. Jejich rozsah se pohybuje od systémů elektronických vstupenek po systémy plateb mýtného u automobilů a od satelitních navigačních služeb, sledování lokalizace například pomocí kamer po geolokalizaci IP adres. V souvislosti s rychlým technologickým rozvojem, zejména s ohledem na mapování bezdrátových přístupových míst a skutečností, že subjekty, které nově vstupují na trh, jsou připraveny vyvíjet nové lokalizační služby na základě kombinace údajů základnové stanice a GPS a WiFi, se pracovní skupina rozhodla konkrétně objasnit právní požadavky na tyto služby podle směrnice o ochraně údajů.

Ve stanovisku je nejdříve popsána technologie, dále jsou určena a posouzena rizika pro soukromí a pak uvedeny závěry týkající se použití příslušných článků právních předpisů v případě různých správců, kteří shromažďují a zpracovávají lokalizační údaje pocházející z mobilních zařízení. Patří mezi ně například poskytovatelé

geolokalizační infrastruktury, výrobci technologie inteligentních telefonů a tvůrci aplikací založených na geolokalizaci.

V tomto stanovisku nebude posuzována zvláštní technologie ukládání geolokalizačních odkazů spojená například s takzvaným webem 2.0, kde uživatelé začleňují informace se zeměpisnými odkazy do sociálních sítí, jako je Facebook nebo Twitter. V tomto stanovisku také nebude podrobně pojednáno o některých dalších geolokalizačních technologiích používaných k propojení zařízení v relativně malé oblasti (obchodní centra, letiště, kancelářské budovy atd.), jako je Bluetooth, ZigBee, hlášení při průchodu definovanými body („geofencing“) a WiFi etikety RFID, přestože mnohé závěry tohoto stanoviska týkající se legitimního základu, informací a práv subjektů údajů se také vztahují na tyto technologie v případě, že jsou používány ke geolokalizaci lidí prostřednictvím jejich zařízení.

2. Souvislosti: různé geolokalizační infrastruktury

2.1 Údaje základnové stanice

Plocha, kterou pokrývají různí telekomunikační operátoři, se rozděluje na oblasti všeobecně známé jako buňky. Aby bylo možné použít mobilní telefon nebo se připojit na internet pomocí komunikace 3G, mobilní zařízení se musí připojit k anténě (dále základnové stanici), která buňku pokrývá. Buňky pokrývají oblasti různých velikostí v závislosti na rušivých vlivech, například hor a vysokých budov.

Po celou dobu, kdy je mobilní zařízení zapnuto, je spojeno s konkrétní základnovou stanicí. Telekomunikační operátor tato spojení nepřetržitě registruje. Každá základnová stanice má jedinečný identifikátor a je registrována s konkrétní lokalizací. Telekomunikační operátor a mnoho samotných mobilních zařízení jsou schopny použít signály z překrývajících se buněk (sousedních základnových stanic) pro přesnější odhad polohy mobilního zařízení. Tato technika se také nazývá triangulace.

Přesnost lze dále zvýšit pomocí informací jako RSSI (indikátor síly příchozího signálu), TDOA (časový posun příchodu) a AOA (úhel příchodu).

Údaje základnové stanice se mohou používat inovačními způsoby, například pro zjištění dopravní zácpy. Na každé silnici je v každém časovém úseku dne určitá průměrná rychlost, pokud ale předávání na sousední základnovou stanici trvá déle, než se očekává, dochází tam zřejmě k dopravní zácpě.

Úhrnem řečeno tato metoda určování polohy poskytuje rychlý a hrubý lokalizační údaj, který ale ve srovnání s údaji GPS a WiFi není velmi přesný. V hustě osídlených oblastech je přesnost přibližně 50 metrů, ale ve venkovských oblastech až několik kilometrů.

2.2 Technologie GPS

Inteligentní mobilní zařízení obsahují čipové sady s přijímači GPS, které určují jejich lokalizaci.

Technologie GPS (globální polohový systém) využívá 31 satelitů, z nichž každý obíhá okolo země na jedné z šesti různých oběžných drah.[1] Každý satelit vysílá velmi přesný rádiový signál.

Mobilní zařízení může určit svoji lokalizaci, jestliže detektor GPS zachytí alespoň čtyři z těchto signálů. Na rozdíl od údajů základnové stanice se tento signál šíří jen jedním směrem. Subjekty spravující satelity nemohou sledovat zařízení, která rádiový signál přijala.

Technologie GPS poskytuje přesné určení polohy v rozmezí čtyř až patnácti metrů. Hlavní nevýhodou GPS je to, že se relativně pomalu spouští.[2] Další nevýhoda spočívá v tom, že nefunguje nebo nefunguje dobře ve vnitřním prostoru. V praxi se proto technologie GPS často kombinuje s údaji základnové stanice a/nebo zmapovanými přístupovými místy WiFi.

2.3 WiFi

2.3.1 Přístupová místa WiFi

Relativně novým zdrojem geolokalizačních informací je využití přístupových míst WiFi. Tato technologie se podobá využití základnových stanic. Obě vycházejí z jedinečného identifikátoru (ze základnové stanice nebo přístupového místa WiFi), který může mobilní zařízení zachytit a zaslat službě, která zná lokalizaci pro každý jedinečný identifikátor.

Jedinečným identifikátorem každého přístupového místa WiFi je jeho adresa MAC (střední kontrola přístupu). Adresa MAC je jedinečným identifikátorem, který je přidělen síťovému rozhraní a obvykle zaznamenán v hardwaru, jako jsou paměťové čipy a/nebo na síťové karty v počítačích, telefonech, laptopech nebo přístupových místech.[3]

Důvod, proč lze přístupová místa WiFi využít jako zdroj geolokalizačních informací, je ten, že tato místa nepřetržitě hlásí svoji existenci. Většina širokopásmových internetových přístupových míst má také implicitně anténu WiFi. Implicitní nastavení nejběžněji používaných přístupových míst v Evropě je takové, že toto připojení je „zapnuto“ i v případě, že uživatel připojil svůj počítač (své počítače) k přístupovému místu pouze pomocí kabelů. Přístupové místo WiFi podobně jako rádio nepřetržitě vysílá svůj název sítě a adresu MAC, i když nikdo připojení nepoužívá a i když je obsah bezdrátové komunikace zašifrován pomocí WEP, WPA nebo WPA2.

---

[1] Globální polohový systém tvoří satelity, které vypustily Spojené státy americké k vojenským účelům. Evropská komise má v úmyslu spustit do roku 2014 program Galileo, síť osmnácti satelitů, která nabízí bezplatné globální satelitní určení polohy pro jiné než vojenské účely. První dva satelity mají být vypuštěny v roce 2011, další dva v roce 2012. Zdroj: Evropská komise, „Commission presents midterm review of Galileo and EGNOS“ (Komise představuje hodnocení programu Galileo a služby EGNOS v polovině období), 25. ledna 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835.

[2] S cílem urychlit počáteční zachycení signálu GPS bude možné si předem stáhnout tak zvané duhové tabulky, které udávají předpokládanou polohu různých satelitů v příštích týdnech.

[3] Příkladem adresy MAC je: 00-1F-3F-D7-3C-58. Adresa MAC přístupového místa WiFi se nazývá BSSID (identifikátor základní sady služeb).

Existují dva různé způsoby shromažďování adres MAC přístupových míst WiFi.[4]

1. Aktivní skenování: vysílání aktivních požadavků[5] všem přístupovým místům WiFi v blízkém okolí a záznam odpovědí. Tyto odpovědi nezahrnují informace o zařízeních připojených k přístupovému místu WiFi.

2. Pasivní skenování: záznam pravidelných monitorovacích rámců, které vysílá každé přístupové místo (obvykle 10krát za sekundu). Nestandardní alternativou jsou některé nástroje, které obecněji zaznamenávají všechny rámce WiFi vysílané přístupovými místy, včetně těch, které nevysílají monitorovací signály. Jestliže se tento typ skenování provádí bez řádné ochrany soukromí již od návrhu, může to vést ke shromažďování údajů vyměněných mezi přístupovými místy a zařízeními, která jsou k nim připojena. Tímto způsobem by mohly být zaznamenávány adresy MAC stolních počítačů, laptopů a tiskáren. Tento typ skenování by také mohl vést k nezákonnému záznamu obsahu komunikace. V případě, že majitel přístupového místa WiFi neumožnil šifrování WiFi (WEP/WPA/WPA2), je možné tento obsah snadno přečíst.

Lokalizaci přístupového místa WiFi lze stanovit dvěma různými způsoby.

1. Staticky/jednou: samotní správci shromažďují adresy MAC přístupových míst WiFi tak, že projíždějí oblast ve vozidlech vybavených anténami. V okamžiku, kdy zachytí signál, zaznamenají přesnou zeměpisnou šířku a zeměpisnou délku vozidla a mohou stanovit lokalizaci přístupových míst mimo jiné na základě síly signálu.

2. Dynamicky/trvale: uživatelé geolokalizačních služeb automaticky shromažďují adresy MAC, které zachytí jejich zařízení s funkcí WiFi, když použijí například internetovou mapu k určení jejich vlastní polohy (Kde jsem?). Mobilní zařízení pak zasílá veškeré dostupné informace včetně adres MAC, identifikátorů SSID a síly signálu poskytovateli geolokalizační služby. Správce může využívat tato trvalá pozorování ke stanovení a/nebo zpřesnění lokalizace přístupových míst WiFi ve své databázi zmapovaných přístupových míst WiFi.

Je důležité poznamenat, že mobilní zařízení se nemusí „připojit“ k přístupovým místům WiFi, aby shromáždila informace WiFi. Tato zařízení automaticky zjišťují přítomnost přístupových míst (v režimu aktivního nebo pasivního skenování) a automaticky o nich shromažďují údaje.

Mobilní telefony požadující stanovení geolokalizace navíc zasílají nejen údaje WiFi, ale často také veškeré další lokalizační informace, které obsahují, včetně údajů GPS a údajů základnové stanice. To umožňuje poskytovateli stanovit lokalizaci „nových“ přístupových míst WiFi a/nebo zpřesnit lokalizaci přístupových míst WiFi, která již byla zahrnuta v databázi. Tak dochází velmi účinným způsobem k decentralizaci

[4] Aktivní a pasivní skenování pro zjišťování přístupových míst bylo standardizováno v IEEE 802.11.

[5] S cílem shromáždit adresy MAC vysílá shromažďovatel všem přístupovým místům „průzkumný požadavek“.

shromažďování informací o přístupových místech WiFi, aniž by o tom zákazníci nutně věděli.

Úhrnem řečeno: geolokalizace na základě přístupových míst WiFi poskytuje rychlou a na základě nepřetržitých měření stále přesnější polohu.

3. Rizika pro soukromí

Inteligentní mobilní zařízení je velmi těsně spjato s konkrétním jednotlivcem. Většina lidí obvykle uchovává svá mobilní zařízení velmi blízko u sebe, v kapse nebo tašce či na nočním stolku vedle postele.

Stává se zřídka, že by osoba takové zařízení půjčila někomu jinému. Většina lidí ví, že jejich mobilní zařízení obsahuje řadu velmi důvěrných informací od e-mailu po soukromé fotografie, od historie prohlížení například po seznam kontaktních osob.

To umožňuje poskytovatelům služeb založených na geolokalizaci získat dokonalý přehled o zvycích a vzorech majitele takového zařízení a vytvářet podrobné profily. Ze vzoru noční nečinnosti lze odvodit místo spánku a z pravidelného vzoru ranního cestování lze odvodit lokalizaci zaměstnavatele. Vzor může také na základě takzvaného *sociálního grafu* zahrnovat údaje odvozené ze vzorů pohybu přátel.[6]

Vzor chování může také zahrnovat *zvláštní kategorie údajů*, jestliže například odhaluje návštěvy nemocnic a náboženských míst, přítomnost na politických demonstracích nebo přítomnost na dalších konkrétních místech, která prozrazuje údaje například o sexuálním životě. Tyto profily lze použít pro rozhodnutí, která majitele významně postihují.

Technologie inteligentních mobilních zařízení umožňuje neustálé sledování lokalizačních údajů. Inteligentní telefony mohou nepřetržitě shromažďovat signály ze základnových stanic a přístupových míst WiFi. Z technického hlediska lze sledování provádět utajeně, aniž by o tom byl majitel informován. Sledování lze také provádět z poloviny utajeně, když lidé „zapomenou“, že lokalizační služby jsou zapnuté nebo o této skutečnosti nejsou řádně informováni nebo když je nastavení přístupnosti lokalizačních údajů změněno ze „soukromé“ na „veřejnou“.

Dokonce i v případě, že lidé záměrně zpřístupní své geolokalizační údaje na internetu prostřednictvím služby místa výskytu a ukládání geolokalizačních odkazů, neomezený globální přístup vede k řadě nových rizik od krádeže údajů po vloupání a dokonce fyzický útok a nebezpečné pronásledování.

Hlavním rizikem využívání lokalizačních údajů je stejně jako u jiné nové technologie vznik nové funkce, tedy skutečnost, že na základě dostupnosti nového typu údajů se vytvářejí nové účely, které se v době původního shromáždění údajů nepředpokládaly.

[6] „Sociální graf“ je výraz, který označuje viditelnost přátel na internetových stránkách sociálních sítí a schopnost odvodit rysy chování z údajů o těchto přátelích.

4. Právní rámec

Příslušným právním rámcem je směrnice o ochraně údajů (95/46/ES). Směrnice se použije v každém případě, kdy dojde ke zpracování osobních údajů v důsledku zpracování lokalizačních údajů. Směrnice o ochraně soukromí v odvětví elektronických komunikací (2002/58/ES ve znění pozměněném směrnicí 2009/136/ES) se vztahuje pouze na zpracování údajů základnové stanice veřejnými službami elektronických komunikací a sítí (telekomunikačními operátory).

4.1 Údaje základnové stanice zpracovávané telekomunikačními operátory

V rámci poskytování veřejných služeb elektronických komunikací telekomunikační operátoři nepřetržitě zpracovávají údaje základnové stanice.[7] Údaje základnové stanice mohou také zpracovávat s cílem poskytovat služby s přidanou hodnotou. Tímto případem se pracovní skupina již zabývala ve stanovisku 5/2005 (WP115). Přestože rozšíření internetové technologie a detektorů do stále menších zařízení způsobilo nevyhnutelnou zastaralost některých příkladů v uvedeném stanovisku, z hlediska používání údajů základnové stanice zůstávají právní závěry a doporučení tohoto stanoviska platné.

1. Vzhledem k tomu, že se lokalizační údaje pocházející ze základnových stanic vztahují k identifikované nebo identifikovatelné fyzické osobě, podléhají ustanovením o ochraně osobních údajů stanoveným ve směrnici 95/46/ES ze dne 24. října 1995.
2. Směrnice 2002/58/ES ze dne 12. července 2002 (ve znění pozměněném v listopadu 2009 ve směrnici 2009/136/ES) je také použitelná na základě definice obsažené v čl. 2 písm. c) uvedené směrnice:
   „lokalizačními údaji“ se rozumějí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací;

Jestliže telekomunikační operátor nabízí hybridní geolokalizační službu, která je založena také na zpracování dalších typů lokalizačních údajů, jako jsou údaje GPS nebo WiFi, je taková činnost hodnocena jako veřejná služba elektronických komunikací. Jestliže telekomunikační operátor poskytuje tyto geolokalizační údaje třetí straně, musí si zajistit předchozí souhlas svých zákazníků.

4.2 Údaje základnové stanice, WiFi a GPS zpracovávané poskytovateli služeb informační společnosti

4.2.1 Použitelnost revidované směrnice o ochraně soukromí v odvětví elektronických komunikací

Společnosti, které poskytují lokalizační služby a aplikace založené na kombinaci údajů základnové stanice, GPS a WiFi, jsou charakteristickými *službami informační*

[7] Upozorňujeme, že poskytování veřejných míst typu WiFi hotspot ze strany poskytovatelů telekomunikačních služeb je také hodnoceno jako veřejná služba elektronických komunikací a mělo by tedy zejména vyhovovat ustanovením směrnice o ochraně soukromí v odvětví elektronických komunikací.

společnosti. Jako takové podle jednoznačné definice služby elektronických komunikací (čl. 2 písm. c) revidované rámcové směrnice (nezměněný))[8] výslovně nepodléhají směrnici o ochraně soukromí v odvětví elektronických komunikací.

Směrnice o ochraně soukromí v odvětví elektronických komunikací se nevztahuje na zpracování lokalizačních údajů službami informační společnosti, ani když je takové zpracování vykonáváno prostřednictvím veřejné sítě elektronických komunikací. Uživatel se může rozhodnout přenášet údaje GPS po internetu, například když na internetu přistupuje na navigační služby. V takovém případě je signál GPS přenášen na úrovni aplikace internetové komunikace nezávisle na síti GSM. Poskytovatel telekomunikační služby poskytuje pouze cestu. Bez velmi rušivého prostředku, jakým je *hloubková kontrola paketů*, nemůže získat přístup k údajům GPS a/nebo WiFi a/nebo základnové stanice zasílaným do inteligentního mobilního zařízení a vysílaným z tohoto zařízení mezi uživatelem/účastníkem a službou informační společnosti.

4.2.2 Použitelnost směrnice o ochraně údajů

V případech, kdy se nepoužije revidovaná směrnice o ochraně soukromí v odvětví elektronických komunikací, použije se podle čl. 1 odst. 2 směrnice 95/46/ES: „*Ustanovení této směrnice upřesňují a doplňují směrnici 95/46/ES pro účely uvedené v odstavci 1.*“

Na základě směrnice o ochraně osobních údajů jsou osobními údaji *veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity* – čl. 2 písm. a) směrnice.

Bod odůvodnění 26 směrnice věnuje zvláštní pozornost výrazu „identifikovatelné“, když uvádí, „že *pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby*“.

Bod odůvodnění 27 směrnice vymezuje široký rozsah ochrany*: „vzhledem k tomu, že rozsah této ochrany nesmí být závislý na použitých technikách, jinak by se vytvořilo vážné riziko jejího obcházení;“*

Ve svém stanovisku č. 4/2007 k pojmu osobní údaje pracovní skupina poskytla podrobné pokyny k definici osobních údajů.

---

[8] Směrnice 2002/21/ES ze dne 7. března 2002, čl. 2 písm. c): „*službou elektronických komunikací" se rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové vysílání, s výjimkou služeb poskytujících obsah nebo vykonávajících redakční dohled nad obsahem přenášeným prostřednictvím sítí a služeb elektronických komunikací; pojem nezahrnuje služby informační společnosti, jak jsou definovány v článku 1 směrnice 98/34/ES, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací;*

Inteligentní mobilní zařízení
Inteligentní mobilní zařízení jsou neoddělitelně spjata s fyzickými osobami. Obvykle existuje přímá a nepřímá identifikovatelnost.

Za prvé: telekomunikační operátoři, kteří poskytují GSM a mobilní přístup na internet, mají obvykle rejstřík obsahující jméno, adresu a bankovní údaje každého zákazníka spolu s několika jedinečnými čísly zařízení, jako je IMEI a IMSI.

Za druhé zakoupení dalšího softwaru pro zařízení (*aplikací* nebo *apps)* obvykle vyžaduje číslo kreditní karty, a obohacuje tak kombinaci jedinečného čísla/čísel a lokalizačních údajů přímo identifikujícími údaji.

Nepřímé identifikovatelnosti lze dosáhnout prostřednictvím kombinace jedinečného čísla/čísel zařízení a jedné nebo více stanovených lokalizací.

Každé inteligentní mobilní zařízení má alespoň jeden jedinečný identifikátor, adresu MAC. Zařízení může mít další jedinečná identifikační čísla, která přidal tvůrce operačního systému. Tyto identifikátory mohou být přenášeny a dále zpracovávány v souvislosti s geolokalizačními službami. Je skutečností, že lokalizaci konkrétního zařízení lze velmi přesně stanovit, zejména pokud existuje kombinace různých geolokalizačních infrastruktur. Taková lokalizace může určit dům nebo zaměstnavatele. Majitele zařízení je možné identifikovat zvláště v případě opakovaných pozorování.

Při úvahách o dostupných prostředcích identifikovatelnosti je třeba zohlednit situaci, kdy lidé odhalují stále více osobních lokalizačních údajů na internetu, například ve spojení s dalšími identifikujícími údaji zveřejňují místo bydliště nebo pracoviště. K takovému zveřejňování může docházet také bez jejich vědomí, jestliže jiní lidé ukládají jejich geolokalizační údaje. Tato situace usnadňuje vytváření vazby mezi lokalizací nebo vzorem chování a konkrétním jednotlivcem.

V návaznosti na stanovisko č. 4/2007 k pojmu osobní údaje a v souvislosti s tím, co bylo uvedeno výše, by mělo být navíc také poznamenáno, že jedinečný identifikátor umožňuje sledování uživatele konkrétního zařízení, a umožňuje tedy, aby byl uživatel/uživatelka jednoznačně určen/určena, přestože jeho/její skutečné jméno není známo.

Přístupová místa WiFi
Tato nepřímá identifikovatelnost se vztahuje také na přístupová místa WiFi.[9] Adresa MAC přístupového místa WiFi spolu s jeho stanovenou lokalizací je neoddělitelně spjata s lokalizací majitele přístupového místa.

Přiměřeně vybavený správce může prostřednictvím uživatelů jeho geolokalizační služby stanovit velmi přesnou lokalizaci přístupového místa WiFi na základě síly signálu a trvalých aktualizací lokalizace.

[9] Přístupová místa WiFi mohou být dokonce přímo identifikovatelná, jestliže poskytovatel přístupu na internet udržuje rejstřík adres MAC směrovačů WiFi, které poskytuje svým identifikovaným zákazníkům.

Pomocí těchto zdrojů lze v mnoha případech identifikovat malou skupinu bytů nebo domů, kde žije majitel přístupového místa. Jak snadno bude možné tohoto majitele identifikovat na základě adresy MAC, bude záviset na prostředí:

- V řídce osídlených oblastech, kde adresa MAC určí jediný dům, lze majitele obydlí určit přímo pomocí takových nástrojů, jako jsou například rejstříky o vlastnictví domů a bytů, bílé stránky seznamů, registrace voličů nebo dokonce jednoduchý dotaz ve vyhledávači.[10]
- V hustěji osídlených oblastech lze pomocí takových zdrojů, jako je například síla signálu a/nebo SSID (který může zachytit každý, kdo má zařízení s WiFi), určit přesnou lokalizaci přístupového místa, a v mnoha případech tedy zjistit totožnost jednotlivce (jednotlivců), který (kteří) žije (žijí) na tomto přesném místě (v domě nebo bytě), kde je lokalizováno přístupové místo.
- Ve velmi hustě osídlených oblastech určí adresa MAC jako možnou lokalizaci přístupového místa několik bytů, a to i za pomoci informací o síle signálu. Za těchto okolností není možné bez vynaložení nepřiměřeného úsilí přesně určit jednotlivce, který žije v bytě, kde je lokalizováno přístupové místo.

Skutečnost, že v některých případech nelze v současnosti majitele zařízení identifikovat bez vynaložení nepřiměřeného úsilí, nebrání obecnému závěru, že s kombinací adresy MAC přístupového místa WiFi a jeho stanovenou lokalizací by se mělo nakládat jako s osobními údaji.

Za těchto okolností a při zohlednění skutečnosti, že je nepravděpodobné, že by správce údajů byl schopen rozlišovat mezi případy, kdy je majitel přístupového místa WiFi identifikovatelný a kdy tomu tak není, správce údajů by měl nakládat se všemi údaji o směrovačích WiFi jako s osobními údaji.

Je důležité připomenout, že není nutné, aby účelem zpracování těchto geolokalizačních údajů byla identifikace uživatelů. Bude-li identifikace majitelů přístupových míst WiFi vyžadovat nepřiměřené úsilí, značně závisí na technických možnostech správce nebo jakékoli jiné osoby, pokud jde o jejich identifikaci.

5. Povinnosti vyplývající ze zákonů o ochraně údajů

5.1 Správce údajů

V souvislosti s internetovými geolokalizačními službami poskytovanými službami informační společnosti se rozlišují tři různé funkce, které jsou spojeny s různou odpovědností za zpracovávání osobních údajů. Jsou to: správce geolokalizační infrastruktury, poskytovatel zvláštní geolokalizační aplikace nebo služby a tvůrce operačního systému inteligentního mobilního zařízení. V praxi často společnosti současně vykonávají řadu úloh, například když kombinují operační systém s databází obsahující zmapovaná přístupová místa WiFi a reklamní platformu.

[10] Dostupnost takových rejstříků nebo seznamů se liší podle členského státu.

5.1.1 Správci geolokalizační infrastruktury

Majitelé databází obsahujících zmapovaná přístupová místa WiFi zpracovávají osobní údaje, když stanovují lokalizaci konkrétního inteligentního mobilního zařízení, podobně jako telekomunikační operátoři, když zpracovávají lokalizaci konkrétního zařízení pomocí svých základnových stanic. Vzhledem k tomu, že oba určují účel a prostředky tohoto zpracování, jsou podle definice v čl. 2 písm. d) směrnice o ochraně údajů správci.

Je důležité zdůraznit, že konkrétní zařízení napomáhá stanovit svoji lokalizaci tím, že předává majiteli databáze vlastní lokalizační údaje (často kombinaci údajů GPS, WiFi a základnové stanice) a jedinečné identifikátory z blízkých přístupových míst WiFi.[11] Takové zařízení také splňuje kritérium čl. 4 odst. 1 písm. c) směrnice o ochraně údajů, *prostředků umístěných na území členského státu*.

Vzhledem k tomu, že by se s adresou MAC přístupového místa WiFi v kombinaci s jeho stanovenou lokalizací mělo nakládat jako s osobními údaji, shromažďování těchto údajů vede také ke zpracování osobních údajů. Bez ohledu na způsob shromažďování těchto údajů (jednou nebo nepřetržitě) by měl majitel takové databáze vyhovět povinnostem směrnice o ochraně údajů.

5.1.2 Poskytovatelé geolokalizačních aplikací a služeb

Inteligentní mobilní zařízení umožňují instalaci softwaru třetích stran, tak zvaných *aplikací*. Tyto aplikace mohou zpracovávat lokalizační údaje (a další údaje) z inteligentního mobilního zařízení nezávisle na tvůrci operačního systému a/nebo správci geolokalizační infrastruktury.

Příklady takových služeb jsou: meteorologická služba, která vydává předpovědi o možnosti deště v několika následujících hodinách ve velmi specifické oblasti, služba, která nabízí informace o obchodech v blízkém okolí, služba zjišťování ztracených telefonů nebo služba, která ukazuje lokalizaci přátel.

Pro zpracování osobních údajů vzešlých z instalace a použití aplikace je poskytovatel aplikace, která je schopná zpracovávat geolokalizační údaje, správcem.

Instalace samostatného softwaru na inteligentním mobilním zařízení není samozřejmě vždy nutná. K mnoha geolokalizačním službám lze přistoupit také prostřednictvím prohlížeče. Příkladem takové služby je používání internetové mapy, která provede osobu po městě.

5.1.3 Tvůrce operačního systému

Tvůrce operačního systému inteligentního mobilního zařízení může být správcem pro zpracování geolokalizačních údajů, když je v přímé interakci s uživatelem a

[11] Mobilní zařízení může předávat různé geolokalizační údaje, které přijímá, aby správce stanovil jeho lokalizaci, nebo může vlastní lokalizaci stanovit samo. V obou případech je zařízení nepostradatelným prostředkem pro zpracování.

shromažďuje osobní údaje (například když žádá o počáteční registraci uživatele a/nebo shromažďuje lokalizační informace pro účely zlepšení služby). Tvůrce jako správce musí uplatňovat zásady soukromí coby aspektu návrhu, aby zabránil utajenému sledování buď ze strany samotného zařízení, nebo různých aplikací a služeb.

Tvůrce je také správcem pro údaje, které zpracovává, jestliže má zařízení funkci „phone home“ pro jeho výskyt. Vzhledem k tomu, že tvůrce v takovém případě rozhoduje o prostředcích a účelu takového toku údajů, je pro zpracování těchto údajů správcem. Běžným příkladem takové funkce „phone home“ je automatické poskytování aktualizací časové zóny na základě lokalizace.

Za třetí je tvůrce správcem, když nabízí reklamní platformu a/nebo prostředí internetového obchodu pro aplikace a může nezávisle na poskytovatelích aplikací zpracovávat osobní údaje pocházející z (instalace a používání) geolokalizačních aplikací.

5.2 Odpovědnost dalších stran

Existuje mnoho dalších internetových stran, které umožňují (další) zpracování lokalizačních údajů, jako jsou prohlížeče, internetové stránky sociálních sítí nebo komunikační média umožňující například ukládání geolokalizačních odkazů. Když tyto strany začleňují do své platformy geolokalizační vybavení, mají významnou odpovědnost při rozhodování o implicitním nastavení aplikace (implicitně zapnuto nebo vypnuto). Přestože jsou tyto strany správci pouze do té míry, do jaké samy aktivně zpracovávají údaje, hrají klíčovou úlohu v oblasti oprávněnosti zpracování údajů ze strany správců, jako jsou poskytovatelé zvláštních aplikací, například pokud se jedná o viditelnost a kvalitu informací o zpracování geolokalizačních údajů.

5.2 Legitimní základ

5.2.1 Inteligentní mobilní zařízení

Jestliže si telekomunikační operátoři přejí použít údaje základnové stanice s cílem dodávat zákazníkovi služby s přidanou hodnotou, musí podle revidované směrnice o soukromí v odvětví elektronických komunikací získat jeho/její předchozí souhlas. Musí rovněž zajistit, že je zákazník o podmínkách takového zpracování informován.

Vzhledem k citlivosti zpracování (vzorů) lokalizačních údajů je *předchozí informovaný souhlas* také hlavním použitelným základem pro zajištění oprávněnosti zpracování údajů v případě zpracování lokalizací inteligentního mobilního zařízení v souvislosti se službami informační společnosti.

Podle čl. 2 písm. h) směrnice o ochraně údajů musí být souhlas svobodný, výslovný a vědomý projev vůle subjektu údajů.

V závislosti na typu použité technologie zařízení uživatele hraje relativně aktivní úlohu při zpracování geolokalizačních údajů. Zařízení je schopné přenášet lokalizační údaje z různých zdrojů jakékoli třetí straně. Tato technická schopnost by neměla být

zaměňována za zákonnost takového zpracování údajů. Jestliže by implicitní nastavení operačního systému umožňovalo přenášení lokalizačních údajů, neměla by být absence zásahu ze strany jeho uživatelů chybně považována za svobodný souhlas.

V rozsahu, do kterého tvůrci operačních systémů a další služby informační společnosti sami aktivně zpracovávají geolokalizační údaje (například když přistupují k lokalizačním informacím ze zařízení nebo jeho prostřednictvím), musí rovnocenným způsobem usilovat o předchozí informovaný souhlas svých uživatelů. Musí být zřejmé, že takový souhlas nelze volně získávat prostřednictvím povinného přijetí všeobecných pravidel a podmínek, ani prostřednictvím možností výjimek. Lokalizační služby by měly být implicitně vypnuty a uživatelé mohou jednotlivě souhlasit se zapnutím konkrétních aplikací.

Souhlas zaměstnanců

V souvislostech zaměstnání je souhlas jako legitimní základ pro zpracování problematický. Pracovní skupina ve svém stanovisku ke zpracování osobních údajů v souvislostech zaměstnání napsala: „*jestliže se od pracovníka požaduje souhlas a neudělení souhlasu vede ke skutečné nebo potenciální relevantní újmě, souhlas ve smyslu splnění článku 7 nebo článku 8 není platný, protože není svobodný. Jestliže pracovník nemůže souhlas odmítnout, nejedná se o souhlas. (…) Problematickou oblastí je případ, kdy je udělení souhlasu podmínkou zaměstnání. Pracovník teoreticky může souhlas odmítnout, ale důsledkem může být ztráta pracovní příležitosti. Za takových okolností není souhlas svobodný a není proto platný.*“[12] Místo aby zaměstnavatelé usilovali o souhlas, musí zjišťovat, zda je prokazatelně nezbytné vykonávat za oprávněným účelem dohled nad přesnými lokalizacemi zaměstnanců a zvažovat tuto nezbytnost s ohledem na základní práva a svobody zaměstnanců. V případech, kdy lze tuto nezbytnost přiměřeně odůvodnit, mohl by právní základ takového zpracování vycházet z oprávněného zájmu správce (čl. 7 písm. f) směrnice o ochraně údajů). Zaměstnavatel musí vždy hledat nejméně invazivní prostředky, zamezit nepřetržitému sledování a například zvolit systém, který zašle upozornění, pokud zaměstnanec překročí předem nastavenou virtuální hranici. Zaměstnanec musí být schopen mimo pracovní dobu vypnout každé monitorovací zařízení a musí se mu vysvětlit, jak to udělat. Zařízení ke sledování vozidel nejsou zařízeními pro sledování zaměstnanců. Jejich funkcí je sledování nebo monitorování lokalizace vozidel, ve kterých jsou instalována. Zaměstnavatelé by je neměli považovat za zařízení ke sledování nebo monitorování chování či místa výskytu řidičů nebo jiných zaměstnanců, například zasíláním upozornění na rychlost vozidla.

[12] WP48, stanovisko č. 8/2001 ke zpracování osobních údajů v souvislostech zaměstnání.

Souhlas dětí

V některých případech musí souhlas dětí udělit rodiče nebo další zákonní zástupci. Znamená to například to, že poskytovatel geolokalizační aplikace musí poskytnout rodičům oznámení o shromáždění a využití geolokalizačních údajů jejich dětí a před dalším shromážděním a využitím těchto geolokalizačních údajů od nich získat souhlas. Některé geolokalizační aplikace jsou zvláště navrženy pro dohled ze strany rodičů, například tak, že nepřetržitě ukazují lokalizaci zařízení na internetových stránkách nebo vydávají upozornění, jestliže zařízení opustí předem navržené území. Používání takových aplikací je problematické. Pracovní skupina zřízená podle článku 29 ve svém stanovisku č. 2/2009[13] k ochraně osobních údajů dětí napsala*: Nikdy by nemělo dojít k tomu, aby děti z bezpečnostních důvodů čelily nadměrnému dohledu, který by omezil jejich samostatnost. V tomto kontextu je třeba usilovat o rovnováhu mezi ochranou intimity a soukromí dětí a jejich bezpečností.*

Právní rámec stanoví, že rodiče jsou odpovědní za zaručení práva dětí na soukromí. Jestliže rodiče usoudí, že používání takové aplikace je za zvláštních okolností odůvodněné, musí být o tom děti přinejmenším informovány a jakmile je to rozumně možné, musí jim být umožněno podílet se na rozhodnutí o používání takové aplikace.

Pro každý z rozdílných účelů, pro které jsou údaje zpracovávány, musí existovat výslovný souhlas. Správce musí zcela jasně uvést, je-li jeho služba omezena na odpověď na dobrovolnou otázku „Kde jsem právě teď?“ nebo je-li jeho účelem odpovídat na otázky „Kde jsi, kde jsi byl a kde budeš příští týden?“. Správce musí jinými slovy věnovat zvláštní pozornost souhlasu pro účely, které subjekt údajů neočekává, jako je například tvorba profilů a/nebo zacílení podle chování.

Dojde-li k podstatné změně účelu zpracování, musí správce usilovat o nový výslovný souhlas. Jestliže například společnost uvedla, že nebude osobní údaje sdílet s žádnou třetí stranou, ale nyní je sdílet chce, musí usilovat o aktivní předchozí souhlas každého zákazníka. Absence odpovědi (nebo jiný scénář výjimky) není dostačující.

Je důležité rozlišovat mezi souhlasem s jednorázovou službou a souhlasem v případě pravidelného čerpání. Například pro využití zvláštní geolokalizační služby může být nezbytné v zařízení nebo v prohlížeči zapnout geolokalizační služby. Je-li tato geolokalizační funkce zapnuta, všechny internetové stránky si mohou přečíst lokalizační údaje uživatele tohoto inteligentního mobilního zařízení. S cílem zabránit rizikům utajeného sledování považuje pracovní skupina zřízená podle článku 29 za zásadní, aby zařízení nepřetržitě upozorňovalo, že je geolokalizace zapnutá, například pomocí stále viditelné ikony.

Pracovní skupina doporučuje, aby po uplynutí přiměřené doby poskytovatelé geolokalizačních aplikací nebo služeb usilovali o nový individuální souhlas (i když nedochází ke změně povahy zpracování). Nebylo by například vhodné pokračovat ve zpracování lokalizačních údajů v případě, že jednotlivec tuto službu aktivně nevyužil v předchozích dvanácti měsících. Když osoba službu využila, měla by jí být alespoň jednou ročně (nebo častěji, odůvodňuje-li to povaha zpracování) připomenuta povaha zpracování jejích osobních údajů a nabídnut snadný prostředek pro ukončení zpracování.

[13] WP160, Stanovisko č. 2/2009 k ochraně osobních údajů dětí (Obecné pokyny a zvláštní případ škol).

V neposlední řadě by subjekty údajů měly být schopné souhlas velmi snadno odejmout, aniž by to mělo jakékoli negativní důsledky pro používání jejich zařízení. Konsorcium World Wide Web (W3C) vytvořilo nezávisle na evropských směrnicích o ochraně údajů návrh normy pro geolokalizační rozhraní pro programování aplikací (API), který zdůrazňuje potřebu předchozího výslovného a informovaného souhlasu.[14] W3C zvláště vysvětluje potřebu respektovat odejmutí souhlasu a doporučuje, aby subjekty provádějící tuto normu vzaly v úvahu, že *„obsah, který se vyskytuje na určitých URL, se mění takovým způsobem, že s ohledem na uživatele již v minulosti udělené lokalizační povolení neplatí. Nebo že uživatelé si to prostě mohou rozmyslet."*

Příklad osvědčeného postupu poskytovatelů geolokalizačních aplikací

Aplikace, která chce využívat geolokalizační údaje, uživatele srozumitelně informuje o účelech, za jakými chce údaje využívat, a pro každý z možných odlišných účelů požádá o jednoznačný souhlas. Uživatel si aktivně vybere úroveň přesnosti geolokalizace (například na úrovni země, města, směrovacího čísla nebo co nejpřesněji). Jakmile je lokalizační služba aktivována, je na každé obrazovce, kde jsou lokalizační služby zapnuty, trvale viditelná ikona. Uživatel má nepřetržitou možnost odejmout souhlas, aniž by musel aplikaci ukončit. Uživatel také může snadno a trvale vymazat veškeré lokalizační údaje uložené v zařízení.

5.2.2 Přístupová místa WiFi

Podle směrnice o ochraně údajů mohou mít společnosti pro zvláštní účel nabídky geolokalizačních služeb oprávněný zájem na nezbytném shromažďování a zpracování adres MAC a stanovených lokalizací přístupových míst WiFi.

Legitimní základ čl. 7 písm. f) směrnice o ochraně údajů vyžaduje rovnováhu mezi oprávněnými zájmy správce a základními právy subjektů údajů. Když vezmeme v úvahu zpola statickou povahu přístupových míst WiFi, mapování přístupových míst WiFi představuje v zásadě menší hrozbu pro soukromí majitelů těchto přístupových míst než sledování lokalizací inteligentních mobilních zařízení prováděné v reálném čase.

Rovnováha mezi právy správce a právy subjektu údajů je dynamická. Aby mohli správci s úspěchem dovolit, že jejich oprávněné zájmy převládnou v čase nad zájmy subjektů údajů, musí vytvořit a zavést záruky, jako například právo být snadno a trvale vymazán z databáze bez nutnosti poskytnout správci takové databáze další osobní údaje. Mohou například používat software pro automatické zjišťování, že je osoba připojená ke konkrétnímu přístupovému místu.[15]

---

[14] Geolokalizační API konsorcia W3C: http://www.w3.org/TR/geolocation-API/.

[15] Toto je možný přístup použití:

1. Subjekt údajů přistoupí na konkrétní internetové stránky, kde může zadat adresu MAC svého přístupového místa WiFi.
2. Jestliže se adresa MAC objevuje v databázi obsahující zmapovaná přístupová místa WiFi, správce může ukázat ověřovací stránku obsahující text, který požaduje tabulku ARP internetového zařízení. Teoreticky lze prostřednictvím příkazu „ARP –a" ukázat adresy WLAN MAC. Pomocí kódu obsaženého v prohlížeči, jako je Java, lze vytvořit tuto tabulku ARP na pozadí.

Pro účel nabídky poskytování geolokalizačních služeb navíc není nutné shromažďovat a zpracovávat identifikátory SSID. Shromažďování a zpracování SSID proto překračuje to, co je nutné pro účel nabídky geolokalizačních služeb na základě mapování lokalizace přístupových míst WiFi.

5.3 Informace

Různí správci musí zajistit, že majitelé inteligentních mobilních zařízení jsou odpovídajícím způsobem informováni o klíčových prvcích zpracování v souladu s článkem 10 směrnice o ochraně údajů, jako je jejich totožnost jako správce, účel zpracování, typ údajů, trvání zpracování, práva subjektů údajů na přístup k jejich údajům, jejich opravu nebo výmaz a právo odejmout souhlas.

Platnost souhlasu je neoddělitelně spjata s kvalitou informací o službě. Informace musí být jasné, vyčerpávající a srozumitelné pro širokou netechnickou veřejnost a musí být trvale a snadno přístupné.

Informace musí být zacíleny na širokou veřejnost. Správci nesmí předpokládat, že jejich zákazníci jsou technicky zdatné osoby jen proto, že vlastní inteligentní mobilní zařízení. Jestliže správce ví, že zařízení je lákavé pro mládež, informace musí být přizpůsobeny věku.

Jestliže poskytovatelé geolokalizačních aplikací mají v úmyslu stanovovat lokalizace zařízení více než jednou, musí v tom smyslu udržovat informovanost svých zákazníků po celou dobu zpracovávání lokalizačních údajů. Musí také svým zákazníkům umožnit udržovat udělení jejich souhlasu v platnosti nebo souhlas odejmout. Pro dosažení těchto cílů by poskytovatelé aplikací měli úzce spolupracovat s tvůrcem operačního systému. Tvůrce je z technického hlediska v nejlepším postavení vytvořit trvale viditelnou připomínku, že jsou zpracovávány lokalizační údaje. Tvůrce je také v nejlepším postavení z hlediska kontroly, že nejsou nabízeny žádné aplikace, které utajeně sledují místo výskytu inteligentních mobilních zařízení.

Jestliže tvůrce operačního systému vytvořil funkci „phone home“ nebo jakýkoli jiný prostředek pro získávání přístupu k údajům uloženým v zařízení nebo jestliže získává přístup k lokalizačním údajům jinými způsoby, například prostřednictvím inzerentů třetích stran, musí subjekt údajů předem informovat o (zvláštních a oprávněných) účelech, za jakými má v úmyslu tyto údaje zpracovávat, a o trvání zpracování.
Povinnost informovat subjekty údajů se vztahuje také na správce databází obsahujících přístupová místa WiFi stanovená pomocí geolokalizace. Správci musí přiměřeně informovat veřejnost o své totožnosti a účelech zpracování a poskytnout jí další příslušné informace. Pouhá zmínka o možném shromažďování údajů o přístupových místech WiFi ve zvláštním prohlášení o soukromí určeném uživatelům geolokalizační aplikace je nedostačující. Pro informování veřejnosti existuje dostatek internetových i jiných prostředků.

3. Jestliže se adresa MAC objevuje v tabulce ARP, je určeno, že uživatel připojený k WLAN je také uživatelem s přístupem k místní adrese WLAN MAC. Správce tak automaticky a snadno ověřuje žádost o výmaz.

5.4 Práva subjektů údajů

Subjekty údajů mají právo získat od různých správců přístup k lokalizačním údajům, které správci shromáždili z jejich inteligentních mobilních zařízení, i informace o účelech zpracování a příjemcích či kategoriích příjemců, kterým jsou údaje sdělovány. Informace musí být poskytovány ve formátu čitelném pro lidi, tedy ve formátu zeměpisných lokalizací, nikoli abstraktních čísel, například základnových stanic.

Subjekty údajů mají také právo přistupovat k možným profilům vycházejícím z těchto lokalizačních údajů. Jsou-li lokalizační údaje ukládány, uživatelům by mělo být umožněno tyto informace aktualizovat, opravovat či mazat.

Pracovní skupina doporučuje, aby správci usilovali o bezpečné způsoby poskytování přímého internetového přístupu k lokalizačním údajům a možným profilům. Hlavní zásadou je, aby byl takový přístup poskytován bez vyžadování dalších osobních údajů ke zjištění totožnosti subjektů údajů.

5.5 Období uchovávání

Poskytovatelé geolokalizačních služeb a aplikací by měli stanovit období uchovávání lokalizačních údajů, které není delší, než je nezbytné pro účely, ke kterým byly údaje shromážděny nebo ke kterým jsou dále zpracovávány. Tito poskytovatelé musí zajistit, že geolokalizační údaje nebo profily odvozené z takových údajů jsou po uplynutí odůvodněného období vymazány.

V případě, že je prokazatelně nezbytné, aby tvůrce operačního systému a/nebo správce geolokalizační infrastruktury shromažďoval za účelem aktualizace nebo zlepšení své služby anonymní údaje lokalizační historie, musí být pečlivě dbáno na to, aby se zamezilo (nepřímé) identifikovatelnosti těchto údajů. Zejména i v případě, že je mobilní zařízení identifikováno pomocí náhodně přiděleného jedinečného identifikátoru zařízení (UDID), takové jedinečné číslo by mělo být k provozním účelům uloženo maximálně pod dobu 24 hodin. Po této době by měla být provedena další anonymizace tohoto identifikátoru UDID s tím, že je třeba vzít v úvahu, že skutečná anonymizace je stále obtížněji proveditelná a že kombinované lokalizační údaje mohou přesto vést k identifikaci. Nemělo by být možné vytvořit vazbu tohoto identifikátoru UDID na předchozí či budoucí identifikátory UDID přidělené tomuto zařízení, ani na jakýkoli pevný identifikátor uživatele nebo telefonu (jako je adresa MAC, číslo IMEI nebo IMSI nebo jakákoli jiná zákaznická čísla).

Pokud se jedná o údaje o přístupových místech WiFi, jakmile dojde na základě nepřetržitých pozorování majitelů inteligentních mobilních zařízení ke spojení adresy MAC přístupového místa WiFi s novou lokalizací, předchozí lokalizace musí být ihned vymazána, aby se zabránilo jakémukoli dalšímu využití údajů k nevhodným účelům, jakým je marketing zacílený na lidi, kteří se přestěhovali.

6. Závěry

Pomocí geolokalizačních technologií, jakými jsou údaje základnové stanice, GPS a zmapovaná přístupová místa WiFi, mohou správci všech druhů sledovat inteligentní mobilní zařízení k účelům, jejichž rozsah se pohybuje od behaviorálně cílené reklamy po sledování dětí.

Vzhledem k tomu, že inteligentní telefony a tabletové počítače jsou neoddělitelně spjaty se svými majiteli, vzory pohybu těchto zařízení poskytují velmi podrobný pohled do soukromého života majitelů. Jedním z velkých rizik je to, že majitelé nemají povědomí o tom, že přenášejí svoji lokalizaci, ani o tom, komu. Dalším souvisejícím rizikem je to, že souhlas udělený určitým aplikacím s využíváním lokalizačních údajů majitelů je neplatný, protože informace o klíčových prvcích zpracování jsou nesrozumitelné, zastaralé nebo jinak nedostačující.

Různé zúčastněné strany od tvůrců operačních systémů po poskytovatele aplikací a strany typu internetových stránek sociálních sítí, které začleňují do svých platforem lokalizační funkce pro mobilní zařízení, mají různé povinnosti.

6.1 Právní rámec

- Právním rámcem EU pro využití geolokalizačních údajů z inteligentních mobilních zařízení je hlavně směrnice o ochraně údajů. Lokalizační údaje z inteligentních mobilních zařízení jsou osobními údaji. S kombinací jedinečné adresy MAC a stanovenou lokalizací přístupového místa WiFi by se mělo nakládat jako s osobními údaji.
- Revidovaná směrnice o ochraně soukromí v odvětví elektronických komunikací 2002/58/ES se navíc vztahuje pouze na zpracování údajů základnové stanice telekomunikačními operátory.

6.2 Správci

- Lze rozlišit tři typy správců. Jsou to: správci geolokalizační infrastruktury (zejména správci zmapovaných přístupových míst WiFi), poskytovatelé geolokalizačních aplikací a služeb a tvůrci operačního systému inteligentních mobilních zařízení.

6.3 Legitimní základ

- Vzhledem k tomu, že lokalizační údaje z inteligentních mobilních zařízení odhalují důvěrné údaje o soukromém životě jejich majitele, hlavním použitelným legitimním základem je předchozí informovaný souhlas.
- Souhlas nelze získat prostřednictvím všeobecných pravidel a podmínek.
- Pro každý z rozdílných účelů, pro které jsou údaje zpracovávány, musí existovat výslovný souhlas, včetně například pro tvorbu profilů a/nebo zacílení podle chování ze strany správce. Dojde-li k podstatné změně účelu zpracování, musí správce usilovat o nový výslovný souhlas.
- Lokalizační služby musí být implicitně vypnuty. Možný mechanismus výjimky není dostačující pro získání informovaného souhlasu uživatele.
- Pokud se jedná o zaměstnance a děti, souhlas je problematický. Pokud se jedná o zaměstnance, zaměstnavatelé mohou tuto technologii používat pouze, když je prokazatelně nezbytná pro oprávněný účel a když nelze stejných cílů dosáhnout méně invazivními prostředky. Pokud se jedná o děti, rodiče musí posoudit, zda je používání takové aplikace za zvláštních okolností odůvodněné. Rodiče o tom musí

děti přinejmenším informovat a musí jim umožnit podílet se na rozhodnutí o používání takové aplikace, jakmile je to rozumně možné.

- Pracovní skupina doporučuje časově omezit působnost souhlasu a připomínat jej uživatelům alespoň jednou ročně. Pracovní skupina také doporučuje zahrnout do souhlasu dostatečnou úroveň přesnosti lokalizačních údajů.
- Subjekty údajů musí být schopné souhlas velmi snadno odejmout, aniž by to mělo jakékoli negativní důsledky pro používání jejich zařízení.
- Pokud se jedná o mapování přístupových míst WiFi, společnosti mohou mít oprávněný zájem v nezbytné míře shromažďovat a zpracovávat adresy MAC a stanovené lokalizace přístupových míst WiFi pro zvláštní účel nabídky geolokalizačních služeb. Rovnováha zájmů mezi právy správce a právy subjektů údajů vyžaduje, aby správce nabízel právo snadného a trvalého výmazu z databáze bez požadování dalších osobních údajů.

6.4 Informace

- Informace musí být jasné, vyčerpávající a srozumitelné pro širokou netechnickou veřejnost a musí být trvale a snadno přístupné. Platnost souhlasu je neoddělitelně spjata s kvalitou informací o službě.
- Třetí strany, jako jsou prohlížeče a internetové stránky sociálních sítí, hrají klíčovou úlohu v oblasti zajištění viditelnosti a kvality informací o zpracování geolokalizačních údajů.

6.5 Práva subjektů údajů

- Různí správci geolokalizačních informací z mobilních zařízení by měli svým zákazníkům umožnit, aby tito měli zajištěn přístup ke svým lokalizačním údajům ve formátu čitelném pro lidi a měli by umožňovat jejich opravu a výmaz, aniž by v nadměrné míře shromažďovali osobní údaje.
- Subjekty údajů mají také právo na přístup, opravu a výmaz možných profilů vycházejících z těchto lokalizačních údajů.
- Pracovní skupina doporučuje vytvoření (bezpečného) internetového přístupu.

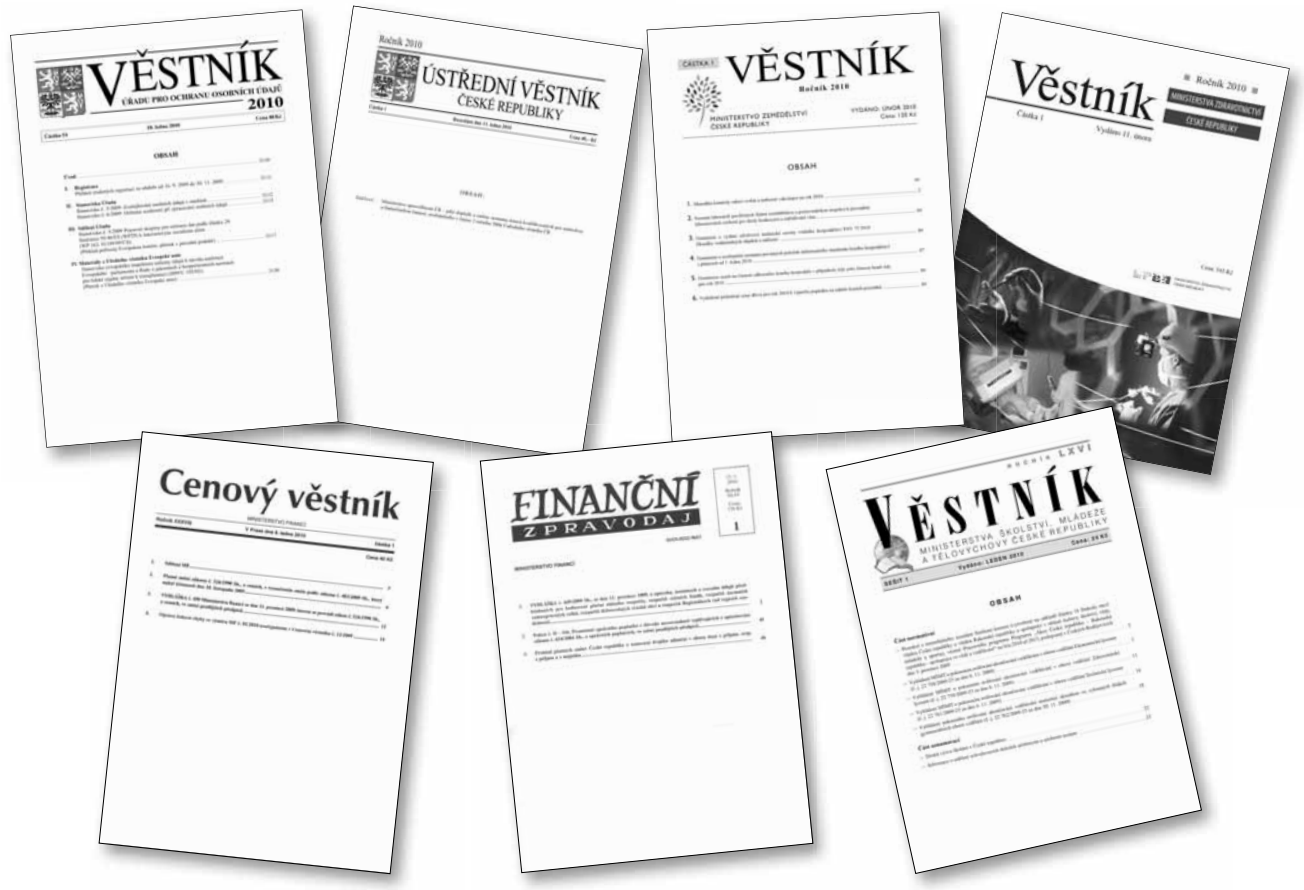
6.6 Období uchovávání

- Poskytovatelé geolokalizačních aplikací nebo služeb by měli provést politiky pro uchovávání, které by zajišťovaly, že geolokalizační údaje nebo profily odvozené z takových údajů jsou po uplynutí odůvodněného období vymazány.
- Jestliže tvůrce operačního systému a/nebo správce geolokalizační infrastruktury zpracovává v souvislosti s lokalizačními údaji jedinečné číslo, jako je adresa MAC nebo identifikátor UDID, jedinečné identifikační číslo může být k provozním účelům uloženo maximálně po dobu 24 hodin.

V Bruselu dne
16. května 2011

Za pracovní skupinu
předseda
Jacob KOHNSTAMM

Vyberte si z nabídky věstníků a zpravodajů



Předpokládaná výše předplatného pro rok 2012 a periodicita distribuovaných věstníků a zpravodajů:		
Název věstníku, zpravodaje	**Předpokládaná periodicita**	**Záloha na předplatné**
Věstník Úřadu pro ochranu osobních údajů	4krát ročně	400 Kč
Ústřední věstník ČR	7krát ročně	950 Kč
Věstník Ministerstva zemědělství	3krát ročně	300 Kč
Věstník Ministerstva zdravotnictví	10krát ročně	3900 Kč
Cenový věstník Ministerstva financí	16krát ročně	1700 Kč
Finanční zpravodaj	6krát ročně	650 Kč
Věstník Ministerstva školství, mládeže a tělovýchovy ČR	12krát ročně	600 Kč

SEVT®

Objednávky přijímá a vyřizuje: SEVT, a. s., oddělení předplatného, Pekařova 4, 181 06 Praha 8 – Bohnice
Tel.: 283 090 354 • Fax: 233 553 422 • e-mail: predplatne@sevt.cz
Obsahy věstníků a zpravodajů na www.sevt.cz

Oficiální distributor Úředního věstníku EU

www.sevt.cz

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 400 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

62012002