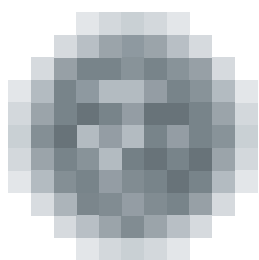


Výroční zpráva 2014



**úřad pro ochranu
osobních údajů**
the office for personal
data protection

Ohlédnutí předsedy Úřadu



Vážení, je to po desáté a naposled, co Vám předkládám výroční zprávu o činnosti instituce, která procházela co do obsahu i formy snad největšími změnami ze všech orgánů státu. Jenom zákon, který nás zřizuje, byl více než 25krát novelizován.

Předně došlo k velkému posunu v uplatňování nových technologií, které mají silný vliv na soukromí. Jednak umožňují shromažďování, uchovávání a rozsáhlé zpracování osobních údajů bezprostředně, ale také v dlouhodobém horizontu. V době, kdy jsem nastoupil na Úřad, neexistovaly např. sociální sítě.

Vznikla nová témata, jako je snaha o zajištění bezpečnosti přenosů osobních údajů do zemí, které nezajišťují dostatečnou ochranu osobních údajů, což se stává přímo bezpečnostním problémem celostátního a evropského dopadu. Tento úhel pohledu pro mne vyvstával zcela zřetelně zejména na základě mého působení v evropském expertním orgánu pro ochranu osobních údajů Evropské komise, za mého působení ve funkci místopředsedy skupiny WP29. Jsem si jist, že tento problém, spojený například s cloud computingem či profilováním, bude naléhavě řešit i český Úřad ještě dlouho poté, kdy z pozice jeho předsedy v září roku 2015 odejdu.

Dalším dokladem toho, že se práce Úřadu značně mění, je proměna kvality dotazů, ale zejména žádostí o konzultace, s nimiž se na Úřad obrací osoby fyzické, ale také právnické. Náročnost práce v tomto ohledu ovšem nepochybně narostla také díky úsilí, které Úřad vynakládal na šíření povědomí o ochraně osobních údajů.

Musím ovšem v tomto kontextu konstatovat také dvě věci: na jedné straně je snaha některých občanů využívat ochranu osobních údajů k zástupnému řešení sporů, které zákon o ochraně osobních údajů řešit nemůže ani nesmí, přesto se ho snaží využít díky většímu právnímu povědomí, leč mylnému výkladu k řešení svých neuspokojených občanskoprávních nároků. Na druhé straně stojí snahy advokátních kanceláří těžit z povinnosti Úřadu poskytovat zdarma konzultace. Rád bych věřil tomu, že nový podpůrný nástroj vypracovaný ve spolupráci Evropské komise a Rady Evropy „Příručka evropského práva v oblasti ochrany osobních údajů“, na niž odkazují webové stránky Úřadu, pomůže i právníkům a advokacii vyrovnávat se s vyžadovanými náročnými konzultacemi. Na straně Úřadu tu jde vždy o čas jasně určeného počtu zaměstnanců, který nelze donekonečna přečerpávat. K anglické verzi publikace v příštím roce navíc přibude i verze česká. Tedy publikace určená především právníkům, kteří se speciálně ochraně osobních údajů nevěnují, která bude bezproblémově dostupná. Nabídne oporu v judikátech Evropského soudu pro lidská práva i lucemburského Soudního dvora Evropské unie v oblasti ochrany základního práva evropských občanů na soukromí.

V této souvislosti nemohu opomenout dlouholetou snahu Úřadu prosadit vyvážený přístup k ochraně soukromí a zajišťování bezpečnosti. Obávám se, že v souvislosti s bojem proti terorismu budou však i nadále přijímána často málo uvážlivá řešení v oblasti bezpečnosti, a tím budou oslabovat jistoty práva na ochranu soukromí. Tyto snahy už Úřad zaznamenal v souvislosti s modernizací Úmluvy č. 108, kdy se projevil tlak ze strany gestora ochrany osobních údajů Ministerstva vnitra nepracovat s možnostmi výjimek, ale požadovat přímo vynětí bezpečnostních složek z jakékoliv kontroly nabízené právními normami, k nimž se demokratické společnosti v Evropě v dlouhodobém procesu dopracovaly. S velkými obavami tedy očekávám, že mohou přijít vniveč i kroky českého Úřadu, které vedly k tomu, že se podařilo najít pravidla pro nakládání policie se záznamy odposlechů a tak lepší ochraně soukromí obyvatel – pro kterou v roce 2006 negativně hodnotila Českou republiku i společnost Privacy International. Obávám se, že dlouholeté úsilí Úřadu a jeho inspektorů k vyváženému přístupu policie k nakládání s profily DNA, které by respektovalo mezinárodně přijímaná pravidla, může v kontextu boje proti terorismu zůstat zcela mimo jakoukoli náležitou úpravu a že volání nejen ochránců ochrany osobních údajů, ale i řady odborníků z řad genetiků po přijetí precizního zákona o DNA bude odsunuto opět do ne-určita (jak se děje už od roku 2006 a naléhavě znovu od roku 2011). Též se obávám v souvislosti s využíváním kamerových sledovacích systémů, poněvadž využívání kamer nemá v České republice speciální právní úpravu.

Ve světle dobré spolupráce s Ministerstvem vnitra při přípravě vstupu České republiky do Schengenského systému mě tyto zkušenosti nenaplňují žádnou radostí. Tím spíše, když si uvědomuji, že pokud se mé obavy naplní, bude to důkazem neblahého ústupku a oslabení demokracie ve vztahu k fundamentalistickým tažením proti jejím hodnotám, mezi něž v průběhu vývoje byla zakotvena, jako základní právo, ochrana soukromého života a osobních údajů.

Spokojeností mě naopak naplňuje několik věcí, které se Úřadu podařily: předně se jedná o zajištění výkonu povinností, které pro Úřad vyplynuly z postupně nově svěřovaných kompetencí v průběhu uplynulých devíti let:

Zvládnutí velmi rozsáhlé agendy spojené s postihem nevyžádaných obchodních sdělení, úspěšné plnění dozorových povinností spojených s provozem Schengenského informačního systému, a to i v rámci mezinárodní participace zaměstnanců Úřadu, kterému předcházela pozitivní mezinárodní evaluace Úřadu před přistoupením České republiky do Schengenu. Další záležitostí je zajištění speciální součásti základních registrů, páteře elektronizace státní správy, která znamenala pro Úřad vybudování zcela nového bezpečnostně náročného pracoviště. Úřad také bezproblémově plnil své povinnosti v období českého předsednictví Evropské unii. Úspěšná byla i spolupráce s Ministerstvem průmyslu a obchodu na konferenci o digitálních výzvách v roce 2014, což už je aktivita, která směřuje k jisté budoucnosti. Dlouhá byla cesta ke zlepšení ochrany osobních údajů v katastru nemovitostí a v živnostenském rejstříku, ale ke zlepšení přeci jen došlo.

Posílení pozice Úřadu v rámci mezinárodních aktivit započalo už v letech 2005–2006, kdy český Úřad poskytoval know-how v rámci evropského Projektu dlouhodobé pomoci Bosně a Hercegovině. Pomoci Komisi Bosny a Hercegoviny. Úřad úspěšně spolupracoval také s polským, maďarským a chorvatským partnerským úřadem: v rámci programu Leonardo da Vinci společně vytvořily dvě příručky o ochraně osobních údajů pro oblast zaměstnanosti. Jedna z publikací je určena pro orientaci podnikajících subjektů v ochraně osobních údajů, druhá přistupuje k problému z hlediska zaměstnance a posiluje znalosti o právech a povinnostech spojených s ochranou jejich osobních údajů.

Úřad přijal a poskytoval konzultace bezpočtu zahraničním odborníkům – namátkově si připomínám albánskou, rumunskou, ukrajinskou a čínskou návštěvu, úspěšný seminář pro studenty práv univerzity v Chicagu, účast na telemostu mezi českými a americkými středoškoláky pořádaný Americkým kulturním střediskem v Praze – ve výčtu by se dalo dlouze pokračovat. V roce 2010 byl Úřad pořadatelem evropské konference komisařů ochrany osobních údajů, která samozřejmě i díky prostředí Pražského hradu, kde byla hostem, zaznamenala velký ohlas. Oceňována je také práce zaměstnanců Úřadu v mezinárodních organizacích, jako je dozorový orgán Europolu, Evropská komise a její WP29, Rada Evropy a její poradní výbor k Úmluvě č. 108, Berlínská skupina, účast na každoročním setkání k výměně poznatků z dozorové činnosti i ve skupině států středoevropské, východoevropské, jihoevropské skupiny a pobaltských států, jež je vhodným prostorem k výměně zkušeností s ochranou osobních údajů ve státech, které mají zkušenosti s totalitními režimy a z toho plynoucími důsledky i pro vytváření prostředí respektujícího ochranu soukromí. Český a polský úřad byly zakládajícími členy této skupiny.

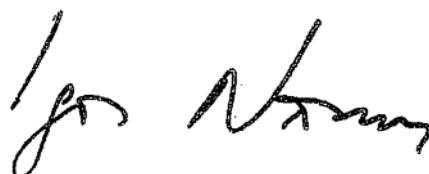
Opomenout nemohu ani mezinárodní ocenění v Madridu, kterého se roku 2007 dostalo Úřadu za nejlepší projekt v oblasti vzdělávání v ochraně osobních údajů, který byl na tři roky rovněž akreditován Ministerstvem školství, mládeže a tělovýchovy. Doposud Úřad pořádá každoročně soutěž pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“, která byla součástí oceněného projektu a která má stále širší podporu ve školách, ale i v médiích, a rozšiřuje svou partnerskou spolupráci. Obdobně i pořádání kulatých stolů s odborníky, kteří se musejí ve svém podnikání či práci vyrovnat s požadavky ochrany osobních údajů (bezpečnostní agentury, advokátní kanceláře, média), plní výborně úlohu dialogu, který napomáhá zakotvení ochrany osobních údajů jakožto nezbytné složky dobrého fungování společnosti respektující svobodu jedince a jeho práva.

V neposlední řadě ovšem musím ocenit spolupráci se zaměstnanci Úřadu, v nichž jsem našel mimořádně kooperativní a profesionálně i morálně zdatný tým. Ocenil jsem velmi, že práce nových inspektorů, kteří přicházeli do Úřadu v roce 2011, organicky navazovala na práci těch, jimž vypršel mandát, a v souladu s tím, jak přicházely nové problémy, se rozvíjela i kontrolní činnost a kooperace kolegia inspektorů.

Účast externích odborníků v práci rozkladové komise, která je mým poradním orgánem, byla přínosná i z hlediska vyváženosti právních názorů, jimiž Úřad prosazuje v České republice jedno ze základních lidských práv. Přál bych si, aby skutečně vyvážený přístup k ochraně osobních údajů byl posilován, což konstatuji s vědomím toho, že ochrana osobních údajů byla v poslední době velmi oktrojována především zdůrazňováním práva na přístup k informacím.

Stejně tak bych si přál, aby Úřad v příštím roce dokázal bez otřesů integrovat zákon o státní službě ve prospěch naplňování smyslu zákona o ochraně osobních údajů, jímž je služba občanům demokratického státu.

Vážený Senáte, chtěl bych Vám poděkovat za velmi dobrou spolupráci i za to, že Úřad si zachoval nezávislost, která je v Evropské unii příkladná.



Igor Němec

Obsah

| | |
|--|----|
| ÚŘAD V ČÍSLECH 2014 | 10 |
| KONTROLNÍ ČINNOST ÚŘADU | 13 |
| KONTROLNÍ PLÁN | 14 |
| 1. Informační systémy s velkým objemem dat | 14 |
| 2. Vliv nových technologií na podmínky zpracování osobních údajů | 16 |
| 3. Dodržování podmínek schengenského právního rámce | 16 |
| 4. Další oblasti kontrol dle kontrolního plánu | 17 |
| 5. Kontroly splnění uložených opatření k nápravě | 19 |
| KONTROLY ZAHÁJENÉ NA ZÁKLADĚ PODNĚTU PŘEDSEDY ÚŘADU | 20 |
| POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI | 25 |
| I. KONTROLNÍ PLÁN | 25 |
| Zpracování osobních údajů žadatelů a příjemců finančních prostředků ze Státního fondu životního prostředí | 25 |
| Zpracování osobních údajů pacientů v elektronické podobě prostřednictvím nemocničního informačního systému | 27 |
| Vězeňská služba ČR – evidence a identifikace vězňených osob | 28 |
| Monitoring zaměstnanců | 30 |
| II. KONTROLY ZAHÁJENÉ NA ZÁKLADĚ PODNĚTU PŘEDSEDY ÚŘADU | 35 |
| Ochrana osobních údajů zpracovávaných v rámci Celního informačního systému (CIS) a v Identifikační databázi celních spisů (FIDE) | 35 |
| Kontrola využívání dynamického biometrického podpisu | 38 |
| Kontrola aplikace Centrální elektronický platební rozkaz | 44 |
| Zpracování osobních údajů v insolvenčním rejstříku | 40 |
| Kontrola zpracování osobních údajů vlastníků a provozovatelů motorových vozidel v systému AUTOTRACER (zpracování VIN automobilů) | 41 |
| III. KONTROLY DLE JEDNOTLIVÝCH TEMATICKÝCH OKRUHŮ | 44 |
| A. Zpracování osobních údajů prostřednictvím sledovacích systémů na pracovištích, v dopravních prostředcích a bytových domech | 44 |
| Kamerový systém v bytovém domě | 44 |
| Rozšíření kamerového systému v bytovém domě | 46 |
| Kamerový systém ve společných prostorách bytového domu provozovaný nájemcem nebytových prostor | 46 |
| Kamerový systém v prostředcích hromadné dopravy | 48 |

| | |
|---|----|
| B. Zpracování citlivých údajů při poskytování zdravotnických služeb | 50 |
| Ztráta zdravotnické dokumentace pacientky v Lužické nemocnici | 50 |
| Obsah údajů v lékařském posudku | 51 |
| Zpracování osobních údajů klientů zdravotní pojišťovny v rámci jejich přeregistrace | 52 |
| C. Osobní údaje zpracovávané v dlužnických registrech | 53 |
| Osobní údaje zpracovávané na www.dluzis.cz a v dlužnických registrech SOLUS | 53 |
| D. Poskytovatelé energetických služeb a zpracování osobních údajů klientů | 57 |
| Dodržování povinností správce osobních údajů se zaměřením na náležitosti souhlasu subjektů údajů při uzavírání smlouvy za využití všeobecných obchodních podmínek | 57 |
| E. Samostatné příspěvky | 57 |
| Kontrola společnosti www.scio.cz, s.r.o. | 57 |
| Seznamy členů sdružení | 59 |

OSTATNÍ DOZOROVÁ ČINNOST 64

VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ 64

NĚKTERÉ POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ 68

| | |
|---|----|
| K řízením podle § 17 zákona č. 101/2000 Sb. | 68 |
| K možnosti upustit od uložení pokuty | 68 |

POZNATKY ZE SOUDNÍCH PŘEZKUMŮ 70

| | |
|--|----|
| Dohled zajišťovaný pomocí videokamer na pracovišti je aplikovatelný pouze v případě, kdy stanovený účel nelze naplnit prostřednictvím mírnějších prostředků; tomuto účelu je nutno přizpůsobit i stanovení lhůty pro zpracování záznamů. Plnění informační povinnosti dle § 11 zákona č. 101/2000 Sb. je závislé na okruhu monitorovaných osob. V případě pochybností má správce osobních údajů požádat o konzultaci podle § 29 odst. 1 zákona č. 101/2000 Sb. | 70 |
|--|----|

| | |
|--|----|
| Provozní a lokalizační údaje evidované a uchovávané podle ustanovení § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, není možno zpřístupnit s odkazem na ustanovení § 40 odst. 1 písm. a) zákona č. 121/2000 Sb., autorský zákon | 72 |
|--|----|

| | |
|--|----|
| Pokud kontrolovaný hodlá poukazovat na to, že mu byly uloženy povinnosti, které již neodpovídají aktuálnímu stavu věci, je třeba, aby toto učinil již v námitkách proti protokolu o kontrole | 72 |
|--|----|

| | |
|---|----|
| Příprava televizní reportáže směřující ke zveřejnění osobních údajů prostřednictvím televizního vysílání je zpracováním osobních údajů ve smyslu zákona č. 101/2000 Sb. | 73 |
|---|----|

Vynaložení veškerého úsilí, které bylo možno požadovat ve smyslu § 46 zákona č. 101/2000 Sb., neznamená jakékoliv úsilí, které správce osobních údajů vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat

| | |
|--|-----|
| o úsilí maximálně možné, které je správce objektivně schopen vynaložit. Jako liberační důvod tudíž nemůže postačovat fakt, že uzavřená smlouva o dílo obsahovala detailní popis postupu od převzetí specifického odpadu od správce další odpovědnou osobou | 73 |
| REGISTRACE | 75 |
| PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ | 78 |
| SCHENGENSKÁ SPOLUPRÁCE | 82 |
| LEGISLATIVNÍ ČINNOST | 85 |
| STYKY SE ZAHRANIČÍM A MEZINÁRODNÍ SPOLUPRÁCE | 90 |
| ÚŘAD, SDĚLOVACÍ PROSTŘEDKY A KOMUNIKAČNÍ NÁSTROJE | 93 |
| Šíření znalostí o ochraně osobních údajů | 94 |
| Knihovna a publikace Úřadu | 95 |
| Webové stránky Úřadu | 95 |
| INFORMAČNÍ SYSTÉM ORG | 96 |
| PERSONÁLNÍ OBSAZENÍ ÚŘADU | 99 |
| HOSPODAŘENÍ ÚŘADU | 101 |
| POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM | 106 |
| VYŘIZOVÁNÍ STÍŽNOSTÍ PODLE § 175 SPRÁVNÍHO ŘÁDU | 108 |

Úřad v číslech 2014

| | | |
|---|---|-------------|
| Dotazy a konzultace | dotazy a konzultace ČR | 2965 |
| | zahraničí | 35 |
| | z toho | |
| | státní správě | 148 |
| | samosprávě | 191 |
| | právníckým osobám | 498 |
| | fyzickým osobám podnikajícím fyzickým osobám | 344 1819 |
| Podání a stížnosti | přijaté podněty dle zákona č. 101/2000 Sb. | 1536 |
| | stížnosti předané ke kontrole nebo správnímu řízení | 237 |
| Nevyžádaná obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.) | podnětů celkem | 7951 |
| | vyřešených podnětů | 5792 |
| | zahájených kontrol | 23 |
| | ukončených kontrol | 14 |
| | správních rozhodnutí o pokutě | 8 |
| | napadeno námitkami | 12 |
| | námitkám vyhověno | 0 |
| | nevyhověno | 10 |
| | převážně vyhověno | 0 |
| převážně nevyhověno | 2 | |
| Kontrolní činnost (vyjma kontrol týkajících se zákona č. 480/2004 Sb.) | zahájeno | 144 |
| | ukončeno | 128 |
| | předáno jiným státním úřadům | 3 |
| | napadeno námitkami | 11 |
| | námitkám vyhověno | 1 |
| | nevyhověno | 7 |
| | převážně vyhověno | 0 |
| | převážně nevyhověno | 4 |
| | analýzy | 34 |

| | | |
|---|---|-----------|
| Správní trestání | správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb., o evidenci obyvatel | 78 |
| | přestupková řízení podle zákona č. 101/2000 Sb. | 17 |
| | správní a přestupkové řízení podle zákona č. 101/2000 Sb. – § 44a, 45a | 10 |
| | přestupková řízení o porušení zákona č. 159/2006 Sb., o střetu zájmů | 0 |
| | rozklady napadená rozhodnutí o porušení zákona | 32 |
| | zamítnutých rozkladů | 20 |
| | zrušeno a vráceno k novému projednání | 2 |
| | zrušených rozhodnutí a zastaveno řízení | 5 |
| | změna rozhodnutí | 6 |
| Soudní přezkum (Pozn.: * celkem od r. 2001) | podaných žalob k soudu | 10 (128*) |
| | zamítnutých žalob soudem | 4 |
| | zrušených rozhodnutí soudem | 9 |
| | ukončených/neukončených soudních řízení od roku 2001 | 88/40 |
| Registrace | přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.) | 7686 |
| | zaregistrovaná zpracování | 7392 |
| | dosud v řízení | 1001 |
| | zrušené registrace | 132 |
| | oznámení o změně zpracování | 845 |
| | řízení podle § 17 | 134 |
| | zastaveno (nedochází k porušení zákona) | 106 |
| | zastaveno z procesních důvodů (např. oznámení vzato zpět) | 13 |
| nepovoleno | 4 | |
| Povolení k předávání osobních údajů do zahraničí | přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.) | 40 |
| | rozhodnutí o povolení předávání | 30 |
| | rozhodnutí o nepovolení | 0 |
| | zastavená řízení z procesních důvodů | 8 |
| Oznámení podle zákona č. 127/2005 Sb. | došlých oznámení | 2 |
| Stížnosti podle § 175 správního řádu | přijatých stížností | 39 |
| | vyřízených jako důvodné | 10 |
| | vyřízených jako částečně důvodné | 5 |
| | vyřízených jako bezdůvodné | 24 |

| | | |
|---|------------------------------|----|
| Žádosti podle zákona č. 106/1999 Sb. | přijatých žádostí | 74 |
| | zcela vyhověno | 43 |
| | částečně vyhověno | 23 |
| | odmítnutých žádostí | 8 |
| Publikované materiály | Věstník Úřadu (počet částek) | 2 |
| | Bulletin Úřadu (počet čísel) | 1 |
| Připomínkové legislativní návrhy | zákony | 81 |
| | prováděcí předpisy | 53 |
| | návrhy nařízení vlády | 15 |
| | návrhy vyhlášek | 38 |
| | ostatní | 61 |
| | zahraniční materiály | 13 |

Kontrolní činnost Úřadu

Úřad pro ochranu osobních údajů (dále jen „Úřad“), který byl zřízen v souladu s právním rámcem Evropské unie jako nezávislý dozorový orgán v oblasti kontroly nad dodržováním povinností odpovědných subjektů při zpracování osobních údajů, se v roce 2014 zaměřil na některé významné trendy a aktivity odpovědných subjektů při využití moderních technologií pro zpracování osobních údajů zaměstnanců, klientů, pacientů, příjemců dotací a dalších kategorií fyzických osob.

Záměry odpovědných subjektů, které jsou často založeny na zákonné bázi pro prvotní účel zpracování, se často kombinují a zaměřují s cílem soustředit a dále využít tyto informace, které jsou osobními údaji, pro účel, jenž se výrazně odlišuje od účelu původního, aniž odpovědný subjekt disponuje zákonnou licenci pro takovéto druhotné zpracování.

Úřad prostřednictvím kontrolního plánu pro určité časové období současně využívá své poznatky z kontrol prováděných v uplynulém období, kdy se ukázalo, že shromažďování nejrůznějších osobních informací a jejich následné vyhodnocení s cílem profilovat jednotlivce z různých úhlů jeho života a následně tyto informace distribuovat pro účely marketingu bylo a zůstává dlouhodobým trendem mnoha podnikatelských subjektů, ale není výjimečné ani ve sféře veřejnoprávní, kdy se občan může obrátit na stát s požadavkem poskytnutí určité služby, finanční částky ve formě sociálního příspěvku, pronájmu obecního bytu, poskytnutí určité úlevy na daních nebo poplatcích apod. a v této souvislosti je nucen doložit řadu informací a dokumentů týkajících se jeho životních podmínek.

Existence databází označovaných aktuálně jako „big data“ nelze tradičně spojovat jen se subjekty státu nebo subjekty typu velkých bankovních a pojišťovacích korporací. Vlastnictví dat znamená být odpovědný za jejich ochranu. Proto se Úřad v roce 2014 důsledněji zaměřil na způsob zabezpečení databází proti neoprávněnému přístupu a manipulaci s osobními údaji.

Při realizaci kontrolního plánu se inspektoři a jejich kontrolní týmy zaměřili na následující obecná témata:

• KONTROLNÍ PLÁN

1. INFORMAČNÍ SYSTÉMY S VELKÝM OBJEMEM DAT

Rozsáhlé informační systémy s velkým objemem dat patří trvale mezi kontrolní záměry Úřadu. Pro možnost srovnání dodržování práv a povinností odpovědných subjektů si každoročně Úřad volí různé oblasti, a díky tomu tak může porovnávat úroveň aplikace zákona č. 101/2000 Sb., o ochraně osobních údajů, v jednotlivých sektorech. V roce 2014 proběhla kontrola těchto databází:

1.1. Centrální elektronický platební rozkaz:

Záměrem Úřadu bylo prověřit rejstřík elektronických platebních rozkazů a další evidenční pomůcky a spisy, které se v elektronickém rozkazním řízení vedou, a všechny další činnosti s řízením související, jež se provádějí výlučně prostřednictvím výpočetní techniky. Za tímto účelem soudy využívají příslušného programového vybavení (aplikace Centrálního elektronického platebního rozkazu, dále „CEPR“), jehož správu zajišťuje Ministerstvo spravedlnosti. Veškeré činnosti prováděné v aplikaci CEPR se řídí příslušnou programovou dokumentací. O zařazení jednotlivých soudů do projektu CEPR rozhoduje Ministerstvo spravedlnosti.

Kontrola proběhla s následujícím výsledkem:

Jedním z důležitých kontrolních zjištění bylo, že nařízená a v praxi realizovaná periodická kontrolní opatření v dostatečné míře eliminují rizika neoprávněného přístupu ke zpracovávaným osobním údajům a nevytvářejí prostor k pochybení systémového charakteru.

Vzhledem k uvedenému byl učiněn závěr, že kontrolou Ministerstva spravedlnosti, jako provozovatele aplikace CEPR, ani kontrolou jednoho z náhodně vybraných uživatelů této aplikace – Okresního soudu v Klatovech, nebylo zjištěno porušení zákona č. 101/2000 Sb.

Více o průběhu a výsledcích kontroly lze nalézt v části Poznatky inspektorů z kontrolní činnosti.

1.2. Realizace operačních a dotačních programů:

1.2.1. Díky možnostem aktivně se zúčastnit a realizovat operační programy, jejichž součástí je dokumentační agenda, vstupuje celá řada odpovědných subjektů do zpracování osobních údajů, aniž si úzkou souvislost a povinnost zpracovávat osobních údaje v souladu se zákonem č. 101/2000 Sb. včas uvědomí. Následné řešení problémů může pro odpovědný subjekt přinést poměrně velké komplikace. Úřad si pro kontrolní aktivity v roce 2014 vytypoval projekt **Klidné příhraničí**, který hodlá realizovat Sdružení obcí mikroregionu Šumava. Kontrola se měla zaměřit na dodržování povinností správce osobních údajů při instalaci a následném provozu preventivních zařízení a prvků, které přispějí ke zvýšení bezpečnosti a plynulosti silničního provozu a k jeho monitoringu.

Vzhledem k tomu, že příprava projektu včetně schvalovacích procedur se prodloužila, bylo rozhodnuto zahájení kontroly odložit na příští sledované období.

1.2.2. Na základě kontrolního plánu Úřadu pro rok 2014 byla zahájena kontrola **Ministerstva školství**, jejímž předmětem je dodržování povinností správce osobních údajů

stanovených v Hlavě II zákona č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů v dokumentační agendě dotačních titulů MŠMT vyhlášených jako Státní podpora sportu pro roky 2013 a 2014.
Uvedená kontrola dosud probíhá.

1.3. Zpracování osobních údajů klientů banky:

Záměrem kontroly bylo v návaznosti na výsledky a zkušenosti z předcházejících období prověřit realizaci opatření směřujících k vytváření objektivních podmínek respektujících zásady ochrany osobních údajů. Oblast bankovníctví a poskytování souvisejících finančních služeb je tradiční součástí kontrolních záměrů Úřadu. I když hodnocení dodržování povinností není vždy přijímáno s potřebným respektem, Úřad se vždy snažil a snaží prosazovat taková pravidla, která by klienty nediskriminovala.

V roce 2014 byla kontrola zaměřena na **Sberbank CZ, a. s.**

Kontrola proběhla s následujícím výsledkem:

Kontrola se zaměřila na dodržování povinností správce při komunikaci s klienty, kdy dochází k shromažďování a dalšímu zpracování osobních údajů klientů v souvislosti s nabízením služeb banky a uzavíráním smluvních vztahů. Účelem tohoto procesu je plnit smluvní podmínky.

Kontrola, která byla v roce 2014 zahájena, konstatovala porušení povinností kontrolovaného subjektu, které mu vyplývají z § 11 odst. 1 zákona č. 101/2000 Sb. V návaznosti na kontrolní poznatky bude Úřad iniciovat jednání s Ministerstvem vnitra, jehož účelem je odstranění současných výkladových problémů při aplikaci zákazu pro pořizování kopií občanských průkazů, které obsahují strojově čitelné údaje.

1.4. Provoz státních fondů v souvislosti se zpracováním osobních údajů:

S vědomím, že součástí odborné agendy fondů jsou rovněž databáze obsahující rozsáhlé skupiny osobních údajů, se Úřad v roce 2014 rozhodl prověřit podmínky, za kterých ke zpracování dochází.

Úřad se v roce 2014 zaměřil na **Státní fond životního prostředí ČR** zřízený zákonem č. 388/1991 Sb., o Státním fondu životního prostředí České republiky jako subjekt spravující prostředky, které lze mimo jiné použít i na podporu investičních a neinvestičních akcí právnických a fyzických osob souvisejících s ochranou a zlepšováním životního prostředí.

Kontrola proběhla s následujícím výsledkem:

Databáze příjemců/žadatelů podpor vedená SFŽP v elektronické podobě byla zabezpečena v souladu se zákonem č. 101/2000 Sb.; k předání osobních údajů žadatelů a příjemců podpor jiné třetí osobě nedochází bez legislativní opory; pokud jde o předávání údajů do zahraničí v rámci dotací z Evropské unie, nebylo před kontrolou ani v době kontroly takovéto předávání realizováno.

Více o průběhu a výsledcích kontroly lze nalézt v části Poznatky inspektorů z kontrolní činnosti.

Dalším fondem, kde bylo v roce 2014 prověřováno zpracování osobních údajů osob v souvislosti s provozem informačního systému s velkým objemem dat, byl **Státní fond kultury ČR**, zřízený zákonem č. 239/1992 Sb., o Státním fondu kultury ČR, jehož prostředky se poskytují jako účelové dotace, půjčky nebo návratné finanční výpomoci pro pořádání kulturních festivalů, přehlídek a obdobných kulturních akcí, podporu kulturních projektů sloužících k uchování

a rozvíjení kultury národnostních menšin v České republice nebo například pro podporu vysoce hodnotných neprofesionálních uměleckých aktivit.

Kontrola dosud probíhá.

2. VLIV NOVÝCH TECHNOLOGIÍ NA PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

V průběhu roku 2014 došlo v rámci technologické podskupiny WP29 k dohodě na společném testu technologie cookies. Cookies, malé datové soubory, jsou při návštěvě určité webové stránky ukládány na koncových zařízeních uživatelů připojených k internetu. Uživatelé tímto způsobem zanechávají stopu o své činnosti v prostředí internetu, ze které mohou provozovatelé cookies získat užitečné informace. Tyto informace jsou částečně potřeba k zajištění funkčnosti webových stránek, např. při přihlášení do e-mailového účtu (tzv. session cookies). Některé cookies slouží pro účely nezasahující do soukromí konkrétních uživatelů. Konečně část těchto uložených informací slouží k marketingovým a reklamním účelům a soukromí uživatelů se již bezprostředně dotýká. Nezanedbatelná část cookies shromažďuje informace o chování konkrétních uživatelů, typicky vytváří profily jejich chování na internetu za účelem adresného marketingu.

V návaznosti na dokument WP29 a dohodu technologické podskupiny byla podrobena kontrole současná praxe několika poskytovatelů služeb elektronických komunikací se zaměřením na publikované podmínky a politiku ochrany osobních údajů.

V září 2014 došlo k provedení testu, ze kterého Úřad zpracoval základní analýzu, jež bude východiskem pro další kontrolní aktivity. Z analýzy mimo jiné vyplývá, že plnění povinností ve vztahu k využívání tzv. cookies obecně není mezi českými provozovateli webových stránek na adekvátní úrovni. Dále je zřejmé, že současný stav v České republice neodpovídá evropské ani české (nedostatečně transponované) právní úpravě, a práva uživatelů internetu tak jsou systematicky narušována.

Úřad se jako regulátor bude i v příštím období prostřednictvím dozorových aktivit touto situací zabývat.

3. DODRŽOVÁNÍ PODMÍNEK SCHENGENSKÉHO PRÁVNÍHO RÁMCE

3.1. Kontrola provozu agendy Vízového informačního systému:

Tak jako každoročně i v roce 2014 provedl Úřad kontroly dodržování podmínek schengenské úmluvy při udělování víz cizincům pro vstup na území ČR. V rámci této agendy, kdy kontrolovaným subjektem bylo Ministerstvo zahraničních věcí, proběhly dvě kontroly na místě, a to kontrola konzulárního úřadu při Velvyslanectví České republiky v Gruzii se sídlem v Tbilisi a kontrola konzulárního úřadu při Velvyslanectví České republiky v Egyptě se sídlem v Káhiře.

Kontroly proběhly s následujícím výsledkem:

Kontrola konzulárního úřadu při **velvyslanectví v Tbilisi** byla zaměřena na plnění povinností správce osobních údajů, zejména s ohledem na plnění ustanovení § 11 zákona č. 101/2000 Sb.

při informování subjektu údajů a povinností správce při zabezpečení osobních údajů dle § 13 zákona č. 101/2000 Sb.

V této souvislosti kontrolující konstatoval, že jak informační povinnost správce, tak způsob zabezpečení nosičů osobních údajů plně odpovídají zákonu č. 101/2000 Sb.

O průběhu a výsledcích kontroly velvyslanectví v Káhiře lze nalézt více v části Schengenská spolupráce.

Jak již bylo uvedeno, jedním z kontrolních záměrů v oblasti čerpání prostředků při realizaci dotačních a operačních programů má být i projekt **Klidné příhraničí**. V rámci tohoto záměru se Úřad bude zaměřovat i na dodržování podmínek, které pro Českou republiku plynou ze Schengenské smlouvy v tom směru, jak odpovědné subjekty při instalaci a následném provozu preventivních zařízení a prvků dodržují povinnosti při zpracování osobních údajů sledovaných osob.

Vzhledem k tomu, že příprava projektu včetně schvalovacích procedur byla, jak je uvedeno výše, prodloužena, bylo rozhodnuto zahájení kontroly odložit na příští sledované období.

4. DALŠÍ OBLASTI KONTROL DLE KONTROLNÍHO PLÁNU

4.1. Novorozenecký screening – kontrola je realizována na základě podnětu sdružení Iuridicum Remedium:

Kontrola se zaměřila na posouzení platné právní úpravy podmínek pro shromažďování a zpracování citlivých údajů o zdravotním stavu novorozenců. V rámci výkonu dozorových činností se proto Úřad dále zaměřil na právní podmínky pro zpracování citlivých údajů novorozenců a uplatnil v průběhu připomínkového řízení k novému návrhu vyhlášky Ministerstva zdravotnictví o zdravotnické dokumentaci některé své návrhy.

Kontrola vzhledem ke své rozsáhlosti dosud nebyla ukončena.

4.2. Monitoring zaměstnanců na pracovištích:

V návaznosti na některé poznatky a dostupné informace týkající se problematiky možného sledování chování zaměstnanců na pracovištích ze strany zaměstnavatele s cílem předcházet škodlivému chování na pracovištích proběhla kontrola ve společnosti ŠKODA AUTO a.s. a společnosti Plzeňský Prazdroj, a. s.

Kontroly proběhly s následujícím výsledkem:

Kontrolujícími bylo konstatováno, že kamerové systémy se záznamovým zařízením jsou provozovány v režimu ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., neboť je to nezbytné pro ochranu práv a právem chráněných zájmů správců. Obě společnosti řádně splnily svoji informační povinnost vůči zaměstnancům i třetím osobám i oznamovací povinnost vyplývající z ustanovení § 16 zákona č. 101/2000 Sb. Kontrolou nebylo zjištěno porušení ani dalších povinností vyplývajících pro provozovatele kamerových systémů se záznamovým zařízením z citovaného zákona.

Závěrem k této části lze konstatovat, že obě kontroly splnily svůj účel. Významným způsobem přispěly k získání relevantních informací důležitých pro predikci a orientaci dozorové činnosti Úřadu v dalším období. Úřad může s uspokojením konstatovat, že tzv. velcí zaměstnavatelé disponující odpovídajícími prostředky i lidskými zdroji věnují ochraně zpracovávaných osobních údajů svých zaměstnanců adekvátní pozornost. Jsou si vědomi rizik protiprávního monitoringu

zaměstnanců na pracovišti nebo ve společných prostorách zaměstnavatele a mají zájem věc uvést do souladu s podmínkami zákona č. 101/2000 Sb.

Více o průběhu a výsledcích kontroly lze nalézt v části Poznatky inspektorů z kontrolní činnosti.

4.3. Dodržování povinností správce osobních údajů se zaměřením na náležitosti souhlasu subjektu údajů při uzavírání smlouvy dle všeobecných obchodních podmínek:

Kontrola proběhla s následujícím výsledkem:

Kontrola byla zaměřena na obchodní společnosti, jejichž činnost je regulována zvláštním zákonem. Byly kontrolovány tři subjekty. RWE Energie, s.r.o., ČEZ Prodej, s.r.o., a O2 Czech Republic a.s.

Kontrola společnosti RWE Energie, s.r.o., byla zahájena již v roce 2013 a dokončena v roce 2014. Kontrolou bylo konstatováno, že společnost RWE Energie, s.r.o., tím, že informuje zákazníky prostřednictvím uzavírané smlouvy dle Obchodních podmínek sdružených služeb dodávky plynu a v Obchodních podmínkách sdružených služeb dodávky elektřiny v neúplném a nepřesném rozsahu a neposkytuje informace o tom, zda je zpracování osobních údajů k uzavření smlouvy povinné či dobrovolné, a rovněž zákazníky nepoučuje o tom, jaké následky má odmítnutí poskytnutí osobních údajů, porušila ustanovení § 11 odst. 2 zákona č. 101/2000 Sb. tím, že neinformovala klienty při uzavírání smluv, že poskytnutí a následné zpracování osobních údajů je povinné pro uzavření smlouvy podle energetického zákona a o tom, že v případě, kdy osobní údaje nebudou poskytnuty, nesmí podle zákona smlouvu uzavřít.

Kontrolou bylo dále konstatováno, že společnost RWE Energie, s.r.o., porušila povinnost správce osobních údajů nesdružovat osobní údaje shromážděné k různým účelům, protože sdílela informace o zákaznících s dalšími společnostmi v rámci skupiny RWE v jedné databázi.

Ve společnostech ČEZ Prodej, s.r.o., a O2 Czech Republic, a.s., kontrola dosud probíhá.

Společným jmenovatelem všech zjišťovaných nedostatků z pohledu plnění zákona č. 101/2000 Sb. je nepřehlednost a formulační nejasnosti v informování subjektů údajů o právech a povinnostech při uzavírání smluv a udílení (neudílení) souhlasu se zpracováváním osobních údajů k účelům, ke kterým to zákon vyžaduje, a dále vyžadování souhlasu klientů v případech, kdy společnost má právo zpracovávat osobní údaje bez souhlasu ze zákona.

Zjištěné skutečnosti v kontrolách vedou k úvaze o potřebnosti vydání Metodického stanoviska Úřadu k této problematice.

4.4. Kontroly některých zpracování, které byly předmětem řízení podle § 17 zákona č. 101/2000 Sb.:

4.4.1. Dopravní podnik města Brna, a.s., s ohledem na specifické nastavení způsobu využívání shromážděných údajů

Kontrola proběhla s následujícím výsledkem:

Provedenou kontrolou nebylo při zpracování osobních údajů cestujících a zaměstnanců zjištěno porušení zákona č. 101/2000 Sb. Dopravní podnik města Brna přijal zásady pro ochranu osobních údajů v souvislosti s provozováním kamerového systému se záznamem v prostředcích hromadné dopravy. Bylo ověřeno fyzické zabezpečení včetně zabezpečení logování a exportu dat. Dopravní podnik města Brna splnil informační povinnost podle ustanovení § 11 a přijal potřebná opatření dle § 13 odst. 1 a 4 zákona č. 101/2000 Sb.

Více o průběhu a výsledcích kontroly lze nalézt v části Poznatky inspektorů z kontrolní činnosti.

4.5. Zpracování osobních údajů klientů správce v souvislosti s provozem sportovního centra

Kontrola proběhla s následujícím výsledkem:

Kontrola společnosti World Class Czech Republic s.r.o. se zaměřila na vedení databází klientů tohoto sportovního centra v souvislosti s nabízením služeb v oblasti sportovních aktivit a s tím souvisejících doplňkových služeb. V této souvislosti byla prověřována databáze klientů společnosti, zejména všechny souvislosti týkající se komunikace se zájemci o tuto službu a klienty centra. Kontrolující vyhodnotili zjištěné poznatky a konstatovali porušení § 11 a 16 zákona č. 101/2000 Sb.

5. KONTROLY SPLNĚNÍ ULOŽENÝCH OPATŘENÍ K NÁPRAVĚ

V rámci sledování dodržování podmínek povinných subjektů byla v roce 2014 provedena kontrola **Vězeňské služby** s cílem monitorovat, jak povinný subjekt splnil opatření, která mu byla uložena na základě výsledků předešlé kontroly, jež byla zaměřena na zpracování osobních údajů vězňených osob v souvislosti s vedením centrální evidence a prováděním identifikace vězňených osob.

Kontrola proběhla s následujícím výsledkem:

Kontrolou nebylo zjištěno porušení povinností kontrolovaného dle zákona č. 101/2000 Sb. v souvislosti s vedením evidence a identifikace vězňených osob. Kontrolující však doporučili kontrolovanému přijmout interní předpis, který sjednotí metodiku identifikace vězňených osob ve všech organizačních jednotkách kontrolovaného. Doporučení kontrolovaný akceptoval.

Více o průběhu a výsledcích kontroly lze nalézt v části Poznatky inspektorů z kontrolní činnosti.

• KONTROLY ZAHÁJENÉ NA ZÁKLADĚ PODNĚTU PŘEDSEDY ÚŘADU

1) Správa základních registrů (dále „SZR“)

Kontrola se zaměřila zejména na dodržování povinností SZR při zpracování osobních údajů v souladu se zákonem č. 101/2000 Sb. a prověření plnění povinností SZR podle § 7 odst. 5 zákona č. 111/2009 Sb., o základních registrech, podle kterého by SZR, má-li důvodnou pochybnost, že orgán veřejné moci neoprávněně přistupuje k osobním údajům, měla informovat neprodleně Úřad pro ochranu osobních údajů.

Dále kontrola měla vyhodnotit postupy SZR podle § 58 zákona č. 111/2009 Sb., kterým jsou upraveny informační povinnosti SZR při poskytování údajů z registru obyvatel a registru práv a povinností fyzické osobě – subjektu údajů, které jsou k ní vedeny v registru obyvatel a registru práv a povinností, na základě žádosti. Kontrola byla zahájena a dále probíhá.

2) Společnost „5P Agency“

Kontrola se zaměřila především na dodržování povinností správce (zpracovatele) při sběru a dalším zpracování nejen kontaktních údajů zákazníků, kteří jsou fyzickými osobami, ve vztahu k § 5 odst. 5 a následujícím zákona č. 101/2000 Sb. Současně se od výsledku kontroly očekávalo posouzení dopadu zpracování kontaktních údajů zaměstnanců společnosti a osob samostatně výdělečně činných v návaznosti na otázky, které Úřad opakovaně klade ve vztahu k soukromí zaměstnanců právnických osob a podnikajících fyzických osob a které jsou vyjádřeny i ve stanoviscích Úřadu, zejména ve stanovisku č. 3/2011 „Ochrana osobních údajů podnikajících fyzických osob“.

Výsledky kontroly:

Kontrolou bylo zjištěno, že kontrolovaný subjekt provádí zpracování osobních údajů fyzických osob, tedy i osob samostatně výdělečně činných, které pocházejí z databáze správce osobních údajů (klienta) za účelem nabízení obchodu a služeb. Kontrolou nebylo zjištěno, že by kontrolovaný zpracovával osobní údaje fyzických osob jako správce osobních údajů. Protože kontrolovaný vystupoval jako zpracovatel osobních údajů, je v této souvislosti nutné naplnění ustanovení § 6 zákona č. 101/2000 Sb., podle kterého, pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá, a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.

Výsledkem kontroly bylo zjištění, že kontrolovaný zpracovává osobní údaje na základě smluv o zpracování osobních údajů se správci osobních údajů podle § 6 zákona č. 101/2000 Sb. V písemných smlouvách byla potřebná pozornost věnována uvedení záruk zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů. Kontrolovaný jako zpracovatel osobních údajů dle § 4 písm. k) zákona č. 101/2000 Sb. nezpracovává osobní údaje fyzických osob pro klienty v rozporu s povinnostmi zpracovatele dle zákona č. 101/2000 Sb.

3) Ministerstvo zahraničních věcí

Kontrola se zaměřila na splnění podmínek ochrany osobních údajů při zpracování údajů v rámci vízového řízení na zastupitelských úřadech především v souvislosti s informováním subjektů údajů o právech vyplývajících z právních podmínek ochrany osobních údajů; a dále na ověření a zajištění ochrany osobních údajů zpracovávaných v rámci vízového informačního systému (VIS).

Dosud žádná z kontrol zpracování osobních údajů v souvislosti s vízovým řízením na zastupitelských úřadech nebyla zaměřena přímo na předávání osobních údajů žadatelů o krátkodobá víza do VIS. Proto se zaměření kontroly tentokrát soustředilo rovněž na předávání osobních údajů do VIS, jak vyplývá rovněž z doporučení expertní komise pro Schengenského hodnocení členských států na úseku ochrany osobních údajů (SchEval), z jednání Koordinační skupiny pro dohled nad VIS a nutnosti zajistit náležitou ochranu osobních údajů v souvislosti s jejich zpracováním ve VIS také na národní úrovni.

Více o průběhu a výsledcích kontroly lze nalézt v části Schengenská spolupráce.

4) Ministerstvo dopravy, případně také subjekt Česká kancelář pojistitelů

Kontrola měla mimo jiné prověřit, jakým způsobem kontrolovaný subjekt získává a dále zpracovává údaje v Centrálním registru silničních vozidel (dále jen „CRV“), jehož je provozovatelem v souladu s § 5 zákona č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích. Zaměřena byla také na to, zda a jakým způsobem dodržuje při zpracování převzatých osobních údajů povinnost zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem, a je-li to nezbytné, osobní údaje aktualizovat v souladu s § 5 odst. 1 písm. c) zákona č. 101/2000 Sb. ve vazbě na ustanovení § 8 tohoto zákona.

Výsledky kontroly:

Kontrolou bylo zjištěno, že nesprávné údaje, které v minulosti obsahoval Centrální registr silničních vozidel a na který se odvolávala Česká kancelář pojistitelů při vymáhání pojistného, byly průběžně opravovány a doplňovány pracovníky pověřených úřadů prostřednictvím nového propojení Informačního systému základních registrů (registru obyvatel, registru osob a registru územní identifikace adres a nemovitostí), osobním kontaktem s dotčenými subjekty i společností ATS-TELCOM Praha a.s., která zpracovává data „čistila“ a třídila. Současně pověřené úřady (registrační místa) vedly správní řízení o odstranění rozporů v údajích vedených v CRV. Do vyřešení jednotlivých případů byla věc vedena odděleně s vyznačením poznámky v CRV, výsledek řízení následně sdělovaly ve smyslu ustanovení § 15 odst. 11 zákona č. 168/1999 Sb., o pojištění odpovědnosti z provozu vozidla, České kanceláři pojistitelů. Kontrolovaný průběžně osobní údaje v CRV doplňoval a opravoval cestou registračních míst i veřejných registrů. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb. Současně byly v průběhu kontroly Ministerstvem dopravy realizovány i související legislativní změny, z nichž nejvýraznější je změna podmínek provedení změny zápisu držitele vozidla spojením úkonu odhlášení a přihlášení vozidla v rámci jednoho úkonu.

5) Městský soud v Praze a další vytipovaný krajský soud, který rozhoduje v souladu s § 7a

zákona č. 192/2006 Sb., insolvenční zákon, jako soud prvního stupně v insolvenčním řízení
Kontrola se zaměřila především na dodržování povinností správce (zpracovatele) při sběru a dalším zpracování osobních údajů dlužníka a jeho věřitelů za podmínek realizace insolvenčního návrhu pro zahájení a vedení insolvenčního řízení v souladu s insolvenčním zákonem.

Při prověřování podmínek pro shromažďování a zpracování osobních údajů včetně jejich zveřejnění bylo nezbytné se zaměřit na aplikaci ustanovení § 422 zákona č. 192/2006 Sb., z něhož vyplývá, že na žádost fyzické osoby, která učinila příslušné podání, může insolvenční soud rozhodnout, že některé z osobních údajů žadatele obsažené v podání nebudou v insolvenčním rejstříku veřejně přístupné. Nejde-li o fyzickou osobu, která učinila podání, zveřejní se u takové fyzické osoby v insolvenčním rejstříku jen její jméno a příjmení. V případě takového postupu insolvenční soud připojí ke vkládanému podání informaci o charakteru osobního údaje, který není zveřejňován.

Výsledky kontroly:

Kontrolou bylo zjištěno, že ne vždy je ve zveřejněných dokumentech insolvenčního rejstříku provedena anonymizace jiných osob v souladu s ustanovením § 422 odst. 2 zákona č. 192/2006 Sb. V závěrech protokolů o kontrole tak bylo konstatováno porušení zákona č. 101/2000 Sb.

Nadto lze uvést, že dle uvedeného ustanovení nastává absurdní situace, kdy soud musí ve zveřejněných dokumentech anonymizovat data, která jsou jinak zveřejněna ve veřejně přístupných registrech (živnostenský rejstřík, obchodní rejstřík), nicméně z pohledu plnění povinností správce (příslušného soudu) tak dochází k porušení zákona č. 101/2000 Sb.

Z posouzení zjištěného skutkového stavu kontrola nezjistila u kontrolovaných subjektů, že by zpracovávaly (shromažďovaly) v insolvenčním řízení osobní údaje fyzických osob nad rámec stanovený zákonem č. 192/2006 Sb.

S ohledem na právní posouzení a zjištěné skutečnosti z provedených kontrol bude problematika zveřejňování osobních údajů a jejich anonymizace v insolvenčním rejstříku pro nejednoznačnost výkladu a zjištěné problémy v praxi projednána s Ministerstvem spravedlnosti.

6) Generální ředitelství cel; při provozování identifikační databáze celních spisů (FIDE), Celního informačního systému (CIS)

Kontrola se zaměřila na implementaci pravidel týkajících se ochrany osobních údajů, zjištění a ověření zajištění ochrany osobních údajů kontrolovaným subjektem v rámci zpracování osobních údajů v CIS, konkrétně § 75, 76 a 78 zákona č. 17/2012 Sb., o celní správě České republiky, podle kterých je Generální ředitelství cel odpovědné za zpracování informací zadávaných do CIS a informací získávaných z tohoto systému; dále se kontrola zaměřila na FIDE, kterou Generální ředitelství cel provozuje na základě § 77 a 79 uvedeného zákona.

Výsledky kontroly:

Z kontrolních zjištění vyplynulo, že osobní údaje jsou v souladu se stanoveným účelem vkládány do CIS zejména proto, aby mohl kterýkoli celní orgán v rámci Evropské unie prověřit, zda v souvislosti s konkrétní osobou, dopravním prostředkem nebo zbožím neexistuje důvodné podezření z porušení celních či zemědělských předpisů Evropské unie, nebo důvodné podezření ze závažného porušení vnitrostátních předpisů. Osobní údaje do CIS/FIDE jsou vkládány pouze v nezbytném rozsahu pro naplnění stanoveného účelu a jsou zpracovávány pouze při dodržení bezpečnostních opatření na zabezpečených počítačích Celní správy České republiky. Celní správa ČR, resp. Generální ředitelství cel plní z hlediska ochrany osobních údajů povinnosti vyplývající jí z nařízení Rady č. 515/97/ES ze dne 13. března 1997 o vzájemné pomoci mezi správními orgány členských států a jejich spolupráci s Komisí k zajištění řádného používání celních a zemědělských předpisů, rozhodnutí Rady 2009/917/SVV ze dne 30. listopadu 2009 o používání informačních technologií pro celní účely, zákona č. 17/2012 Sb. a zákona č. 101/2000 Sb.

Uživatelé CIS dodržují veškerá opatření týkající se ochrany osobních údajů, včetně bezpečnostních, která jsou uvedena ve služebních předpisech Celní správy ČR.

7) Společnost Cebia, spol. s r.o.

Cílem kontroly bylo prověřit postupy kontrolovaného subjektu při shromažďování a dalším zpracování osobních údajů vlastníků a provozovatelů motorových vozidel v návaznosti na dodržování povinností správce nebo zpracovatele podle zákona č. 101/2000 Sb.

V návaznosti na shora uvedené je kontrolovaný subjekt od roku 2012 provozovatelem systému **AUTOTRACER**, který obsahuje celou historii vozidla obsahující informace nejen technického charakteru, ale také informace o vlastníku, respektive vlastnících, a dále zprostředkovává náhled do exekučního nebo insolvenčního rejstříku a databáze neplatných nebo falešných dokladů a registračních značek.

Výsledky kontroly:

Údaje o registrační značce vozidla však nejsou v systému AUTOTRACER shromažďovány a bez tohoto údaje nelze pouze na základě VIN vozidla identifikovat vlastníka či provozovatele vozidla (fyzickou osobu). Kontrolující inspektorka v závěru kontrolního protokolu konstatovala, že společnost Cebia, spol. s r.o., neshromažďuje ani nezpracovává osobní údaje v režimu zákona č. 101/2000 Sb.

8) Společnost Air Bank a.s.

Kontrola měla nejen prověřit shodu postupů kontrolovaného subjektu s podmínkami zákona č. 101/2000 Sb., ale současně by prostřednictvím kontrolních zjištění a závěrů mělo dojít k vytvoření základního přístupového rámce pro dodržování povinností odpovědných subjektů při zpracování dynamického biometrického podpisu svých klientů.

Výsledky kontroly:

Nezbytnou podmínkou každého zpracování je existence zákonem uznaného právního titulu pro zpracování údajů. Zpracování osobních údajů může v souladu s § 5 odst. 2 zákona č. 101/2000 Sb. probíhat buď na základě souhlasu subjektu údajů, nebo na základě některého z dalších právních titulů uvedených pod písm. a) až g) tohoto ustanovení. Pokud je dynamický biometrický podpis zpracováván ve stejném rozsahu, stejným způsobem a za stejným účelem jako podpis klasický, lze pro jeho shromažďování a další zpracování aplikovat především právní titul podle § 5 odst. 2 písm. b) zákona č. 101/2000 Sb., který se uplatní právě v případě zpracování nezbytného pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů.

Kontrolou nebylo zjištěno porušení ustanovení § 5 odst. 1 písm. a), b) a odst. 2 zákona č. 101/2000 Sb. Je nutné ale zdůraznit velmi tenkou hranici při používání technologie biometrického podpisu, protože jakýkoliv další krok směrem k využívání a zpracování citlivých údajů, jímž biometrický podpis je, např. při automatickém využívání biometrických informací ke kontrole podpisu klienta, by již podléhal přísnějšímu režimu pro zpracování citlivých údajů dle § 9 zákona č. 101/2000 Sb.

9) Společnost A – GIGA s.r.o.

Kontrola se zaměřila zejména na dodržování povinností správce při sběru a dalším zpracování osobních údajů zákazníků za podmínek realizace smlouvy mezi kontrolovaným subjektem

a Vězeňskou službou ČR upravující podmínky provozu civilního call centra podpory prodeje společnosti A-GIGA, které bylo zřízeno a je provozováno ve věznici Vinařice.

Výsledky kontroly:

Kontrola byla ukončena. Nebylo zjištěno porušení zákona č. 101/2000 Sb.

10) Společnost Google Czech Republic, s.r.o.

Kontrola prověřila shodu postupů kontrolovaného subjektu s podmínkami zákona č. 101/2000 Sb. s deklarovaným záměrem, sděleným Úřadu v rámci registračního řízení v dubnu 2011.

Kontrola byla realizována v návaznosti na judikát Soudního dvora Evropské unie ve věci Google v. Costeja ze dne 13. května 2014. Je zřejmé, že v souladu s článkem 4 odst. 1 písm. a) směrnice Evropského parlamentu a Rady 95/46/ES má být za odpovědný subjekt pro výše uváděné zpracování považována domovská pobočka v České republice, která zaměřuje svou činnost na veškeré fyzické osoby žijící na území státu. Podle názoru Úřadu je ve shodě s uvedeným judikátem totiž základním posláním této pobočky podpora prodeje produktů společnosti Google Inc., případně prodej reklamního prostoru nabízeného v rámci souvisejících služeb (např. služby vyhledávače).

Cílem kontroly bylo prověřit postupy kontrolovaného subjektu při přijímání žádostí dotčených fyzických osob o odstranění jejich jména z vyhledávače a způsobu ověřování identity žadatele.

Výsledky kontroly:

Kontrola byla zahájena a dosud probíhá.

11) Statutární město Plzeň

V návaznosti na podnět veřejné ochránkyně práv, který se týkal problematiky pravidel pro přidělování bytů v majetku města Plzně ve vztahu k rovnému přístupu k bydlení, se kontrola zaměřila na Nová pravidla pro nakládání s byty a nebytovými prostory a Podmínky pro výběr nájemců do uvolněných bytů v domech ve vlastnictví města Plzně.

Tato pravidla sice nelze podle veřejné ochránkyně práv primárně považovat za diskriminační, ale současně je třeba zohlednit požadavky zákona č. 101/2000 Sb.

Samostatnou otázkou, kterou měla kontrola prověřit, bylo, zda nároky na rozsah povinně předávaných a v této souvislosti zpracovávaných osobních údajů žadatele o byt – budoucího nájemce jsou – v souladu s příslušnými ustanoveními citovaného zákona.

Výsledky kontroly:

Kontrola byla provedena s cílem prověřit stav, kritizovaný veřejnou ochránkyní práv. Kontrola byla ukončena a konstatováno porušení zákona č. 101/2000 Sb., konkrétně § 5 odst. 1) písm. d) zákona č. 101/2000 Sb., a to tím, že pro zařazení žádosti uchazeče o byt do pořadníku byl od uchazeče požadován i výpis z rejstříku trestů, který si kontrolovaný ponechával. Tento postup byl změněn.

Protože kontrolovaný odstranil závadný stav ještě v průběhu kontroly, rozhodla kontrolující inspektorka postupovat v souladu s § 40a citovaného zákona. O výsledcích kontroly byla informována Kancelář veřejné ochránkyně práv.

• POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

I. KONTROLNÍ PLÁN

Zpracování osobních údajů žadatelů a příjemců finančních prostředků ze Státního fondu životního prostředí

V rámci kontrolního plánu Úřadu pro rok 2014 byl kontrolován Státní fond životního prostředí České republiky (dále „SFŽP“). Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených v Hlavě II zákona č. 101/2000 Sb. v souvislosti s plněním povinností vyplývajících z příslušných předpisů upravujících ochranu osobních údajů, zejména při zpracovávání osobních údajů subjektů údajů, kterými jsou žadatelé a příjemci finančních prostředků ze SFŽP.

SFŽP může podle ustanovení § 1a zákona č. 388/1991 Sb., o Státním fondu Životního prostředí České republiky, zpracovávat osobní údaje žadatelů o podporu vždy jen v rozsahu, který je nezbytný ke splnění daného úkolu.

Mezi tyto osobní údaje v souvislosti s poskytováním referenčních údajů ze základního registru obyvatel, údajů z agendového informačního systému evidence obyvatel a údajů z agendového informačního systému cizinců od Ministerstva vnitra nebo Policie ČR patří jméno, popřípadě jména, příjmení, rodné příjmení, datum, místo a okres narození, u subjektu údajů, který se narodil v cizině, datum, místo a stát, kde se narodil, rodné číslo, adresa místa trvalého pobytu, datum a místo úmrtí, jde-li o úmrtí subjektu údajů mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo, je-li vydáno rozhodnutí soudu o prohlášení za mrtvého, den, který je v rozhodnutí uveden jako den smrti nebo den, který subjekt údajů prohlášený za mrtvého nepřežil, a datum nabytí právní moci tohoto rozhodnutí, adresa místa pobytu, státní občanství, popřípadě více státních občanství, u cizinců druh a adresa místa pobytu, počátek pobytu, případně datum ukončení pobytu. Tímto způsobem je u SFŽP zajištěna kontrola přesnosti údajů uvedených v žádostech o podporu. Pokud by se tímto způsobem zjistily nepřesné nebo chybějící údaje žadatele o podporu, je žadatel zpravidla vyzván k doplnění nepřesných nebo chybějících údajů anebo jsou nepřesné údaje přímo v evidenci kontrolované osoby opraveny nebo chybějící údaje doplněny. Poskytování podpory v rámci jednotlivých dotačních programů se řídí příslušnými směrnicemi Ministerstva životního prostředí (dále „MŽP“). Žadatelé o podporu, resp. příjemci podpory, mj. fyzické osoby, jsou povinni k žádosti v rámci administrace žádosti o podporu a v rámci realizace projektu doložit listiny stanovené příslušnou směrnicí MŽP nebo závaznými pokyny, ze kterých vyplývá splnění podmínek dotace. Některé tyto listiny obsahující osobní údaje (ne všechny jsou vyžadovány u všech dotačních programů): výpis z bankovního účtu, stanovisko banky k poskytnutí úvěru, úvěrová smlouva nebo příslib spolufinancování (smlouva o poskytnutí dotace, půjčky či jiné formy spolufinancování), potvrzení o příjmu žadatele (průměrný měsíční příjem za poslední tři měsíce a poslední kalendářní rok, předběžný návrh na zajištění půjčky), výpis z katastru nemovitostí, dokumenty vydané stavebním úřadem, faktury za provedené práce, dodací listy, soupisy provedených prací, dokumenty k veřejné podpoře.

V případě změn údajů u stávajícího žadatele či převodu žádosti na nového žadatele se tyto skutečnosti dokládají: kopií občanského průkazu u změny trvalého pobytu a dále např. kopií oddacího listu u změny příjmení, čestným prohlášením u změny korespondenční adresy, telefonního nebo e-mailového kontaktu, kopií smlouvy o vedení bankovního účtu nebo kopií výpisu z bankovního účtu u změny bankovního účtu, ověřenou kopií úmrtního listu, pravomocného usnesení o skončení dědického řízení, přechází-li podle něho předmět podpory z programu na pozůstalého u změny žadatele z důvodu úmrtí, případně dalšími doklady, které jsou vždy striktně uvedeny v příslušné směrnici MŽP nebo závazných pokynech.

Podpora ze SFŽP je poskytována (vznik právního nároku) na základě uzavření smlouvy o poskytnutí podpory mezi SFŽP a příjemcem. Žájemcům o podporu z programů administrovaných SFŽP, kteří využili nastavený systém v oblasti stížností – tedy vyčerpali všechny řádné prostředky, a přesto mají o výsledku šetření pochybnosti, případně nejsou spokojeni s jejich vyřízením, je k dispozici samostatné oddělení ombudsmana SFŽP.

Žádosti o podporu (vyjma Národních programů) s vyplněnými osobními údaji a požadovanými kopiemi listin obsahujících osobní údaje se podávají elektronicky prostřednictvím on-line formuláře přístupného na internetových stránkách příslušného programu, např. u programu Nová zelená úsporám: <http://www.nova-zelenausporam.cz>.

U Národních programů se žádosti podávají v písemné formě do podatelny SFŽP spolu s povinnými přílohami a tyto jsou následně převáděny i do elektronické podoby. MŽP je povinno ve smyslu ustanovení § 1 odst. 11 zákona č. 388/1991 Sb. rozhodnutí ministra o použití prostředků kontrolované osoby zveřejňovat. Seznam fyzických i právnických osob, tj. příjemců dotací, o jejichž výši dotace ministr rozhodl, je tak zveřejněn i na internetových stránkách SFŽP, a to v rozsahu těchto osobních údajů: jméno, příjmení, obec, okres, kraj realizace, typ nemovitosti, výše dotace, číslo rozhodnutí ministra životního prostředí. V rámci Národních programů se v případě skupinových rozhodnutí uvádí do seznamu příjemců podpory akceptační číslo konkrétní žádosti, pod kterým je následně evidována případná smlouva o poskytnutí podpory. Do centrální evidence dotací vedené Ministerstvem financí předává SFŽP jako poskytovatel dotací osobní údaje žadatelů a příjemců podpor podle zákona č. 218/2000 Sb., o rozpočtových pravidlech [§ 3 písm. a) a § 18a]. Ministerstvo financí je povinno zveřejnit dokumenty a údaje týkající se poskytování dotací a návratných finančních výpomocí na internetových stránkách po dobu alespoň 10 let, a to bez ohledu na skutečnosti, které nastaly po jejich zveřejnění (§ 18a odst. 6 tohoto zákona).

Údaje o příjemcích jsou dále poskytovány: Generálnímu finančnímu ředitelství do systému centrální evidence dotací CEDR čtvrtletně podle ustanovení § 75b zákona č. 218/2000 Sb., v rozsahu stanoveném vyhláškou Ministerstva financí, Ministerstvu financí (pouze v případě žádostí financovaných nebo kofinancovaných přes státní rozpočet) – informační systém programového financování EDS (Evidenční dotační systém), který realizuje podmínky vyhlášky č. 560/2006 Sb. ze dne 11. prosince 2006 ve znění vyhlášky č. 11/2010 Sb. ze dne 7. ledna 2010 s účinností od 19. ledna 2010, do registru podpor de minimis (pouze v případě, že jsou naplněny definiční znaky veřejné podpory) podle zákona č. 215/2004 Sb., o úpravě některých vztahů v oblasti veřejné podpory a o změně zákona o podpoře výzkumu a vývoje a prováděcí vyhlášky č. 465/2009 Sb., o údajích zaznamenávaných do centrálního registru podpor malého rozsahu, umožňující kromě samotného zadávání informací o podporách a jejich příjemcích také prohlížet data o celkové výši poskytnutých podpor v ČR a zjišťovat celkovou výši podpory

poskytnuté konkrétnímu subjektu, resp. ověřovat výši poskytnuté finanční částky za rozhodné období, žadateli podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Na každý program existuje vlastní databáze s vlastním přístupem, z nichž jsou zveřejňovány pouze seznamy příjemců podpory, u kterých bylo vydáno rozhodnutí ministra životního prostředí, tj. přijaté a schválené žádosti o podporu v programech, které průběžně na svých stránkách SFŽP aktualizuje.

V době provádění kontroly byly na internetových stránkách SFŽP zveřejněny osobní údaje subjektů údajů v seznamech žádostí: Národní programy, u kterých bylo vydáno rozhodnutí ministra životního prostředí – rok 2012 (cca 613 osob), rok 2013 (cca 1374 osob) a rok 2014 (k datu provedené kontroly cca 1487 osob), program Zelená úsporám, u kterých bylo vydáno rozhodnutí ministra životního prostředí a došlo k výplatě podpory (viz <http://www.zelenausporam.cz/sekce/629/prehled-prijemcu-podpory/>) – celkem více než 75 000 žadatelů (není rozlišen typ žadatele fyzická/právnícká osoba), seznam žádostí pro programy Nová zelená úsporám 2013 a Nová zelená úsporám nebyly prozatím uveřejněny, Operační program Životní prostředí: schválené projekty z OPŽP jsou zveřejněny na <http://www.opzp.cz/sekce/504/prehledy-schvalenych-projektu/>, tento seznam není rozlišen na typ žadatele fyzická/právnícká osoba, dále seznamy přijatých a schválených žádostí, které kontrolovaná osoba administruje, tj. vydaných rozhodnutí ministra u schválených žádostí v již uzavřeném Operačním programu Infrastruktura, u přehledu příjemců v již ukončeném programu Zelená úsporám, u přijatých a schválených žádostí – probíhajících průběžných programů v Národních programech a u přijatých a schválených žádostí o projektech podpořených v rámci OŽP.

Seznamy žadatelů nebo příjemců podpory, včetně osobních údajů subjektů údajů SFŽP není oprávněn dále nikomu dalšímu předávat, kromě orgánů veřejné správy a orgánům činným v trestním řízení podle zvláštního zákona. V rámci trestního řízení SFŽP již poskytnul vyžádané podklady ke konkrétnímu žadateli, resp. příjemci podpory orgánům činným v trestním řízení.

K uvedené kontrole lze konstatovat, že databáze příjemců/žadatelů podpor vedená SFŽP v elektronické podobě byla řádně z hlediska zákona č. 101/2000 Sb. zabezpečena, k předání osobních údajů žadatelů a příjemců podpor jiné třetí osobě nedochází bez opory v zákoně, a pokud jde o předávání údajů do zahraničí v rámci dotací z Evropské unie, nebylo před kontrolou ani v době kontroly takovéto předávání realizováno.

Zpracování osobních údajů pacientů v elektronické podobě prostřednictvím nemocničního informačního systému

V rámci kontrolního plánu Úřadu pro rok 2013 byly kontrolovány dvě náhodně vybrané nemocnice, a to Nemocnice Rudolfa a Stefanie Benešov, a.s., a Nemocnice Tábor, a.s., (dále také „Nemocnice“), jejichž kontrola byla ukončena v roce 2014. Předmětem kontrol bylo dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb. se zaměřením na zpracování osobních údajů pacientů ve zdravotnické dokumentaci vedených v elektronické podobě prostřednictvím nemocničního informačního systému a zabezpečení zdravotnické dokumentace.

Obě Nemocnice v rámci součinnosti předložily veškeré požadované dokumenty a doklady, včetně vnitřních směrnic a smluv s externími subjekty, které poskytují Nemocnicím externí služby v rámci provozu nemocničních informačních systémů. Fyzicky bylo kontrolujícími zkontrolováno nakládání se zdravotnickou dokumentací v rámci Nemocnic a zabezpečení nemocničního

informačního systému. Pozornost byla zaměřena na dodržování § 13 zákona č. 101/2000 Sb., tj. na stanovení a plnění technicko-organizačních opatření Nemocnic, jakožto správců osobních údajů pacientů vedených ve zdravotnické dokumentaci, zejména na přidělování práv přístupu zdravotnického personálu ke zdravotnické dokumentaci vedené v elektronické formě, kontrole oprávněnosti přístupu ke zdravotnické dokumentaci a archivaci zdravotnické dokumentace.

V Nemocnici Rudolfa a Stefanie Benešov, a.s., bylo zjištěno, že pořizuje záznamy o všech případech do automatizovaných systémů Nemocnice (i dálkových) a pořizuje záznamy o prováděných změnách v automatizovaných systémech. Tyto přístupy jsou namátkově kontrolovány, jejich kontrola probíhá také v případech, že je zjištěno časté přistupování do zdravotnické dokumentace jednoho pacienta. Nemocnice zároveň zajišťuje, aby automatizované systémy Nemocnice používaly pouze oprávněné osoby. Kontrolou nebylo zjištěno porušení ustanovení § 13 odst. 4 zákona č. 101/2000 Sb. Závěrem kontrolního protokolu bylo konstatování, že Nemocnice při zpracování osobních a citlivých údajů ve zdravotnické dokumentaci vedené v elektronické podobě prostřednictvím informačních systémů Nemocnice a při jejím zabezpečení neporušila zákon č. 101/2000 Sb.

Zjištění kontrolujících v Nemocnici Tábor, a.s. bylo obdobné. Nemocnice taktéž při zpracování osobních a citlivých údajů ve zdravotnické dokumentaci vedené v elektronické podobě prostřednictvím informačních systémů Nemocnice a při jejím zabezpečení neporušila zákon č. 101/2000 Sb. Vzhledem k avizované přípravě smlouvy s externí společností, která měla nadále zajišťovat provoz informačního systému Nemocnice v oblasti digitalizace obrazové zdravotnické dokumentace, kontrolující doporučili začlenit do smlouvy ustanovení ve smyslu § 6 zákona č. 101/2000 Sb., neboť nebylo možno vyloučit, že smluvní společnost nebude v budoucnu přistupovat k osobním údajům pacientů Nemocnice vedených v elektronické formě zdravotnické dokumentace, a tím bude vůči Nemocnici v postavení zpracovatele osobních údajů pacientů.

K uvedeným kontrolám lze konstatovat, že úroveň zabezpečení zdravotnické dokumentace vedené v elektronické podobě byla na vysoké úrovni, oprávnění přístupů zdravotnických pracovníků byla rozdělena dle jejich specializace a kontrola oprávněnosti přístupů byla prováděna pravidelně. V obou Nemocnicích se na provozu informačních systémů podílelo více externích subjektů při dodržení všech povinností souvisejících se zákonem č. 101/2000 Sb. Ze zkušenosti kontrolujících se tímto potvrzuje skutečnost, že při neexistenci celostátního systému elektronického zdravotnictví jsou Nemocnice, resp. všechna zdravotnická zařízení poskytující zdravotnické služby v souladu se zákonem č. 372/2011 Sb., o zdravotních službách, nuceny, v rámci zajištění elektronizace vlastního systému, poptávat více externích dodavatelských subjektů, zajišťujících nejen dodání příslušného systému, ale i jeho provoz a servisní služby.

Vězeňská služba ČR – evidence a identifikace vězněných osob

Na základě kontrolního plánu Úřadu pro rok 2014 a rovněž několika obdržených stížností byla provedena kontrola Vězeňské služby ČR (dále také „VS“) se zaměřením na dodržování povinností správce/zpracovatele osobních údajů v souvislosti s vedením evidence vězněných osob a identifikací vězněných osob.

Kontrola byla provedena jednak na Generálním ředitelství vězeňské služby ČR (dále „GŘ VS“), které vede centrální evidenci osob ve výkonu zabezpečovací detence, ve výkonu vazby

a trestu odnětí svobody, provádí centrální správu údajů vedených v této evidenci, skartační řízení, archivaci této evidence a rovněž poskytuje oprávněným subjektům údaje z této evidence a dále ve vybraných organizačních jednotkách (vybraných věznicích). Organizačním úsekem pro vedení evidence vězněných osob, zpracování údajů, včetně poskytování a likvidace těchto údajů, jsou správní oddělení jednotlivých věznic.

Evidence vězněných osob je vedena v elektronické i listinné podobě. Elektronickou evidenci vězněných osob tvoří modul Správa vězňů vězeňského informačního systému a vybrané systémy, které slouží rovněž ke statistickému zpracování. Kontrola se v této souvislosti zaměřila také na zabezpečení údajů vedených v centrální evidenci vězněných osob a na dodržování přijatých interních předpisů. Namátkovou kontrolou bylo zjištěno, že evidenční karty vězněných osob obsahují pouze ty osobní údaje, jejichž rozsah stanoví zvláštní právní předpis, kterým je zákon č. 555/1992 Sb., o Vězeňské službě a justiční strážci České republiky.

Evidované osobní údaje zpracováváné Vězeňskou službou ČR odpovídají stanovenému účelu, k němuž jsou zpracovávány. V tomto případě se jedná o evidování a uchovávání dokladů a záznamů vzniklých v rámci právních vztahů zejména mezi orgány veřejné moci a vězněnou osobou, mezi vězněnou osobou a Vězeňskou službou ČR.

Údaje z evidence vězněných osob poskytuje VS pouze na žádost. Žádost musí být podána v listinné nebo elektronické podobě a musí být doručena v předepsaném formátu prostřednictvím poskytovatele poštovních služeb do datové schránky, na adresu elektronické podatelny anebo podána on-line přístupem do systému eLustrace. Kontrolou bylo zjištěno, že poskytování informací z této evidence je v souladu se zvláštním předpisem, kterým je zákon č. 555/1992 Sb. Žádosti o zřízení on-line přístupu musí schválit ředitel správního odboru GŘ VS. Za stanovených podmínek lze sdělit žadateli údaje z evidence také telefonicky. Telefonický dotaz lze však uplatnit výhradně za použití hesla přiděleného odborem správním GŘ VS a o žádosti se učiní záznam do vězeňského informačního systému. Všechny přístupy do vězeňského informačního systému jsou logované a pro budoucí zpětnou kontrolu musí každý, kdo nahlíží na údaje konkrétní vězněné osoby, vyplnit důvod. Dotazů doručených do datové schránky GŘ VS je cca 1000 denně, informace se podávají formou – ve které věznici jmenovaný vykonává trest odnětí svobody a odkdy dokdy. Pokud je dotaz směřován na další údaje (např. výši výdělku ve věznici), musí se žadatel obrátit přímo na konkrétní věznici. Pro pracovníky VS platí nařízení generálního ředitele VS č. 20/2005 o přístupu do informačního systému, se kterým jsou všichni příslušní zaměstnanci seznámeni.

Kontrolovaný subjekt má zřízenou Komisi na ochranu osobních údajů, jako poradní orgán generálního ředitele VS a obdobnou funkci plní i Komise na ochranu osobních údajů, zřízené jako poradní orgány ředitelů věznic – organizačních jednotek. Kontrolující si vyžádali „Zprávu o stavu a kontrolní činnosti v oblasti ochrany osobních údajů v podmínkách Vězeňské služby ČR za 1. pololetí 2014“. Ze zprávy je patrné, že Vězeňská služba ČR i její organizační jednotky plnily své úkoly v rámci prováděné kontrolní činnosti s vědomím významu a důležitosti kontrolní činnosti a odpovědnosti za správu a ochranu osobních údajů vězněných osob, stejně tak zaměstnanců a příslušníků Vězeňské služby ČR. Organizační jednotky provedly v rámci kontrolovaného období v průměru tři až čtyři kontrolní akce. Věznice Plzeň sedm, včetně mimořádné kontroly.

Kontrolující následně provedli kontroly zaměřené na evidenci vězněných osob a jejich identifikaci ve vybraných organizačních jednotkách. Jednalo se o věznici Valdice, věznici Kynšperk

nad Ohří, věznici Plzeň a věznici Světlá nad Sázavou. Ve všech kontrolovaných věznicích bylo zjištěno, že s vězněnými osobami se komunikuje pod jejich jmény. Identifikační štítek, případně průkaz vězně, vždy obsahuje jeho jméno, příjmení a fotografii. Dále je praxe a používání dalších osobních údajů při identifikaci vězňů rozdílná. Liší se dle typu věznice a dle interních předpisů jednotlivých věznic, které tuto identifikaci stanovují. Již v průběhu kontroly provedli odpovědní pracovníci těch kontrolovaných věznic, kde identifikační štítek vězně umístěný viditelně na oděvu obsahoval kromě fotografie, jména a příjmení vězně a názvu věznice další osobní údaje, zejména datum narození, případně datum ukončení výkonu trestu, úpravu rozsahu uvedených osobních údajů tak, aby viditelná strana identifikačního štítku obsahovala pouze osobní údaje v souladu s § 5 odst. 1 písm. d) zákona č. 101/2000 Sb.

Kontrolou nebylo zjištěno porušení povinností kontrolovaného dle zákona č. 101/2000 Sb. v souvislosti s vedením evidence a identifikace vězněných osob. Kontrolující však doporučili kontrolovanému vydat a přijmout interní předpis, který sjednotí metodiku identifikace vězněných osob ve všech organizačních jednotkách kontrolovaného.

Monitoring zaměstnanců

Na základě analýzy dozorové praxe Úřadu tvořila problematika monitoringu zaměstnanců na pracovišti a ve společných prostorách zaměstnavatele jedno z nosných témat kontrolního plánu Úřadu na rok 2014. Úřad vycházel z kvalifikovaného předpokladu značné latence protiprávního jednání zaměstnavatelů, mimo jiné i proto, že značný podíl na obdržených stížnostech zaměstnanců tvořily stížnosti anonymní. Svou roli zde zřejmě sehrála celospolečenská situace na trhu práce.

Současně je ovšem třeba uvést, že v řadě případů nebyl obsah stížností shledán věrohodným. Zejména u nepřijatých uchazečů o zaměstnání nebo zaměstnanců, s nimiž byl ukončen pracovní poměr, mohl být v řadě případů motivací podání stížnosti jakýsi druh pomsty s cílem způsobit společnosti v postavení správce osobních údajů nepřijemnosti, včetně zaplacení případné peněžité sankce.

V období od 9. září do 3. listopadu 2014 byla na základě kontrolního plánu Úřadu na rok 2014 provedena kontrola společnosti ŠKODA AUTO a.s. Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených v Hlavě II zákona č. 101/2000 Sb. při zpracování osobních údajů v souvislosti s monitoringem zaměstnanců na pracovišti a ve společných prostorách zaměstnavatele. Prakticky totožná kontrola, včetně předmětu kontroly byla realizována v období od 10. října do 30. listopadu 2014 u společnosti Plzeňský Prazdroj, a. s.

Kontrolní zjištění u obou kontrolovaných společností byla metodicky rozčleněna do jednotlivých oblastí, v nichž bylo možné předpokládat aktivity zaměstnavatele označitelné jako monitoring zaměstnanců na pracovišti a ve společných prostorách zaměstnavatele.

V ý b ě r o v á ř í z e n í

Realizované kontroly neprokázaly porušování interních postupů respektujících příslušná ustanovení zákoníku práce. Používané tiskopisy a formuláře obsahovaly jen osobní údaje nezbytné pro případné následné uzavření pracovněprávního vztahu, tedy jméno, příjmení, datum narození, bydliště, dosažené vzdělání a pozici, o niž se zájemce uchází. Po ukončení výběrového řízení byly osobní údaje nepřijatých uchazečů likvidovány. Nebylo zjištěno např. shromažďování nadbytečných informací včetně osobních údajů uchazečů o zaměstnání z otevřených zdrojů typu Facebook, Twitter apod. Byl učiněn závěr, že kontrolované subjekty se nedopouštěly

porušování ustanovení § 5 odst. 1 písm. d) a e) zákona č. 101/2000 Sb., tedy povinností shromažďovat osobní údaje v rozsahu odpovídajícím pouze stanovenému účelu a uchovávat osobní údaje jen po dobu nezbytnou k účelu jejich zpracování.

Personální agenda

Oba kontrolované subjekty měly zpracovaný pracovní řád obsahující mimo jiné samostatnou kapitolu upravující ochranu osobních údajů zaměstnanců. Osobní spisy zaměstnanců byly uloženy v odpovídajícím režimu (uzamykatelné kanceláře i pořadače) na útvarech péče o lidské zdroje. Přístup k nim měly jen osoby oprávněné ze zákoníku práce, tedy v zásadě nadřízení zaměstnance a personalisté. Režim nakládání s osobními spisy a dokumenty důsledně vychází z příslušných obecně závazných právních předpisů (zákon o archivnictví) i interních směrnic (Spisový řád). V této souvislosti bylo konstatováno, že oba subjekty věnovaly náležitou pozornost plnění povinností vyplývajících z ustanovení § 13 zákona č. 101/2000 Sb., tedy přijmout a dokumentovat taková opatření, aby nemohlo dojít k neoprávněnému přístupu nepovolaných osob k osobním údajům zaměstnanců a jejich zneužití.

Průkazy zaměstnance

Všichni zaměstnanci obou společností byli vybaveni multifunkční kartou. Ta obsahovala fotografii, jméno a příjmení zaměstnance a dva čipové kódy. Karta byla majetkem společností, ale její držitel odpovídala za její správné uložení, ochranu a každou ztrátu musí neprodleně nahlásit. Karta umožňuje vlastní vstup do areálu závodu, přístup na konkrétní pracoviště a do chráněných zón, slouží k odběru stravy, evidenci pracovní doby, má funkci elektronického podpisu, používá se k šifrování a logování přístupu k elektronické poště podle uvedeného rozsahu oprávnění (čtení, psaní, mazání atd.). K záznamům o pracovní době měli přístup jen oprávněné osoby, tedy nadřízení zaměstnance a pracovníci personálního a mzdového oddělení. Záznamy byly uloženy v souladu s povinností vést přehled pracovní doby zaměstnanců vyplývající zaměstnavateli z obecně závazných právních předpisů. Povinnosti držitele karty a další podrobnosti upravují interní předpisy ŠKODA AUTO a.s. i Plzeňského Prazdroje, a. s.

Docházkové systémy

Příchod zaměstnanců do všech závodů obou kontrolovaných společností, tedy v Mladé Boleslavi, Kvasinách, Vrchlabí, Plzni, Nošovicích a Velkých Popovicích i na konkrétní pracoviště, byl evidován prostřednictvím multifunkčních karet. Každý nadřízený mohl on-line sledovat, zda jeho pracovník již prošel hlavní bránou, což je důležité v okamžiku, má-li spustit výrobní linku a někdo ze zaměstnanců ještě není na pracovišti. Podle uděleného oprávnění měli držitelé karty přístup do jednotlivých chráněných zón. Každý vstup i výstup byl logován. Používaný systém byl plně funkční, žádná jiná opatření ke kontrole využívání pracovní doby nebo kontrole přítomnosti či nepřítomnosti v konkrétním prostoru, což je velmi důležité při nutnosti evakuace osob v případě havárie, požáru nebo jiné mimořádné události, není nutné přijímat.

Každý návštěvník hlavního závodu ŠKODA AUTO a.s. v Mladé Boleslavi obdrží na vrátnici vchodu pro pěší tiskopis „Poučení při vstupu do areálu Škoda Auto“. Jeho občanský průkaz je načten čtečkou (jen nezbytné osobní údaje, tedy bez fotografie, podpisu, rodného čísla, dat příbuzných). Je mu vystavena návštěvní karta, která jej opravňuje k pohybu po areálu v závislosti na pracovišti navštívené osoby, která jej zpravidla doprovází. Karta je nepřenositelná, po ukončení

návštěvy se vrací. Ztráta nebo poškození karty se musí hlásit útvaru Bezpečnost a ochrana značky. Plzeňský Prazdroj, a. s., denně navštíví řádově několik stovek našich i zahraničních turistů, kteří jsou prováděni průvodci po exkurzních trasách. Pohyb mimo tuto veřejnou část závodu, tedy po jednotlivých pracovištích, je možný jen prostřednictvím kódovaných přístupů závislých na oprávnění konkrétních zaměstnanců zakódovaných v čipu multifunkční karty.

K a m e r o v é s y s t é m y

Všechny závody společnosti ŠKODA AUTO a.s. byly vybaveny samostatnými kamerovými monitorovacími systémy se záznamovým zařízením, elektronickou zabezpečovací a požární signalizací a perimetrickou ochranou. Kamerový systém se záznamovým zařízením byl instalován v závodě Vrchlabí v roce 2005, v hlavním závodě v Mladé Boleslavi v roce 2006 a v závodě Kvasiny v roce 2007. Místním šetřením v závodě Mladá Boleslav a v závodě Kvasiny bylo ověřeno, že všechny monitorované prostory byly řádně označeny informačními tabulkami s logem kamery a doprovodným textem v českém a anglickém jazyce. Pracovní řád ŠKODA AUTO a.s. deklaruje, že při využívání těchto technických prostředků bude společnost dbát na respektování práva na ochranu osobnosti a soukromí zaměstnanců i třetích osob. Výsledky monitorování neslouží ke kontrole pracovní výkonnosti zaměstnanců, ale výlučně k ochraně majetku, prevenci a odhalování trestné činnosti. Jediným místem s centrálním přístupem do celého kamerového systému je místnost krizového řízení a je umožněno jen administrátorovi systému. Významná oprávnění mají pracovníci interní bezpečnostní služby a stálá obsluha pracoviště „Pult centrální ochrany“. Záznamy jsou předávány zásadně pracovníky útvaru Bezpečnost a ochrana značky a výlučně jen orgánům činným v trestním řízení.

Místním šetřením v závodě Plzeňského Prazdroje, a. s., v Plzni bylo zjištěno, že kamery monitorují parkoviště před objektem, vjezdy do areálu, nádvoří, vstupy do vytipovaných budov, venkovní sklady, prostory pro nakládku a vykládku zboží a venkovní perimetr celého areálu. Uvnitř budov se monitoruje automatická pokladna, stáček linky a výrobní provozy s automatickým režimem. Informační tabulky s logem kamery a kontaktními údaji správce se nacházejí na všech vjezdových branách a před vstupem do vybraných budov, ve kterých jsou instalovány kamery. Záběry všech venkovních kamer jsou přenášeny on-line na monitory „dohledového centra“ vybaveného tzv. pultem centrální ochrany. Zde bylo pouze z jednoho zařízení umožněno pořídit kopii záznamu. Dohledové centrum spravuje externí bezpečnostní agentura, která provádí ostrahu objektu Prazdroje. Přístup k záznamovému zařízení měl omezený počet osob, přístupy byly logovány.

Pro oba kontrolované provozovatele kamerových systémů je naprostou samozřejmostí, že z monitorování jsou vyloučeny všechny prostory, v nichž dochází k úkonům osobní povahy (šatny, sprchy, toalety). Obecnou zásadou je, že zaměstnanci nejsou snímáni ani v době, kdy nejsou povinni vykonávat práci (např. v průběhu přestávek) a v místech určených pro odpočinek (vyhrazené prostory pro kouření, občerstvovací automaty apod.). Společnost ŠKODA AUTO a.s. i společnost Plzeňský Prazdroj, a. s., jsou si plně vědomy přísných podmínek pro možnost nepřetržitého sledování zaměstnanců na pracovišti vyplývajících z ustanovení § 316 zákoníku práce. Do současné doby nebyla řešena žádná stížnost zaměstnance na neoprávněný nebo protiprávní monitoring na pracovišti. Každý záměr monitorovat nějaké pracoviště je předem projednán s odborovou organizací. Přípomínky jsou předmětem diskuse, a jsou-li shledány jako opodstatněné, jsou respektovány. Všechny kamerové systémy se záznamovým zařízením jsou registrovány Úřadem.

Vzhledem k uvedenému bylo kontrolujícími konstatováno, že kamerové systémy se záznamovým zařízením jsou provozovány v režimu ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., neboť je to nezbytné pro ochranu práv a právem chráněných zájmů správců. Obě společnosti řádně splnily svoji informační povinnost vůči zaměstnancům i třetím osobám i oznamovací povinnost vyplývající z ustanovení § 16 zákona č. 101/2000 Sb. Kontrolou nebylo zjištěno porušení ani dalších povinností vyplývajících pro provozovatele kamerových systémů se záznamovým zařízením z citovaného zákona.

I n t e r n í p e r i o d i k a a j i n é t i s k o v i n y

Zaměstnanci obou kontrolovaných společností poskytují souhlas se zveřejněním svých osobních údajů včetně fotografií v interních tiskovinách.

G P S v e s l u ŷ e b n í c h v o z i d l e c h

Zařízením GPS byla vybavena pouze dvě vozidla interní bezpečnostní služby v hlavním závodě v Mladé Boleslavi a po jednom vozidle bezpečnostní služby v pobočných závodech ve Vrchlabí a v Kvasinách. Vozidla byla označena a nevyjíždějí mimo areály společnosti. Cílem tohoto opatření je, aby stálá služba na pracovišti „Pult centrální ochrany“ měla neustálý přehled o místě výskytu vozidel a v případě jakéhokoliv incidentu mohla operativně kontaktovat nejbližší vozidlo. Osádky vozidel byla samozřejmě o využívání GPS informovány. U standardních manažerských a referenčních vozidel není zařízení GPS využíváno.

Služební vozidla Plzeňského Prazdroje, a. s., byla vybavena zařízením GPS disponujícím funkcí přepínání režimů „zapnuto“ – „vypnuto“ pro rozlišení soukromé a pracovní cesty. Některým zaměstnancům zejména obchodního oddělení byly služební vozy zapůjčeny i k soukromému užívání. Jednotka GPS slouží zejména k evidenci vykonaných jízd prostřednictvím elektronické knihy jízd, dále umožňuje zajistit aktivní ochranu majetku (sledování provozu vozidla a zvýšené zabezpečení proti krádeži), vytvářet elektronické platební příkazy a následně vyúčtování cestovních náhrad včetně pohonných hmot. Kontrolujícími bylo konstatováno, že k zásahům do soukromí zaměstnanců kontrolované společnosti nedochází, respektive jednoduchým úkonem závislým na svobodné vůli subjektu údajů – přepnutím tlačítka soukromé/služební cesty, docházet nemusí. Po celou dobu používání GPS ve služebních vozech Plzeňského Prazdroje, a. s., nebyla řešena ani jedna stížnost řidičů služebních vozidel na zpracování osobních údajů prostřednictvím GPS.

I n t e r n e t a e l e k t r o n i c k á p o š t a

Obsah organizační normy „Bezpečnost IT“ navazuje na Bezpečnostní politiku IT koncernu Volkswagen. Pravidla bezpečnosti slouží k ochraně důvěrnosti, integrity a dostupných informací, jakož i k zachování práv a zájmů společnosti a všech fyzických a právnických osob, které jsou se společností v obchodním styku nebo pro ni pracují. Elektronická pošta byla pravidelně prověřována na přítomnost nevyžádaných zpráv. Vytváření, odesílání a přeposílání řetězových a hromadných nevyžádaných obchodních a soukromých sdělení je zakázáno.

Zaměstnanci, kteří to potřebují k výkonu své práce, mají přístup na internet, jež je možné využívat jen pro pracovní účely. Vybrané oblasti, např. přístup na placené stránky, je blokován. Společnost disponuje kontrolními mechanismy způsobilými stupňovitě odhalit nestandardní chování i vzniklé excesy. Dá se zjistit jak doba, délka, tak i konkrétní navštívené oblasti internetu nebo

odhalit soukromé e-maily s rizikovými klíčovými slovy. Nejde ovšem o kontrolu pošty ve smyslu listovního tajemství. V minulosti bylo několik případů zneužívání přístupu na internet pracovníci nelegálně řešeno. Celá tato citlivá oblast je detailně popsána v metodickém pokynu společnosti ŠKODA AUTO a.s. – „Kontrola dat uložených v informačních systémech“. Metodický pokyn „Zaznamenávání údajů o provozu informačních systémů“ pak nařizuje, že: „Všechny informační systémy a jeho komponenty používané ve společnosti ŠKODA AUTO a.s. musí umožňovat zaznamenávání údajů o své činnosti – tzv. logování“. Minimálními údaji v logu jsou identifikátor iniciátora operace, datum a čas operace a její specifikace. Logy jsou ukládány v centrálním úložišti po dobu minimálně tří měsíců od pořízení záznamu. U systémů se zvýšenou úrovní logování, tedy s klasifikací firemních dat tajné, jsou logy uchovávány 12 měsíců.

Zaměstnanci Plzeňského Prazdroje, a. s., používající ke své činnosti PC, mohou využívat i internet, a to v přiměřené míře i k soukromým účelům. Společnost plošně blokuje internetové stránky s nevhodným obsahem. Pohyb zaměstnanců na internetu není monitorován, existuje pouze omezení přístupu pro jednotlivá pracoviště v závislosti na náplni jejich činnosti. Vedoucí zaměstnanci disponují možností dálkového přístupu k síti Plzeňského Prazdroje, a. s. Podrobnosti upravuje interní směrnice k používání IT.

Kontrolním závěrem k této oblasti bylo, že obě společnosti přísně dbají na dodržování listovního tajemství, jako práva ústavního, a jsou si vědomy přesahu případného protiprávního jednání i do práva trestního.

Systémy Data Loss Prevention

Systémů Data Loss Prevention, tzv. DLP, ve vlastním významu tohoto pojmu a rozsahu jejich možností kontrolované společnosti dosud nevyužívají. ŠKODA AUTO a.s. o tom do budoucna uvažuje, v současné době je jakási obdoba jen na úseku vývoje, kde stávající systém loguje, respektive zabraňuje neoprávněnému kopírování chráněného know-how na externí média.

Monitoring v mimopracovní době

Ve společnosti ŠKODA AUTO a.s. existují čtyři stupně klasifikace informací – veřejné, interní, důvěrné a tajné. Toto „firemní tajemství“ ovšem nelze směřovat s utajovanými informacemi ve smyslu příslušného zákona a prověřováním osob na úrovni oprávnění Národního bezpečnostního úřadu. Zaměstnanci společnosti ŠKODA AUTO a.s. proto nejsou po pracovní době žádným způsobem monitorováni, dle sdělení společnosti nikdy takováto potřeba nenastala. Totéž platí i pro zaměstnance Plzeňského Prazdroje, a. s., včetně těch, kteří disponují znalostmi pokládávanými za obchodní tajemství.

Závěrem možno konstatovat, že obě kontroly zařazené do kontrolního plánu Úřadu pro rok 2014 splnily svůj účel. Významným způsobem přispěly k získání relevantních informací důležitých pro predikci a orientaci dozorové činnosti Úřadu v dalším období. Úřad může s uspokojením konstatovat, že tzv. velcí zaměstnavatelé disponující odpovídajícími prostředky i lidskými zdroji věnují ochraně zpracovávaných osobních údajů svých zaměstnanců adekvátní pozornost. Jsou si vědomi rizik protiprávního monitoringu zaměstnanců na pracovišti nebo ve společných prostorách zaměstnavatele a mají zájem dodržovat platnou právní úpravu včetně všech ustanovení zákona č. 101/2000 Sb.

II. KONTROLY ZAHÁJENÉ NA ZÁKLADĚ PODNĚTU PŘEDSEDY ÚŘADU

Ochrana osobních údajů zpracovávaných v rámci Celního informačního systému (CIS) a v Identifikační databázi celních spisů (FIDE)

Na základě podnětu předsedy Úřadu byla provedena kontrola Celního informačního systému – Customs Information System (dále také „CIS“) a Identifikační databáze celních spisů – Customs File Identification Database (dále také „FIDE“), které v rámci České republiky spravuje Celní správa ČR, resp. jeho orgán Generální ředitelství cel (dále také „GŘC“).

Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených v Hlavě II zákona č. 101/2000 Sb. v souvislosti s plněním povinností vyplývajících z příslušných předpisů upravujících ochranu osobních údajů Celní správou České republiky jako soustavy správních orgánů a ozbrojeného bezpečnostního sboru, resp. jeho orgánu Generálního ředitelství cel, jako správce osobních údajů zpracovávaných v rámci Celního informačního systému (CIS) a v Identifikační databázi celních spisů (FIDE). Kontrola byla zaměřena především na technické a fyzické zabezpečení osobních údajů, včetně nastavení pravidel a postupů při zpracování, uchování a likvidaci osobních údajů, zajišťování ochrany práv subjektů údajů obsažených v CIS a FIDE, zabezpečení informací o přístupu k osobním údajům (logům) a opatření proti neoprávněnému zpracování osobních údajů.

V rámci mezinárodní spolupráce mezi celními správami členských zemí Evropské unie, které společně zajišťují provádění dohledu nad jednotným celním územím Evropské unie na základě společné celní legislativy, je používán společný Celní informační systém a Identifikační databáze celních spisů.

Účelem CIS je napomáhat předcházení, šetření a odhalování operací, které jsou v rozporu s celními nebo zemědělskými předpisy Evropské unie nebo jsou závažnými porušeními vnitrostátních předpisů členských států Evropské unie, a to zvýšením účinnosti spolupráce a kontroly příslušných orgánů členských států prostřednictvím rychlého šíření informací. CIS je tvořen dvěma centrálními databázemi CIS EU a CIS MS (MS = member state, členský stát), které spravuje Evropský úřad pro boj proti podvodům – European Anti-Fraud Office (OLAF). Rozdíl mezi CIS EU a CIS MS je v tom, zda jsou informace do nich vkládány podle legislativy Evropské unie nebo legislativy jednotlivých členských států Evropské unie.

CIS obsahuje rovněž zvláštní databázi s názvem Identifikační databáze celních spisů (FIDE), která je rovněž rozdělena na FIDE EU a FIDE MS. Databáze jsou vytvořeny na základě nařízení Rady (ES) č. 515/97, resp. rozhodnutí Rady 2009/917/SVV. Cílem FIDE je napomáhat předcházení operací, které jsou v rozporu s celními předpisy a se zemědělskými předpisy vztahujícími se na zboží, které vstupuje na celní území EU nebo je opouští, a usnadňovat a urychlovat jejich odhalování a stíhání. Účelem FIDE je umožnit Evropské komisi a příslušným orgánům členských států pověřených celním šetřením, pokud zahajují vyšetřování nebo vyšetřují jednu či více osob nebo podniků, aby zjistily, které příslušné orgány ostatních členských států vedou nebo vedly vyšetřování dotčených osob nebo podniků, aby tak na základě informací o existenci vyšetřovaných spisů dosáhly lépe svých cílů. Vyšetřovacím spisem je dle ustanovení § 74 odst. 3 zákona

č. 17/2012 Sb., o Celní správě České republiky, správní nebo trestní spis vedený příslušným orgánem v souvislosti s podezřením ze závažného porušení právních předpisů nebo jeho zjištěním. Databáze CIS/FIDE zahrnuje tyto osobní údaje, resp. do databáze lze zahrnout tyto osobní údaje: příjmení, rodné příjmení, křestní jména, dřívější příjmení a pseudonymy; datum a místo narození; státní příslušnost; pohlaví; číslo, místo a datum vydání dokladů totožnosti (pas, občanský průkaz, řidičský průkaz); adresu; zvláštní objektivní a trvalá tělesná znamení; důvod pro zadání údajů; navrhované opatření; výstražný kód upozorňující na předchozí zkušenosti týkající se ozbrojení, násilí nebo útěku; registrační značku dopravního prostředku.

Do databáze CIS se v žádném případě nezadávají podle čl. 4 odst. 5 rozhodnutí Rady 2009/917/SVV ze dne 30. 11. 2009, ve spojení s Rámcovým rozhodnutím Rady 2008/977/SVV ze dne 27. 11. 2008, osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém přesvědčení nebo o členství v odborových organizacích, jakož i nedochází ke zpracování údajů týkajících se zdraví nebo sexuálního života. Zpracování je přípustné pouze tehdy, je-li to nezbytně nutné a stanoví-li vnitrostátní právo odpovídající ochranná opatření. Kontrolou bylo zjištěno, že tyto osobní údaje Generální ředitelství cel nezpracovává, jelikož to není upraveno vnitrostátním právem tak, jak je přípustné dle mezinárodních předpisů.

Přístup k systémům CIS/FIDE je realizován přes webové rozhraní AFIS Portál, který je spravován OLAFem. CIS je v rámci AFIS Portálu implementován do aplikace MAB (Mutual Assistance Broker), který navíc umožňuje i bezpečnou výměnu žádostí o vzájemnou pomoc mezi členskými státy Evropské unie. Naproti tomu FIDE je podřazena pouze pod AFIS Portál. GŘC nevlastní žádnou technickou či provozní dokumentaci k CIS/FIDE, jelikož je pouze klientem/uživatelé CIS/FIDE s možností ukládání sdílených dat jako koncový uživatel a nemůže zasahovat do komunikační trasy mezi Centrem OLAF k uživatelským účtům a naopak.

Přímý přístup k záznamům v CIS, neboli k terminálům MAB/CIS, mají registrovaní uživatelé CIS, kterým bylo přiděleno uživatelské ID a heslo. Služebním předpisem GŘC jsou definovány útvary Celní správy ČR, které mohou vkládat záznamy do CIS EU a CIS MS, včetně oprávnění dotazovat se do CIS prostřednictvím registrovaných uživatelů. Přístup k CIS/FIDE za účelem ukládání nových záznamů/dotazování je umožněn pouze ze služebních počítačů schváleným uživatelům, kterým bylo přiděleno uživatelské jméno a heslo. Podmínkou pro přidělení uživatelských práv do CIS/FIDE je absolvování příslušného školení zaměřeného na CIS/FIDE. Ostatní celníci, kteří mohou naplňovat stanovený účel CIS a jsou neregistrovanými uživateli, mohou mít přístup k CIS zprostředkovaný přes registrované uživatele. K získání přístupu k datům je potřeba získat dvojí oprávnění. Každý uživatel je zařazen do skupin, které zařazují jejich členy do jednotlivých rolí v informačním systému CIS/FIDE. Do privilegovaných rolí s vyšším oprávněním má přístup jen omezený počet uživatelů.

Kromě příslušníků Celní správy ČR mají přístup k údajům v CIS, případně právo žádat o vložení požadavku na provedení stanoveného opatření i další orgány, které jsou podle vnitrostátních právních předpisů oprávněny jednat k dosažení stanoveného účelu. Pro CIS EU jsou takovými orgány Ministerstvo zemědělství, Ministerstvo životního prostředí, Státní zemědělský a intervenční fond, orgány rostlinolékařského a veterinárního dozoru, Policie ČR, státní zastupitelství a soudy. Pro CIS MS jsou takovými orgány Finančně analytický útvar Ministerstva financí, Policie ČR, státní zastupitelství a soudy. Konkrétně je přístup k údajům v CIS využíván pouze celníky Celní správy ČR. Pokud orgány uvedené v odstavci výše nemají přímý přístup

k záznamům, mohou jim údaje na základě jejich písemné žádosti poskytnout služebním postupem registrovaní uživatelé CIS.

Jako terminály MAB/CIS slouží PC standardní konfigurace používané v Celní správě ČR. Terminály MAB/CIS nesmí být připojeny k webovému rozhraní. Tisknout dokument z CIS je možné pouze na tiskárnách, které jsou umístěné ve stejné místnosti nebo v blízkosti terminálu MAB/CIS.

Za správu MAB/CIS je na centrální úrovni odpovědný OLAF, který zodpovídá zejména za klientský software a centrální databázi. Za komunikační síť CCN/CSI je odpovědné Generální ředitelství pro cla a nepřímé daně Evropské komise. Za komunikační síť v rámci Celní správy ČR, ze zřízení účtů na národní bráně CCN/CSI pro interní potřeby Celní správy ČR je odpovědné GŘC. Za lokální nastavení pracovních stanic MAB/CSI na úrovni GŘC i na úrovni celních úřadů zodpovídá, vzhledem ke specifickým datům uloženým na pracovních stanicích, GŘC.

Přesnost/správnost údajů vkládaných do CIS/FIDE je zajištěna skutečností, že k vložení údajů dochází na základě předcházejícího zjištění porušení celních předpisů, které je zadokumentováno v příslušných evidencích Celní správy ČR (např. Hlásná služba). Přesnost údajů v těchto předchozích evidencích je dána tím, že s osobou, která porušila příslušné předpisy, byl sepsán protokol, a její osobní údaje byly tudíž ověřeny. Tato skutečnost je v případě CIS potvrzena při vkládání případu do CIS. V úvodu zapisování záznamu do CIS je nutné uvést „typ zdroje“, „hodnocení zdroje“ a „hodnocení informace“. Vzhledem k této skutečnosti je u vkládaných záznamů do CIS uváděno, že „informace pochází z oficiálního zdroje“, „zdroj je hodnocen jako spolehlivý“ a „vyhodnocení informace bylo správné“.

Záznam vložený do CIS musí obsahovat údaje o době platnosti a je uchovávan pouze po dobu nezbytnou pro dosažení účelu, pro který byl do CIS vložen.

Pro účely FIDE u spisů týkajících se probíhajících vyšetřování nesmějí být záznamy uchovávány déle než tři roky, pokud není zjištěno žádné porušení předpisů, u spisů týkajících se vyšetřování, která vedla k prokázání porušení předpisů, ale dosud nevedla k odsouzení nebo k uložení peněžité sankce, nesmějí být uchovávány déle než šest let a u spisů týkajících se vyšetřování, která vedla k odsouzení nebo k uložení peněžité sankce, nesmějí být uchovávány déle než deset let. Údaje z FIDE jsou smazány automaticky, jakmile uplyne maximální doba pro jejich uchování.

Z kontrolních zjištění vyplynulo, že osobní údaje jsou v souladu se stanoveným účelem vkládány do CIS zejména proto, aby mohl kterýkoli celní orgán v rámci Evropské unie prověřit, zda v souvislosti s konkrétní osobou, dopravním prostředkem nebo zbožím existuje důvodné podezření z porušení celních či zemědělských předpisů Evropské unie, nebo důvodné podezření ze závažného porušení vnitrostátních předpisů. Osobní údaje do CIS/FIDE jsou vkládány pouze v nezbytném rozsahu pro naplnění stanoveného účelu a jsou zpracovávány pouze při dodržení bezpečnostních opatření na zabezpečených počítačích Celní správy České republiky. Celní správa ČR, resp. GŘC plní z hlediska ochrany osobních údajů povinnosti vyplývající jí z nařízení Rady (ES) č. 515/97 ze dne 13. března 1997 o vzájemné pomoci mezi správními orgány členských států a jejich spolupráci s Komisí k zajištění řádného používání celních a zemědělských předpisů, v platném znění, rozhodnutí Rady 2009/917/SVV ze dne 30. listopadu 2009 o používání informačních technologií pro celní účely, zákona č. 17/2012 Sb. a zákona č. 101/2000 Sb. Uživatelé CIS dodržují veškerá opatření týkající se ochrany osobních údajů, včetně bezpečnostních, která jsou uvedena ve služebních předpisech Celní správy ČR.

Kontrola využívání dynamického biometrického podpisu

Na základě podnětu předsedy Úřadu byla provedena kontrola společnosti Air Bank a.s. v souvislosti s užíváním dynamického biometrického podpisu a jeho užití při poskytování služeb v oblasti bankovníctví.

Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených v Hlavě II zákona č. 101/2000 Sb. společností Air Bank a.s. (dále také „Air Bank“ nebo „kontrolovaný“) v souvislosti se zpracováním osobních údajů klientů Air Bank, kteří se při podepisování smluv nebo dodatků podepisují pomocí zařízení SignPad nebo obdobného zařízení zpracovávajícího dynamický biometrický podpis.

Podle ustanovení § 5 odst. 1 písm. a) a b) zákona č. 101/2000 Sb. je správce povinen stanovit účel, prostředky a způsob zpracování, k němuž mají být osobní údaje zpracovány. Povinnost vyplývající z tohoto ustanovení je jednou ze základních zásad, která předurčuje obsah řady dalších povinností při následném zpracování osobních údajů.

Ve vnitřním dokumentu kontrolovaného *Informace o zpracování osobních údajů* se mimo jiné uvádí, že výše uvedené údaje slouží k jednoznačné identifikaci při využívání služeb Air Bank. Mezi identifikační osobní údaje je v dokumentu mimo jiné zahrnut také podpis, učiněný prostřednictvím zařízení SignPad.

Písmo a stejně tak i podpis lze považovat za jedinečný znak každého jednotlivce. Podrobnou analýzou vlastnoručního podpisu lze zpracovávat nejrůznější informace o pohybu ruky v době pořízení podpisu, jako například sklon písma, tlak ruky, rychlost psaní, velikost písma apod., z nichž pak znalec dokáže tuto osobu s větší či menší mírou pravděpodobnosti identifikovat nebo autentizovat. Tyto informace, resp. dynamické rysy odpovídají definici biometrického, a tedy i citlivého údaje ve smyslu zákona č. 101/2000 Sb. Klasický podpis zachycený na papír, a stejně tak i dynamický biometrický podpis obsahují odpovídající sumu informací (sklon písma, tlak a rychlost psaní atd.), a jsou tedy nositeli biometrických údajů.

Při posuzování další aplikace zákona č. 101/2000 Sb. je nezbytné vycházet z toho, co je o zpracování údajů výše uvedeno. Samotné pořizování a uchovávání podpisu bez jeho využití jako citlivého údaje proto nelze bez dalšího nakládání s biometrickými charakteristikami považovat za zpracování citlivých údajů. K takovému zpracování dochází až tehdy, pokud je podpis např. podroben písmoznalecké analýze za účelem ověření jeho pravosti v případě sporu.

Z písemného vyjádření kontrolovaného vyplývá, že ve chvíli, kdy je podpis sejmuto SignPadem, je vkládán přímo do PDF podoby smluvní dokumentace a není jinak v databázi uchováván. Klient i banka vidí podpis pouze v grafické podobě. Aby byla možná další analýza biometrie podpisu, je nutné vlastnit software na dešifraci a znát příslušný hash (klíč). Dle písemného vyjádření kontrolovaný v současné době dešifrovací software a hash nevlastní ani jinak nevyužívá.

Nezbytnou podmínkou každého zpracování je existence zákonem uznaného právního titulu pro zpracování údajů. Zpracování osobních údajů může v souladu s § 5 odst. 2 zákona č. 101/2000 Sb. probíhat buď na základě souhlasu subjektu údajů, nebo na základě některého z dalších právních titulů uvedených pod písm. a) až g) tohoto ustanovení. Pokud je dynamický biometrický podpis zpracováván ve stejném rozsahu, stejným způsobem a za stejným účelem jako podpis klasický, lze aplikovat především právní titul podle § 5 odst. 2 písm. b) zákona č. 101/2000 Sb., který se uplatní právě v případě zpracování nezbytného pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů.

Kontrolou nebylo zjištěno porušení ustanovení § 5 odst. 1 písm. a), b) a odst. 2 zákona č. 101/2000 Sb. Je nutné ale zdůraznit velmi tenkou hranici při používání této technologie, protože jakýkoliv další krok směrem k využívání a zpracování citlivých údajů, např. při automatickém využívání biometrických dat pro ověřování podpisu zákazníka, by již podléhal přísnějšímu režimu dle § 9 zákona č. 101/2000 Sb.

Kontrola aplikace Centrální elektronický platební rozkaz

Na základě kontrolních zjištění z incidenčních kontrol a vzhledem ke značnému objemu zpracovávaných osobních údajů při vydávání elektronických platebních rozkazů soudy byla do kontrolního plánu Úřadu pro rok 2014 zařazena kontrola zpracování osobních údajů v aplikaci Centrální elektronický platební rozkaz (dále „CEPR“). Provozovatelem aplikace CEPR, jejíž provoz byl zahájen dnem 1. ledna 2012 s konečným cílem vedení soudního spisu v elektronické podobě, a tedy správcem osobních údajů, je Ministerstvo spravedlnosti.

Kontrola tohoto subjektu byla provedena v období od 13. února do 25. června 2014. Protože správci osobních údajů jsou rovněž všichni uživatelé aplikace CEPR, tedy okresní a krajské soudy, bylo součástí kontroly i prověření postupů při vydávání elektronických platebních rozkazů u namátkou vybraného Okresního soudu v Klatovech. Předmětem kontroly bylo zejména dodržování povinností uložených správcům a zpracovatelům v § 13 zákona č. 101/2000 Sb.

Návrh na vydání elektronického platebního rozkazu obsahuje u fyzických osob osobní údaje v rozsahu: jméno, příjmení, datum narození, rodné číslo, bydliště, u žalobce navíc vyšší požadované finanční částky a bankovní údaje včetně čísla účtu. Vyžádané přehledy o vyřizování agendy elektronických platebních rozkazů uvádějí, že v roce 2013 činil nápad případů řešených v aplikaci CEPR u krajských soudů celkem 5 551 a u okresních soudů souhrnně dokonce 365 770 případů.

Kontrolou bylo zjištěno, že aplikace CEPR byla zaváděna na základě Smlouvy o údržbě a podpoře informačních systémů v resortu Ministerstva spravedlnosti uzavřené mezi Českou republikou – Ministerstvem spravedlnosti a společností CCA Group a.s. dne 16. března 2011. V článku 9 uvedené smlouvy – „Ochrana informací“ se dodavatel zavazuje k mlčenlivosti, povinnosti chránit důvěrné informace vyplývající z této smlouvy a k plnění povinností vyplývajících ze zákona č. 101/2000 Sb. Podrobnosti pracovních postupů při vydávání elektronických platebních rozkazů upravuje uživatelská příručka „Centrální elektronický platební příkaz“ ze dne 26. února 2014. Bylo ověřeno, že technické řešení přijaté společností CCA Group a.s. dlouhodobě spolupracující s resortem Ministerstva spravedlnosti (uzavřeno celkem 17 smluv o dílo k dodání požadovaného programového vybavení pro potřeby informačních systémů justice a státních zastupitelství) nevytváří podmínky k jakémukoliv neoprávněnému zpracování osobních údajů.

Pokud jde o plnění povinností vyplývajících z ustanovení § 13 zákona č. 101/2000 Sb., bylo kontrolou zjištěno, že Ministerstvo spravedlnosti má dlouhodobě přijatá a dokumentovaná technicko-organizační opatření k zajištění ochrany osobních údajů, k zabránění přístupu neoprávněných osob k prostředkům pro jejich zpracování, jakož i opatření umožňující určit a ověřit, komu byly osobní údaje předány. Uživatelé aplikace CEPR (soudy) mají zpracovány vnitřní předpisy upravující postup a odpovědnost určených osob oprávněných provádět zpracování osobních údajů uvedených v návrhu na vydání elektronického platebního rozkazu včetně přístupu do Centrální evidence obyvatel. Obsah těchto vnitřních předpisů vychází z Instrukce Ministerstva spravedlnosti č. 224/2002-OI-SP.

Každý vstup do aplikaci CEPR je logován. Příslušný formulář je obligatorně označen mj. spisovou značkou příslušného soudního spisu, do něhož je také zakládán. Je tedy kdykoliv snadno zjištělné mj. i kdo, kdy a proč prováděl prostřednictvím systému CEPR lustraci v Centrální evidenci obyvatel.

Jedním z důležitých kontrolních zjištění bylo, že nařízená a v praxi realizovaná periodická kontrolní opatření v dostatečné míře eliminují rizika neoprávněného přístupu ke zpracovávaným osobním údajům a nevytvářejí prostor k pochybení systémového charakteru.

Vzhledem k uvedenému byl učiněn závěr, že kontrolou Ministerstva spravedlnosti, jako provozovatele aplikace CEPR, ani kontrolou jednoho z náhodně vybraných uživatelů této aplikace – Okresního soudu v Klatovech nebylo zjištěno porušení zákona č. 101/2000 Sb.

Zpracování osobních údajů v insolvenčním rejstříku

Na základě obdržených stížností a podnětu předsedy Úřadu byly provedeny dvě kontroly Městského soudu (dále jen „MS“) a vytipovaného Krajského soudu (dále jen „KS“), které rozhodují v souladu § 7a zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), jako soudy prvního stupně v insolvenčním řízení. Kontroly byly zaměřeny na dodržování povinností správce při shromažďování a dalším zpracování osobních údajů dlužníka a jeho věřitelů za podmínek realizace insolvenčního návrhu pro zahájení a vedení insolvenčního řízení v souladu se zákonem č. 182/2006 Sb., zejména na aplikaci ustanovení § 422 zákona č. 182/2006 Sb., z něhož vyplývá, že na žádost fyzické osoby, která učinila příslušné podání, může insolvenční soud rozhodnout, že některé z osobních údajů této fyzické osoby, obsažené v podání, nebudou v insolvenčním rejstříku veřejně přístupné. Kontrolou MS a KS byla zjištěna porušení zákona č. 101/2000 Sb., a to v ustanovení § 5 odst. 2 a 3. Při zpracování osobních údajů (shromažďování, jejich anonymizace, zveřejnění) soudy postupují podle zvláštních právních předpisů upravujících insolvenční řízení a dále podle zákona č. 101/2000 Sb. Informace o subjektech údajů shromažďované v insolvenčním řízení jsou osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. Zpracování osobních údajů bez souhlasu subjektu údajů je nezbytné pro plnění právních povinností kontrolovaného dle zákona č. 182/2006 Sb. § 5 odst. 2 písm. a) zákona č. 101/2000 Sb.]. Insolvenční řízení včetně insolvenčního rejstříku, zpracování osobních údajů a jejich anonymizaci upravuje zákon č. 182/2006 Sb., vyhláška č. 311/2007 Sb., o jednacím řádu pro insolvenční řízení, kterou se provádějí některá ustanovení zákona č. 182/2006 Sb. a Instrukce Ministerstva spravedlnosti č. j. 505/2001-Org. – vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy.

Kontrolou bylo zjištěno, že aplikace a výklad § 422 odst. 1 zákona č. 182/2006 Sb. (anonymizace osobních údajů v souvislosti s podanou přihláškou fyzické osoby a žádostí o anonymizaci a následné zveřejnění) činí v praxi potíže, ne vždy soudy vztáhly anonymizaci na veškeré dokumenty v insolvenčním řízení, a to z důvodu nejednoznačného výkladu tohoto ustanovení zákona č. 182/2006 Sb., důsledkem je pak zveřejnění osobních údajů těchto fyzických osob v jiných částech insolvenčního rejstříku.

Ustanovení § 422 odst. 1 věta první zákona č. 182/2006 Sb. (... na žádost fyzické osoby, která učinila příslušné podání, může insolvenční soud rozhodnout, že některé z osobních údajů této fyzické osoby, obsažené v podání, nebudou v insolvenčním rejstříku veřejně přístupné. Takovou žádost lze podat kdykoliv v průběhu insolvenčního řízení. Jméno a příjmení takové fyzické osoby insolvenční soud v insolvenčním rejstříku zveřejní vždy.) umožňuje dvojí výklad ohledně

anonymizace. Lze z něho dovodit, že se anonymizují pouze osobní údaje uvedené v podání fyzické osoby, nikoliv stejné osobní údaje, které mohou být obsaženy v jiných dokumentech, obsažených (zveřejněných) v insolvenčním rejstříku. Takový výklad však činí anonymizaci zcela formální, neboť zpravidla by osobní údaje konkrétní fyzické osoby bylo možno získat z jiných zveřejněných dokumentů v insolvenčním rejstříku.

Dále pak bylo kontrolou konstatováno, že pokud jde o pohledávky věřitelů a jejich výši, jsou předmětem insolvenčního řízení v rámci řízení o dlužníkově úpadku a způsobu jeho řešení ve smyslu § 2 písm. a) zákona č. 182/2006 Sb., jejich anonymizací by byl zmařen záměr zákonodárce. Přihláška pohledávky je procesní úkon, kterým věřitel uplatňuje uspokojení svých práv v insolvenčním řízení. Náležitosti přihlášky jsou stanoveny v ustanovení § 21 vyhlášky č. 311/2007 Sb. V případě, kdy věřitel podá přihlášku, rozhoduje o případné anonymizaci údajů opět výhradně soud podle § 422 odst. 1 zákona č. 182/2006 Sb. Úřadu pak nepřísluší přezkoumávat rozhodnutí soudu o anonymizaci. V případě, kdy bylo stěžovateli namítáno zveřejnění pohledávky věřitele, která byla předmětem insolvenčního řízení (v daném případě finanční prostředky fyzické osoby na konkrétním účtu u úpadce), kontrolující přisvědčili názoru soudů, že výše pohledávky a její právní důvod s ohledem na účel insolvenčního rejstříku a práva účastníků řízení přihlášenou pohledávku věřitele popřít např. co do výše a právního důvodu, včetně účtu u dlužníka, nelze anonymizovat a nedošlo tak ke zveřejnění osobních údajů klientů v rozporu se zákonem č. 101/2000 Sb.

Kontrolou bylo zjištěno, že ne vždy je ve zveřejněných dokumentech insolvenčního rejstříku provedena anonymizace údajů jiných osob v souladu s § 422 odst. 2 zákona č. 182/2006 Sb., v závěrech protokolů o kontrole tak bylo konstatováno porušení zákona č. 101/2000 Sb.

Nadto lze uvést, že dle uvedeného ustanovení nastává absurdní situace, kdy soud musí ve zveřejněných dokumentech anonymizovat data, která jsou jinak dostupná ve veřejně přístupných registrech (živnostenský rejstřík, obchodní rejstřík...), nicméně z pohledu plnění povinností správce (příslušného soudu) tak dochází k porušení zákona č. 101/2000 Sb.

Z posouzení zjištěného skutkového stavu kontrolou nebylo u kontrolovaných subjektů konstatováno, že by zpracovávaly (shromažďovaly) v insolvenčním řízení osobní údaje fyzických osob nad rámec stanovený zákonem č. 182/2006 Sb.

S ohledem na právní posouzení a zjištěné skutečnosti z provedených kontrol bude problematika zveřejňování osobních údajů a jejich anonymizace v insolvenčním rejstříku pro nejednoznačnost výkladu a zjištěné problémy v praxi projednána s Ministerstvem spravedlnosti.

Kontrola zpracování osobních údajů vlastníků a provozovatelů motorových vozidel v systému AUTOTRACER (zpracování VIN automobilů)

Předmětem kontroly zahájené Úřadem ve společnosti Cebia, spol. s r.o., (dále jen „Společnost“) v únoru 2014 na podnět předsedy Úřadu bylo dodržování povinností správce/zpracovatele osobních údajů při zpracování osobních údajů vlastníků a provozovatelů motorových vozidel zpracovávaných v souvislosti s provozováním systému AUTOTRACER, se zaměřením na dodržování povinností dle § 5 odst. 2, § 5 odst. 4, § 11 odst. 1 a § 13 zákona č. 101/2000 Sb.

Společnost provozující systém AUTOTRACER podniká v oblasti prověřování původu a historie ojetých vozidel. Informační systém AUTOTRACER vznikl před pěti lety jako on-line informační systém, který poskytuje okamžitou pomoc každému, kdo si kupuje ojeté vozidlo.

Dle zjištění kontrolujících v průběhu kontroly, cca 90 % datové základny systému tvoří tyto údaje: VIN (Vehicle Information Number) vozidla stav tachometru a datum, kdy byl příslušný stav tachometru zapsán (tzv. trojička). Systém dále obsahuje přehledy materiálu použitého na opravy a přehledy opravárenských prací, vztahujících se k danému vozidlu. Tyto údaje jsou čerpány od značkových a neznačkových servisů (cca 750). Většina souborů obsahuje tři sloupce: VIN vozidla, stav tachometru a datum, kdy byl příslušný stav tachometru zapsán. Společnost neručí za informace obsažené v systému, cca ve 20 případech měsíčně je zjištěna v systému chyba v záznamu, takový údaj Společnost ze systému odstraňuje. Do databáze AUTOTRACER je ukládána pouze uvedená trojice údajů (tzv. trojička), údaj o zdroji dat do databáze není ukládán, nelze jej tedy zpětně zjistit. Data jsou značkovými a neznačkovými servisy poskytována na základě podepsané smlouvy mezi servisem a Společností. U značkových servisů jsou vždy před započítáním spolupráce s danou značkou dohodnuty podmínky spolupráce s importérem nebo výrobcem (Škoda – poskytuje stejný rozsah informací do elektronické servisní knížky, která je uložena v centrální databázi, majitel vozidla si může vyžádat opis v autorizovaném servisu, VW importér, Honda, Mitsubishi, Toyota – poskytují stejné informace, které jsou veřejně dostupné na jejich webovém portále).

V systému AUTOTRACER Společnost eviduje cca 120 tis. dotazů měsíčně nejen od tuzemských klientů/zákazníků, ale i klientů/zákazníků ze zahraničí, zejména ze zemí východní Evropy, kam jsou auta z České republiky vyvážena. Systému využívají nejen běžní klienti/zákazníci, ale také autobazary a subjekty státní správy (Policie ČR, finanční úřady apod.). Systém AUTOTRACER poskytuje stejné informace jak běžným klientům/zákazníkům, tak smluvním partnerům i subjektům státní správy. Systém AUTOTRACER je využíván mnoha státními úřady, které údaje ze systému používají pro svoji každodenní práci.

Systém AUTOTRACER dále využívá data pojišťoven na základě uzavřených smluv se společnostmi Global Expert, s. r. o., a UNIQUA pojišťovna, a.s. (struktura dat – VIN, kalkulace poškození vozidla, popis poškození, vyčíslená škoda); vlastní systém pro zjištění skutečného roku výroby vozidla – z VIN kódu; veřejně dostupné údaje z webových serverů výrobců vozidel, sloužících pro servisní podporu (struktura dat – technické údaje k vozu – značka, model, typ motoru a další); veřejně dostupné informace z webových serverů leasingových společností v České republice (cca 24), ve Slovenské republice prostřednictvím Asociace leasingových společností (v obou případech pouze informace ano/ne financováno). Stav se zjišťuje on-line v okamžiku dotazu do systému AUTOTRACER, informace se v systému dále neukládá. Dále server využívá veřejně dostupné údaje z webového serveru MV ČR a MV SR (VIN, odcizeno v ČR či SR ke dni dotazu), data však nejsou shromažďována v systému. Využíván je dále unikátní systém ICARIS, tj. využívány jsou údaje pro identifikaci vozidla – obecné informace, jak identifikovat vozidlo a jak ověřit důvodnost jeho identifikátorů (ražba VIN, typový štítek a další). Do systému ICARIS jsou tyto údaje shromažďovány techniky Společnosti na základě fyzické prohlídky vozidla. Pro ověření původu vozidla jsou využívána i data ze zahraničí od společnosti, která provozuje portály zaměřené na prodej autovraků, a to na základě smlouvy. Rok prodeje vozidla, uváděný ve výpisu AUTOTRACER, je odvozen z data, které autobazar předá při zaslání stavu tachometru.

Dle zjištění kontrolujících systém AUTOTRACER neobsahuje registrační značky vozidel ani osobní údaje bývalých nebo současných vlastníků či provozovatelů vozidel.

VIN je číslo/kód, který se obvykle skládá ze 17 znaků (písmena a číslice) a jeho formát je od roku 1983 určen normou ISO 3779:2009. Význam jednotlivých znaků je následující:

1. znak – kód země, kde bylo vozidlo vyrobeno
2. znak – definuje výrobce (značku) vozidla
3. znak – definuje typ vozidla nebo výrobní divizi
- 4.– 8. znak – VDS (Vehicle Descriptor Section) – výrobcem specificky zakódované vlastnosti vozidla (motor, model, série apod.)
9. znak – kontrolní číslice
10. znak – rok výroby
11. znak – kód montážního závodu
- 12.–17. znak – pořadové (výrobní) číslo vozidla, je jedinečné v rámci výrobce a montážního závodu

VIN je tedy údaj o vozidle, který je s ním neoddělitelně spojen po celý „životní“ cyklus. Jedná se o tzv. „rodné číslo“ vozidla – neměnný identifikátor, na rozdíl od registrační značky vozidla, která se vytváří a mění v souladu s mezinárodní legislativou a je vždy přidělena konkrétnímu vozidlu a konkrétnímu vlastníkovému vozidlu. Zpracování údajů o vozidle (VIN) ve spojení s registrační značkou, resp. údaji o vlastníkovému vozidlu může být za určitých okolností zpracováním osobních údajů v režimu zákona č. 101/2000 Sb. Údaje o registrační značce vozidla však nejsou v systému AUTOTRACER shromažďovány a bez tohoto údaje nelze pouze na základě VIN vozidla identifikovat vlastníka či provozovatele vozidla (fyzickou osobu). Kontrolující inspektorka v závěru kontrolního protokolu konstatovala, že společnost Cebia, spol. s r. o., neshromažďuje ani nezpracovává osobní údaje v režimu zákona č. 101/2000 Sb.

Úřad v průběhu výše uvedené kontroly obdržel podnět, který směřoval proti zveřejňování informací o vozidlech s údajně upraveným stavem tachometru na internetových stránkách www.sdruzeni-sova.cz, s tím, že se v uvedeném případě jedná o zpřístupňování informací vztahujících se ke konkrétnímu vozidlu, přičemž v některých případech jsou zároveň zveřejňovány údaje o vlastníkovému, resp. provozovateli vozidla. Úřad konstatoval, že údaje zveřejňované Sdružením na ochranu vlastníků automobilů – SOVA, o.s. (dále jen „Sdružení“) se vztahují ke konkrétním automobilům. Je skutečností, že na jejich základě, především při využití VIN kódu v internetovém vyhledávači, obvykle lze najít zdrojový inzerát, který v případě, kdy automobil prodává fyzická osoba, obsahuje i některé její kontaktní údaje (jméno, telefon či e-mailovou adresu), které tato osoba sama na internet vložila za účelem prodeje daného vozidla. Minimálně v případě automobilů prodávaných fyzickou osobou se tak jedná či může jednat o osobní údaje dle definice § 4 písm. a) zákona č. 101/2000 Sb. ve smyslu čl. 2 písm. a) a recitálu 26 směrnice Evropského parlamentu a Rady 95/46/ES. Tyto údaje jsou pak spolu s údaji o prodávajících, právnických osobách, Sdružením bez dalšího rozlišení shromažďovány, porovnávány a dále zveřejňovány. Ač cílem činnosti Sdružení zjevně není identifikovat konkrétní fyzické osoby, ale zpracovávat údaje o některých prodávaných automobilech, Sdružení si musí být vědomo, že mezi údaji, které takto zpracovává, jsou i osobní údaje o prodávajících, fyzických osobách. Proto minimálně u zveřejňování informací o automobilech, které v daný okamžik prodávají fyzické osoby, se dle zákonné definice formálně o zpracování osobních údajů jedná. Účelem činnosti Sdružení, který je jím deklarován a který byl zjištěn i předchozím šetřením ze strany Úřadu, je zveřejnění informací o prodávaných automobilech, u kterých existuje podezření z uvádění nepřesných informací o jejich technickém stavu, především o nepravdivém stavu tachometru. Takovýto účel zpracování údajů lze obecně považovat za legitimní a legální, čímž jsou i v případě, pokud bude tato činnost považována za zpracování osobních údajů, splněny podmínky,

kteře na účel zpracování klade jak česká, tak evropská legislativa. Dalším z předpokladů pro zákonnost zpracování osobních údajů je existence právního titulu, tedy právem předvídaného důvodu pro zpracování osobních údajů. V podnětu bylo uvedeno, že zjevně nedisponuje souhlasem prodávajících s dalším využitím jejich údajů. Dle Úřadu je však souhlas pouze jedním z možných právních titulů pro zpracování údajů. Tituly, které lze při činnosti Sdružení aplikovat, jsou především ty upravené § 5 odst. 2 písm. d) a e) zákona č. 101/2000 Sb. Podle prvního z nich je možné osobní údaje i bez souhlasu dotčené osoby zpracovávat tehdy, pokud se jedná o oprávněně zveřejněné osobní údaje. Druhý z uvedených titulů pak umožňuje zpracovávat údaje v situaci, kdy je takové zpracování nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby, kterou v tomto případě mohou být i potencionální kupci či zájemci o koupi daného automobilu, u něhož existuje podezření z uvádění nepravdivých technických údajů. I v případě, kdy by daná činnost Sdružení byla posouzena jako zpracování osobních údajů, jednalo by se o zpracování údajů, které lze na základě výše uvedených zákonných důvodů provádět bez souhlasu dotčených osob. V činnosti Sdružení nelze shledat ani podezření z porušení dalších povinností upravených zákonem č. 101/2000 Sb. Úřad zároveň konstatoval, že v případě, kdy se prodávající, ať už právnická či fyzická osoba, domnívá, že mu činností Sdružení byla způsobena škoda, především tím, že jím prodávaný automobil byl označen jako vozidlo s upraveným tachometrem, je nutno takto vzniklou škodu vymáhat cestou občanského práva, neboť Úřad k rozhodování takovýchto sporů není kompetentní. Jak je výše uvedeno, účel ochrany práv a právem chráněných zájmů při zveřejňování informací o prodávaných automobilech, u kterých existuje důvodné podezření z uvádění nepravdivých technických údajů, se Úřadu obecně jeví jako legitimní. S ohledem na tuto skutečnost a rovněž na zásadu ultima ratio, podle které je nutné prostředky veřejného práva, například kontrolu či správní řízení, uplatnit až tehdy, pokud nápravu nenabízejí instituty práva soukromého, ochrana práv dle občanského práva, nebude Úřad v tomto případě do posuzovaných vztahů mezi prodávajícími a dalšími subjekty vstupovat.

III. KONTROLY DLE JEDNOTLIVÝCH TEMATICKÝCH OKRUHŮ

A. Zpracování osobních údajů prostřednictvím sledovacích systémů na pracovištích, v dopravních prostředcích a bytových domech

Kamerový systém v bytovém domě

Úřad obdržel v červenci 2014 od zástupkyně společenství vlastníků domu v Kolíně (dále jen „Společenství“) podnět ke kontrole na Stavební bytové družstvo Kolín (dále jen „Družstvo“) ve věci provozování kamerového systému v bytových domech, zakládající podezření na porušení ustanovení § 5 a § 10 zákona č. 101/2000 Sb. Z podnětu vyplývalo, že dané Společenství vzniklo ze zákona v prosinci 2013 a po ustavujícím shromáždění, konaném v březnu 2014, kdy proběhla volba orgánů, převzalo i správu domu. Součástí převzetí bytových domů od Družstva byl i ka-

merový systém, od něhož Společenství údajně, přes ústní i písemné vyžádání, neobdrželo administrativní podklady umožňující jeho řádné provozování. V červnu 2013 dle Společenství předalo Družstvo nedostatečné podklady, neboť nepředalo všechny informované souhlasy dotčených subjektů osobních údajů v souvislosti s provozem kamerového systému instalovaného v bytovém domě, což se týkalo monitorování výtahových kabin. Dále byl Společenství předán údajně neplatný podpisový arch, neboť nebyl aktualizovaný. Namítaný nesoulad fakticky provozovaného kamerového systému s legislativou na žádost Společenství Družstvo neodstranilo. Z toho důvodu se Společenství domnívalo, že nemůže realizovat přeregistraci u Úřadu, a tvrdilo, že kamerový systém je nadále nelegálně provozován a spravován cizím subjektem bez souhlasu Společenství. Na základě výše uvedeného Společenství podalo podnět ke kontrole bývalého vlastníka (Družstva) v souvislosti s provozováním kamerového systému v konkrétním bytovém domě v Kolíně. V rámci úkonů před zahájením kontroly dle ustanovení § 3 zákona č. 255/2012 Sb., o kontrole (kontrolní řád), bylo kontrolujícími zjištěno, že Společenství předmětný kamerový systém od Družstva převzalo dnem ukončení smlouvy o správě domu, respektive následně po ustavující schůzi Společenství, od bývalého předsedy navíc převzalo klíče od společných prostor domu. Družstvo ke konci dubna 2013 tedy ukončilo správu předmětného domu.

Na základě zjištění kontrolující inspektorka konstatovala, že dnem převzetí správy domu se Družstvo zprostito všech povinností či závazků plynoucích z postavení správce osobních údajů k předmětnému kamerovému systému a Společenství se ujalo svých vlastnických práv i ve vztahu k provozovanému kamerovému systému, o čemž navíc svědčil i zápis z ustavující schůze Společenství. Společenství se tedy poté, co převzalo do svého vlastnictví instalovaný kamerový systém, stalo fakticky vlastníkem kamerového systému, a tedy i správcem osobních údajů dle zákona č. 101/2000 Sb. Od tohoto období se tak Společenství stalo výlučně odpovědným subjektem za jeho zákonné provozování a ve smyslu ustanovení § 5 odst. 4 zákona č. 101/2000 Sb. bylo a je povinno prokázat souhlas subjektů údajů se zpracováním osobních údajů po celou dobu zpracování. Pokud tedy stěžovatel namítal nezákonnost provozování kamerového systému, bylo jeho povinností zpracovávání osobních údajů pomocí kamerového systému v bytovém domě ukončit v momentě převzetí kamerového systému od Družstva, respektive tuto činnost neprodleně uvést do souladu se zákonem. Zákonem stanovená povinnost registrace a s tím spojené povinnosti ve smyslu ustanovení § 5 odst. 4 zákona č. 101/2000 Sb. prokázat souhlas subjektů údajů se zpracováním osobních údajů přešla na stěžovatele, který nejpozději po dni následujícím po převzetí domu od Družstva měl zhojit případné nedostatky v dokumentaci, namítanou provozovanou kameru ve výtahu odpojit a nově se registrovat u Úřadu.

Společenství byla v rámci úkonů v souladu s ustanovením § 3 zákona č. 255/2012 Sb. zaslána výzva s upozorněním na možné porušení zákona č. 101/2000 Sb. a výzva k uvedení zpracovávání osobních údajů do souladu se zákonem č. 101/2000 Sb., včetně změny registrace u Úřadu, což povede k uvedení stavu do souladu se zákonem č. 101/2000 Sb. s tím, že pokud budou požadované kroky provedeny, bude podnět odložen. Společenství byla rovněž uložena povinnost ve stanoveném termínu informovat inspektorku Úřadu. Následně stěžovatel předmětný kamerový systém u Úřadu nově registroval, o čemž podal inspektorce Úřadu informaci. Rovněž tak Družstvo požádalo o ukončení registrace. Na základě uvedeného obě zúčastněné strany zjednaly nápravu, daný stav uvedly do souladu se zákonem č. 101/2000 Sb., a proto byl podnět odložen.

Rozšíření kamerového systému v bytovém domě

Ve stížnosti, kterou Úřad obdržel v souvislosti s provozem kamerového systému v bytovém domě, stěžovatel uvedl, že se na řádné schůzi shromáždění Společenství vlastníků bytových jednotek (dále jen „SVJ“) dozvěděl, že došlo k rozšíření instalace kamerového systému u nich v domě, k instalaci třetí kamery ve společné části domu před nástupem do výtahu. Ze stížnosti vyplývalo, že kamera je umístěna tak, že snímá vstupy do bytů nebo prostory před byty v prvním a druhém nadzemním podlaží. Záznamové zařízení je umístěno v místnosti WC pro nebytový prostor papírnictví. Nebyla poskytnuta informace členům SVJ o aktivaci kamery, neexistoval souhlas potřebného počtu vlastníků, nebyla stanovena lhůta k uchování záznamu, docházelo k porušení osobnostních práv dle Ústavy a Listiny základních práv a svobod. Úřad sdělením doporučil stěžovateli využít svého práva podle § 21 zákona č. 101/2000 Sb. a požádat SVJ o vysvětlení. V následujícím podání stěžovatel uvedl, že vyzval SVJ k odstranění kamer z důvodu nezákonnosti jejich umístění, a doložil doručení výzvy SVJ. Odpověď však nedostal. Jelikož z obsahu podnětu vyplývalo možné porušení zákona č. 101/2000 Sb., byla zahájena s SVJ kontrola. Kontrolou bylo zjištěno, že souhlas s provozem kamerového systému se záznamem nedali všichni uživatelé bytů (vlastníci jednotek a nájemníci). Kamerový systém se záznamem byl tak provozován bez potřebného souhlasu všech subjektů údajů dle § 5 odst. 2 věta první zákona č. 101/2000 Sb. V této souvislosti bylo třeba důrazně upozornit na nezbytnost využití kamerového systému se záznamem výhradně ke stanovenému účelu a v rozsahu nezbytně nutném k dokumentování případného protiprávního jednání.

Způsob instalace a provoz kamerového systému se záznamem, kdy jsou monitorovány i vchody do domů či do bytů, je zásahem do práva subjektů údajů na ochranu soukromého a osobního života, a je tak vyloučeno pořizování záznamu z kamerového systému bez souhlasu obyvatel bytů podle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

SVJ provozovalo kamerový systém se záznamem umístěný ve veřejných prostorách domu v Praze po určitou dobu bez potřebného předchozího souhlasu všech subjektů údajů (vlastníků či nájemců bytů), čímž porušilo ustanovení § 5 odst. 2 věta první zákona č. 101/2000 Sb. a dále bez toho, aby subjekty údajů předem informovalo podle § 11 odst. 1 a 2 zákona č. 101/2000 Sb. a bez potřebného technicko-organizačního zabezpečení podle § 13 odst. 1 zákona č. 101/2000 Sb. a dále bez řádného splnění oznamovací povinnosti podle § 16 odst. 1 zákona č. 101/2000 Sb. V průběhu kontroly SVJ odstranilo závadný stav a instalovanými kamerami již nebyl pořizován záznam. V navazujícím správním řízení byla SVJ uložena pokuta ve výši 3 000 Kč.

Kamerový systém ve společných prostorách bytového domu provozovaný nájemcem nebytových prostor

Kontrola byla zahájena na základě stížnosti, jejímž obsahem bylo tvrzení, že podnikající fyzická osoba (dále jen „Provozovatel“) provozuje za účelem zajištění ochrany majetku zdravotnického zařízení provozovaného v nebytových prostorách, které jsou součástí bytového domu v Praze, kamerový systém, který je zároveň umístěn ve společných prostorách domu. Dle vyjádření stěžovatele neseznámil Provozovatel s provozem kamerového systému další obyvatele domu, kteří užívají společné prostory a byty v domě, a jejich monitorováním prostřednictvím kamerového systému dochází k porušování jejich osobnostních práv. Stěžovatel dále uvedl, že podává k Úřadu podnět k zahájení řízení ve smyslu § 17 zákona č. 101/2000 Sb., v jehož důsledku

dojde Úřad ke zjištění, že jsou splněny podmínky pro zrušení registrace kamerového systému provozovaného Provozovatelem.

V průběhu kontroly bylo zjištěno, že dům na uvedené adrese je ve spoluvlastnictví právnické osoby, a to hlavního města Prahy, přičemž správou části domu ve vlastnictví hlavního města Prahy je pověřena Městská část Praha 1. Provozovatel je ode dne 19. července 2013 registrován ve veřejném registru správců osobních údajů jako správce osobních údajů a v registraci uvedl, že bude zpracovávat osobní údaje prostřednictvím kamerového systému s nahráváním, a to se souhlasem subjektů údajů, přičemž bude zpracovávat osobní údaje svých zákazníků a zaměstnanců. Při místním šetření bylo zjištěno, že se klinika nachází v prvním patře prostor pronajatých Provozovatelem od spoluvlastníka domu, Městské části Praha 1. V této části se nachází operační sál s nezbytným zázemím. Ve zbývajících částech prvního patra se nachází byt třetí osoby. Ve druhém patře pronajaté části domu se pak nacházejí ordinace a hlavní recepce kliniky. Kamerový systém byl instalován za účelem zajištění bezpečnosti zaměstnanců kliniky a ochrany majetku kliniky, přičemž hodnota přístrojového vybavení kliniky je v řádu milionů korun. V době před instalací kamerového systému došlo ke dvěma vykradením sanitky, která před domem parkuje, dále ke vloupání do prostor kliniky v prvním patře, kde byly odcizeny fotografické přístroje v ceně cca 60 000 Kč, odcizení mosazných tabulek na dveřích kliniky a také byl v domě opakovaně zaznamenán pohyb nežádoucích osob. V jednom případě došlo k pokusu o ublížení na zdraví pracovnice recepce kliniky. V průběhu místního šetření byla kontrolujícími pořízena fotodokumentace rozmístění jednotlivých kamer a bylo zjištěno, že kamerový systém se skládá ze záznamového zařízení a osmi kamer, které sledují kromě vnitřních prostor kliniky prostory u hlavního vchodu do domu, také prostor přímo před hlavním vchodem do domu a monitorovány jsou také části veřejných chodeb a dveře soukromého bytu. Zjištěno bylo, že kamerovým systémem jsou monitorovány prostory, ve kterých se pohybují vlastníci bytů, rodinní příslušníci, včetně jejich návštěv. Dále bylo zjištěno, že Provozovatel i zaměstnanci kliniky mohou sledovat pouze on-line přenos na monitoru. K ovládání záznamového zařízení přístupová oprávnění nemají. Dle sdělení Provozovatele mají přístup k záznamům na záznamovém zařízení pouze zástupci společnosti, která zajišťovala servis kamerového systému. Kontrolující v době místního šetření navíc zjistili, že záznamové zařízení bylo nastaveno pouze v režimu on-line, bez záznamu, což bylo také signalizováno svítící kontrolkou „Stop“ a na monitoru kamerového systému nebyl záznam indikován. Provozovatel uvedl, že o zastavení záznamu rozhodl již dříve nezávisle na zahájení kontroly. Přibližně ve dvou případech Policie ČR žádala o umožnění náhledu na pořízené záznamy, což jí bylo umožněno, požadované informace se však z pořízených záznamů nezdařilo získat. Kopie pořízených záznamů pro potřeby Policie ČR nebyly pořízeny a také nebyly nikdy pořízeny a předány kopie záznamů pro jiné účely, ani pro potřeby orgánů činných v trestním řízení.

Provozovatel kontrolujícím při ústním jednání zároveň sdělil, že při instalaci kamerového systému bylo záznamové zařízení původně nastaveno tak, aby se záznamy prostřednictvím záznamového zařízení pořizovaly. Později zjistil, že kamerové záznamy nevyužívá, a proto požádal servisní společnost, aby záznamové zařízení vyřadila z provozu. Dle „Protokolu o kontrole funkce a nastavení“, který vystavila servisní společnost, byl kamerový systém nastaven pouze na monitorování on-line, tedy bez záznamu. Protokol byl vystavený dne 18. června 2014, tedy před datem 25. června 2014, kdy byla kontrola zahájena.

S ohledem na rozhodnutí Provozovatele ve společných prostorách bytového domu nezpracovávat osobní údaje prostřednictvím kamerového systému se záznamem je nezbytné, aby byl zajištěn postup dle § 17a zákona č. 101/2000 Sb., tedy pomine-li účel, pro který bylo zpracování zaregistrováno, Úřad z vlastního podnětu, nebo na žádost správce, rozhodne o zrušení registrace. V daném případě bylo výhradně na Provozovateli, jako správci osobních údajů, jakým způsobem bude provozovat kamerový systém, který kromě společných prostor je instalován i v prostorách, jež jsou výhradně v jeho užívání. Kontrolující při místním šetření ani v dalším průběhu kontroly nezjistili existenci kamerových záznamů. Pro posouzení toho, zda byla ustanovení zákona č. 101/2000 Sb. porušena, neměli kontrolující žádné konkrétní důkazy. Dle názoru kontrolujících Provozovatel v době kontroly neporušoval v souvislosti s provozem kamerového systému zákon č. 101/2000 Sb., a to i přes existující registraci. Samotné svědectví Provozovatele o tom, že v minulosti provozoval kamerový systém se záznamem, nestačí k tomu, aby kontrolní orgán bez dalších důkazů konstatoval porušení zákona č. 101/2000 Sb. Kopie záznamů si nepřevzala ani Policie ČR či jiný orgán činný v trestním řízení. Kontrolující inspektorka v závěru kontrolního protokolu konstatovala, že Provozovatelem nejsou prostřednictvím kamerového systému zpracovávány osobní údaje, jelikož nejsou pořizovány záznamy fyzických osob. Na základě uvedených skutečností inspektorka Úřadu celou záležitost posoudila se závěrem, že s ohledem na ustanovení § 3 zákona č. 101/2000 Sb. se v daném případě nejedná o zpracování, shromažďování ani uchování osobních údajů ve smyslu § 4 písm. e), f) a g) zákona č. 101/2000 Sb., a proto také není dána věcná příslušnost Úřadu dle § 2 odst. 2 a 3 a § 29 odst. 1 písm. a) zákona č. 101/2000 Sb. zabývat se stížností stěžovatele. Závěrem inspektorka Úřadu konstatovala, že se monitorování fyzických osob prostřednictvím kamerového systému provozovaného v režimu on-line řídí ustanovením § 81 a násl. zákona č. 89/2012 Sb., občanský zákoník.

Kamerový systém v prostředcích hromadné dopravy

Dne 19. června 2013 zaslal Dopravní podnik Města Brna (dále jen „DPMB“) Úřadu oznámení o zpracování osobních údajů cestujících. Úřad rozhodl o zahájení správního řízení vzhledem k důvodné obavě z porušení ustanovení § 5 odst. 1 písm. e), odst. 2 a § 10 zákona č. 101/2000 Sb. Po provedeném správním řízení Úřad rozhodnutím správního řízení podle ustanovení § 17 odst. 2 zákona č. 101/2000 Sb. zastavil, neboť bylo zjištěno, že účastník řízení oznámeným zpracováním neporušuje podmínky stanovené zákonem č. 101/2000 Sb. DPMB ve správním řízení doložil a zdokumentoval dříve přijatá opatření, která nevedla k nápravě a minimalizaci vzniklých škod v hromadných dopravních prostředcích a nedařilo se tak méně invazivními postupy eliminovat, nebo alespoň snížit vzniklé škody.

Úřad obzvláště pečlivě zkoumal úmysl zpracovávat osobní údaje bez souhlasu subjektů údajů, a zda takové zpracování není v rozporu s právem subjektů údajů na ochranu jejich soukromého a osobního života. Vycházel přitom především z účastníkem deklarovaných skutečností, zejména z výše uváděných škod, k jejichž minimalizaci by mělo nasazením kamerového systému dojít, a dále z opatření, které účastník řízení přijal předtím, než přistoupil k zavedení kamerového systému. Jednalo se o kombinaci personálních, technických a dalších preventivních opatření, která měla sloužit k zabránění páčání škod ve vnitřních prostorách tramvají a ochraně jak cestujících, tak řidičů tramvají. Z umístění kamer vyplývalo, že budou zaznamenávat pouze vnitřní prostor tramvají, přičemž nebude docházet k monitorování prostoru řidiče. Umístění kamerového systému se záznamem ve vozech tramvají lze považovat za adekvátní vzhledem

k deklarovanému účelu a prostředkům a opatřením, které byly před jeho zavedením použity. V případě účastníka řízení se jedná o provozování veřejné dopravy přepravující každodenně velké množství cestujících, kde se prostor k navazování mezilidských vztahů a pro projevy osobní povahy značně minimalizuje, a je snahou účastníka řízení tímto způsobem přispět k celkovému veřejnému pořádku a bezpečnosti ve městě. Minimalizace zásahů do práv dotčených subjektů vyplývá též z doby, po kterou budou záznamy uchovávány, neboť ta neumožňuje významný zásah do soukromí, spočívající ve sledování pravidelných zvyklostí subjektů údajů. Správní orgán přihlédl ke skutečnosti, že účastník řízení klade velký důraz na plnění povinností dle § 13 zákona č. 101/2000 Sb. V maximální míře minimalizoval přístup k záznamům z kamerového systému, přičemž jeho jedinými příjemci budou orgány činné v trestním řízení a každý export dat bude podroben řádnému přezkumu jeho nezbytnosti. Účastník řízení stanovil celý soubor organizačních, technických, personálních a administrativních opatření k zajištění bezpečnosti osobních údajů a rovněž stanovil způsob kontroly dodržování těchto opatření a proces vyhodnocování efektivnosti nasazení kamerového systému.

Ve správním řízení bylo zaregistrováno zpracování osobních údajů cestujících prostředky městské hromadné dopravy prostřednictvím kamerového systému se záznamem ve 29 tramvajích Škoda 13 T.

K prošetření skutečností uvedených DPMB v oznámení o zpracování (změně zpracování) osobních údajů cestujících a zjištěných Odborem správních činností Úřadu v rámci správního řízení podle § 17 zákona č. 101/2000 Sb. a plnění povinností správce byla kontrola DPMB zařazena do kontrolního plánu Úřadu pro rok 2014. Kontrola byla zahájena dne 15. ledna 2014.

Instalovaný a provozovaný kamerový systém byl DPMB zvažován zejména v souvislosti se značnými finančními náklady na odstranění škod způsobených na dopravních prostředcích MHD, tedy z naléhavé potřeby ochránit zejména značné majetkové hodnoty správce. Dalším souvisejícím opatřením byla i možnost dokumentace násilné trestné činnosti páchané na cestujících, případně na zaměstnancích kontrolovaného, výrazné preventivní působení na potenciální pachatele trestné činnosti a vandalismu, neboť budou k dispozici objektivní a veřejné informace o tom, že při spáchání trestného činu budou dopadeni a bude po nich vymáhána náhrada škody.

Provedenou kontrolou nebylo při zpracování osobních údajů cestujících a zaměstnanců zjištěno porušení zákona č. 101/2000 Sb. DPMB přijal zásady pro ochranu osobních údajů v souvislosti s provozováním kamerového systému se záznamem v prostředcích hromadné dopravy. Bylo ověřeno fyzické zabezpečení včetně logování a exportu dat. DPMB splnil informační povinnost podle ustanovení § 11 a přijal potřebná opatření dle § 13 odst. 1 a 4 zákona č. 101/2000 Sb. Pořízení kamerového záznamu podle ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., tj. bez souhlasu subjektů údajů, je výjimečně možné jen v případě, že je monitorován majetek kontrolovaného, jsou chráněny oprávněné zájmy subjektů údajů – cestujících, zaměstnanců (ochrana jejich majetku, zdraví) a dosud provedená opatření nebyla postačující. V daném případě s ohledem na monitorování provozu ve veřejném dopravním prostředku, výši způsobené škody na dopravních prostředcích, potřebě zajištění bezpečnosti a ochrany majetku cestujících a bezpečnosti pracovníků DPMB bylo konstatováno, že uvedené zpracování osobních údajů není v rozporu s ustanovením § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Doba uchování záznamu neumožňuje pravidelné sledování subjektů údajů, kteří jsou o rozsahu monitorování informováni. Opatřeními dle § 13 zákona č. 101/2000 Sb., včetně minimalizace přístupu k záznamům, je zabezpečeno zpracování osobních údajů ke stanovenému účelu bez

zásahu do soukromí, které by nebylo adekvátní tomuto účelu. Kontrolou nebylo zjištěno, že by shromažďování osobních údajů bylo v rozporu s ustanovením § 316 odst. 2 zákoníku práce. Provoz kamerového systému pak odpovídá skutečností zjištěným v rámci řízení o registraci a v navazujícím řízení podle § 17 zákona č. 101/2000 Sb.

Vzhledem k zavedenému provozu kamerového systému DPMB v hromadném dopravním prostředku bude Úřad pravidelně vyhodnocovat jeho nezbytnost a přiměřenost, a proto byla vyžádána hodnotící zpráva za první pololetí 2014 jako podklad pro posouzení, zda nadále trvají podmínky pro provoz kamerového systému se záznamem. DPMB tak zaslal Úřadu vyhodnocení efektivnosti pořizování záznamů z kamerových systémů v tramvajích za první pololetí roku 2014.

B. Zpracování citlivých údajů při poskytování zdravotnických služeb

Ztráta zdravotnické dokumentace pacientky v Lužické nemocnici

Inspektorka Úřadu provedla v termínu od září 2012 do března 2013 kontrolu, jejímž předmětem bylo dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb. se zaměřením na zpracování osobních údajů pacientů zdravotnického zařízení Lužické nemocnice a polikliniky, a. s. (dále jen „Nemocnice“) a s tím související kontrolu zabezpečení zdravotnické dokumentace dle ustanovení § 13 zákona č. 101/2000 Sb.

Stížnost zaslala Úřadu pacientka Nemocnice (dále jen „Stěžovatelka“), která poukázala na údajnou ztrátu její zdravotnické dokumentace (dále jen „ZD“), což doložila dokumenty vypracovanými příslušným orgánem České lékařské komory (dále jen „ČLK“) v Děčíně, k němuž ve věci posouzení poskytnutí péče podala v červnu 2009 stížnost. ČLK v něm konstatovala nemožnost dohledání její ZD, čímž zároveň zdůvodnila nezahájení disciplinárního řízení ve věci neposkytnutí správné péče při jejich hospitalizacích v roce 2009.

Z poznatků získaných v průběhu kontroly na základě vyžádaných dokladů a dokumentů byl zjištěn skutkový stav a následně provedeno právní hodnocení jak ve věci nakládání se ZD Stěžovatelky, tak posouzení současného stavu, především z pohledu dodržování povinností Nemocnice, jako správce osobních údajů vedených ve ZD, vyplývajících z § 13 odst. 1 zákona č. 101/2000 Sb. Zjištěno bylo, že část ZD Stěžovatelky vedenou v listinné podobě Nemocnice ztratila, což i sama Nemocnice přiznala, a ZD vedená v elektronické podobě je neúplná. Nemocnice v době, kdy došlo ke ztrátě ZD Stěžovatelky, neměla přijata opatření, aby nedošlo ke ztrátě ZD, čímž porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. Zároveň Nemocnice porušila ustanovení § 13 odst. 2 zákona č. 101/2000 Sb., neboť v době, kdy došlo ke ztrátě části ZD Stěžovatelky, neměla zpracována a dokumentována přijatá technicko-organizační opatření k zajištění ochrany osobních údajů.

Při posuzování současného stavu bylo taktéž zjištěno, že přijatá opatření jsou stále nedostatečná. Dostatečně nebyly zabezpečeny příruční spisovna a centrální spisovna, pro případy manipulace se ZD nebyly vnitřními předpisy nastaveny takové postupy, aby při nich ke ztrátě ZD nemohlo dojít, čímž Nemocnice porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. Nemocnice navíc nepožadovala elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu bylo na osobní údaje ve ZD vedené v elektronické podobě nahlíženo, a tím porušila ustanovení § 13 odst. 4 písm. c) zákona č. 101/2000 Sb., tedy Nemocnice není schopna průběžně zajišťovat namátkovou kontrolu oprávněnosti přístupů do NIS.

Stěžovatelka za účelem posouzení jí poskytnuté zdravotní péče na gynekologicko–porodnickém oddělení Nemocnice, kdy dle jejího tvrzení nebylo při hospitalizaci rozpoznáno ohrožení plodu a následně porodila mrtvý plod, podala stížnost na ČLK. Okresní sdružení ČLK v Děčíně ve věci stížnosti provedlo opakované šetření, jehož výsledkem bylo rozhodnutí Revizní komise o nezahájení disciplinárního řízení, ve kterém kromě jiného konstatuje, že „i když v předložených částech ZD nelze nalézt žádné důkazy toho, že by postup lékařů byl chybný, a k nitroděložním úmrtím plodů dochází ve značné části případů nečekaně a bez jasného vysvětlení, bez dostupnosti kompletní dokumentace nelze odpovědně a objektivně ve věci rozhodnout. Revizní komise požádala i krajského perinatologa o posouzení případu, ale ten bez dokumentace posudek vypracovat odmítl.“ Dále Revizní komise ČLK v Děčíně uvedla, že „v dané věci vydává nové rozhodnutí o nezahájení disciplinárního řízení z důvodu, že vinu žádného obviněného lékaře se nepodařilo prokázat.“

Stěžovatelka až v roce 2012 podala na Policii ČR trestní oznámení ve věci ztráty její ZD a zanedbání péče Nemocnicí. Úřadu bylo v této věci Policií ČR sděleno, že trestní věc podezření ze spáchání trestného činu ublížení na zdraví podle § 224 odst. 1 trestního zákoníku, kterého se měl dopustit podezřelý neznámý pachatel, se odkládá, neboť na základě provedeného šetření nebylo zjištěno, že by došlo ke spáchání trestného činu, kterého by se dopustila určitá osoba. Z usnesení Policie ČR však zároveň vyplynulo, že Policie ČR přibrala k vypracování znaleckého posudku odborníka – znalce z oboru gynekologie a porodnictví, který konstatoval, že „na řádně podanou žádost obdržel od Nemocnice pouze nekompletní ZD s tím, že mělo dojít k její ztrátě, její absence mu nedává seriózní možnosti zodpovědět kladené otázky, není schopen se jednoznačně vyjádřit a posoudit okolnosti, které k úmrtí plodu vedly.“ Zároveň však znalec dále konstatoval: „Velice závažná je v tomto případě informace, že stačí při neúspěšném závěru zdravotní činnosti ztratit dokumentaci a tím navodit situaci – nejsou důkazy, není možné vznést obvinění!“ Znalec dále uvedl, že se obává se, že ztráta ZD by se mohla stát „národním sportem“.

Úřad se s názorem uvedeného znalce ztotožnil a vyslovil obavu, aby se podobné případy neopakovaly, a z toho důvodu ještě více zaměřil svou kontrolní činnost na nakládání se ZD ve zdravotnických zařízeních s důrazem na plnění povinností dle § 13 zákona č. 101/2000 Sb.

Následně byla v roce 2014 v rámci správního řízení Lužické nemocnici s poliklinikou, a. s., uložena pokuta ve výši 120 000 Kč.

Úřad současně nemohl nechat bez povšimnutí jednání ČLK, která nejenže neoznámila ztrátu části ZD příslušnému orgánu, tedy Úřadu, ale svojí liknavostí zavinila i promlčení správního deliktu spočívajícího ve ztrátě části konkrétní ZD, tedy zamezení potrestání Nemocnice, jako správce osobních údajů, který porušil své povinnosti. Z toho důvodu v rámci kontrolního plánu Úřadu pro rok 2013 provedl Úřad kontrolu zpracování osobních údajů v ČLK v rámci stížnostní agendy na výkon povolání lékařů.

Obsah údajů v lékařském posudku

Úřad obdržel stížnost směřující proti lékařce, která byla dle sdělení stěžovatele požádána referentkou Úřadu práce ČR o posouzení jeho zdravotního stavu. Lékařka dle jeho sdělení vypracovala a předala lékařský posudek o jeho zdravotním stavu v souvislosti s jeho žádostí o pracovní rehabilitaci na Úřad práce ČR. Stěžovatel měl možnost se s obsahem posudku následně seznámit a domníval se, že rozsah informací o jeho zdravotním stavu ve zdravotním posudku neodpovídá standardům běžného lékařského posudku. Lékařka dle něj poskytla bez jeho

souhlasu údaje o jeho zdravotním stavu a o zdravotním stavu jeho nejbližších rodinných příslušníků třetí osobě, tj. referentu Úřadu práce ČR, čímž se dle jeho názoru dopustila nejen velmi hrubého porušení lékařské etiky, ale zároveň jednala protiprávně.

Dle zjištění inspektorky Úřadu při vypracování lékařského posudku provedla lékařka vyšetření a při vydání tohoto posudku postupovala v souladu s ustanovením § 9 odst. 1 zákona č. 453/2004 Sb., o zaměstnanosti, zákona č. 373/2011 Sb., o specifických zdravotních službách, a zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Stěžovatel se však domáhal kontroly obsahu a rozsahu posudku o jeho zdravotním stavu. Inspektorka Úřadu v uvedené věci odkázala na stanovisko Ministerstva zdravotnictví, které Úřad obdržel v jiné kontrolované věci a jenž se týkalo obsahu zápisu ve ZD. V uvedené věci Úřad požádal Ministerstvo zdravotnictví o zodpovězení otázky, který dozorový orgán je oprávněn provádět dozorovou činnost v uvedené oblasti.

Ministerstvo zdravotnictví zaslalo Úřadu své stanovisko k otázce určení správního orgánu k doзору nad vedením ZD a kromě jiného Úřadu sdělilo, že zákon č. 372/2011 Sb. neoznačuje jeden jediný správní orgán povolany k tomu, aby dozoroval pouze vedení ZD, a tudíž jím není ani Úřad pro ochranu osobních údajů.

Na základě výše uvedeného stanoviska inspektorka Úřadu konstatovala, že Úřad nemá kompetenci posuzovat obsah a rozsah posudku o zdravotním stavu, který vydala lékařka na žádost Úřadu práce ČR, neboť Úřad nemá pravomoc k provádění kontrolní činnosti v oblasti zpracování osobních údajů z hlediska oprávněnosti a úplnosti zápisů v návaznosti na poskytování zdravotní péče. Z tohoto důvodu byla stížnost odložena.

Zpracování osobních údajů klientů zdravotní pojišťovny v rámci jejich přeregistrace

Inspektorka Úřadu provedla v termínu od srpna 2013 do února 2014 kontrolu Vojenské zdravotní pojišťovny České republiky (dále jen „VoZP ČR“), jejímž předmětem bylo dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb. se zaměřením na zpracování osobních údajů pojištěnců VoZP ČR v souvislosti s jejich registrací. Kontrola byla provedena na základě stížností celkem 22 subjektů údajů, jejichž meritem byla skutečnost, že osobní údaje stěžovatelů byly bez jejich souhlasu v první polovině roku 2012 využity k neoprávněné registraci k VoZP ČR.

Z kontroly vyplynulo, že došlo k neoprávněnému registrování subjektů údajů k VoZP ČR bez jejich vědomí, a to v důsledku zprostředkovatelské činnosti probíhající na základě smlouvy o nevýhradním obchodním zastoupení, kterou VoZP ČR uzavřela s fyzickou osobou podnikající dle živnostenského zákona nezapsanou v obchodním rejstříku. Uvedená fyzická osoba vykonávala smluvní činnost prostřednictvím cca 200 „náborářů“. Ze zjištění kontrolujících vyplynulo, že k sepsání Přihlášek pojištěnců a Evidenčních listů zdravotní pojišťovny nedošlo za přítomnosti dotčených osob (stěžovatelů). Kontrolující inspektorka konstatovala, že VoZP ČR neměla dostatečně nastaveny mechanismy při přeregistraci pojištěnců prostřednictvím obchodních zástupců tak, aby odhalila, že došlo k předložení „fiktivních“ Přihlášek pojištěnců a Evidenčních listů zdravotní pojišťovny a zajistila tak, jako správce osobních údajů klientů (pojištěnců) a potencialních klientů, jejich shromažďování a zpracovávání v souladu se zákonem č. 101/2000 Sb. S ohledem na smlouvu s fyzickou osobou, jejímž cílem bylo zajištění nových klientů (pojištěnců), měla VoZP ČR již při uzavírání smlouvy nastavit interní pravidla pro ověřování údajů uvedených na Přihláškách pojištěnců a Evidenčních listech zdravotní pojišťovny pře-

dávaných obchodním zástupcem spolu se jmenným seznamem osob podávajících Přihlášku pojištění, potažmo žádost o přeregistraci, a to ještě před provedením samotné registrace.

Povinnost registrovat pojištění ve smyslu zákona č. 48/1997 Sb., o veřejném zdravotním pojištění, kontrolující inspektorka tímto nezpochybnila, avšak konstatovala, že platí povinnost správce osobních údajů, tedy VoZP ČR, vyplývající z ustanovení § 5 odst. 1 písm. c) zákona č. 101/2000 Sb., tj. zpracovávat přesné osobní údaje. VoZP ČR tím, že prokazatelně na základě „fiktivních“ Přihlášek pojištěnců a Evidenčních listů zdravotní pojišťovny, které jí byly předloženy obchodním zástupcem, zpracovávala nepřesné osobní údaje osob, porušila jako správce osobních údajů klientů ustanovení výše uvedeného § 5 odst. 1 písm. c) zákona č. 101/2000 Sb.

VoZP ČR se nepřesvědčila o tom, že přijatá technicko-organizační opatření obchodního zástupce, jako zpracovatele osobních údajů, odpovídají požadavkům na ochranu osobních údajů definovaných v § 13 zákona č. 101/2000 Sb.

Shodné prohlášení smluvních stran, že ve smyslu zákona č. 101/2000 Sb. má VoZP ČR pro účely plnění předmětu této smlouvy postavení správce a obchodní zástupce postavení zpracovatele a že smluvní strany jsou si vědomy závazků vyplývajících z této smlouvy a nezbytného režimu ochrany osobních údajů, nebylo dle kontrolující inspektorky možné považovat za naplnění smyslu zákonem stanovené povinnosti, tedy skutečnosti, aby se správce osobních údajů přesvědčil o tom, že jeho zpracovatel bude zpracovávat osobní údaje tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. VoZP ČR porušila tímto svým jednáním povinnost stanovenou v § 6 zákona č. 101/2000 Sb. VoZP ČR byla následně v rámci správního řízení za porušení povinnosti stanovené v § 5 odst. 1 písm. c) zákona č. 101/2000 Sb. uložena pokuta ve výši 70 000 Kč.

C. OSOBNÍ ÚDAJE ZPRACOVÁVANÉ V DLUŽNICKÝCH REGISTRECH

Osobní údaje zpracovávané na www.dluzis.cz a v dlužnických registrech SOLUS

1.

V roce 2014 provedl inspektor Úřadu na základě více stížností od občanů kontroly nebankovních dlužnických registrů. Jednalo se zejména o problematiku zpracovávání, zpřístupňování a zveřejňování osobních údajů ve spojitosti s informacemi o neplnění povinností klientů a o jejich údajném dluhu vůči různým společnostem. Související kontroly probíhaly u společností, které poskytují nebankovní úvěrové služby, leasingových společností a telefonních operátorů, kteří vkládají informace o neplnění závazků svých klientů do příslušných dlužnických registrů. Rovněž byly provedeny kontroly dvou provozovatelů dlužnických registrů. Celkem bylo provedeno sedm souvisejících kontrol.

Společným jmenovatelem téměř všech zjištění bylo konstatování absence právního titulu zpracování osobních údajů v registrech dlužníků, jeho výsledkem bylo porušení povinnosti stanovené § 5 odst. 2 zákona č. 101/2000 Sb., tedy povinnost zpracovávat osobní údaje pouze se souhlasem subjektu údajů, neboť ke zpracování osobních údajů v registrech dlužníků nelze aplikovat žádnou z výjimek uvedených zákonem.

Jedním z kontrolovaných subjektů byla fyzická osoba podnikající podle živnostenského zákona, která provozuje na webových stránkách www.dluzis.cz dlužnický registr, v němž zveřejňuje

jména a adresy údajných dlužníků a zpřístupňuje osobní údaje neomezenému okruhu osob. Kontrolovaný provozuje internetovou aplikaci „Dlužíš.cz“, jejímž cílem je umožnit věřitelům za úplaty zveřejnění inzerátu na webových stránkách, a to za účelem vyhledání dalších věřitelů pro podání případného insolvenčního návrhu proti konkrétnímu dlužníkovi. Dalším zájmem věřitelů na zveřejnění identifikace dlužníka a informace o jeho závazku je současně i nátlak na dlužníka, aby uhradil svůj dluh. Projekt „Dlužíš.cz“ je určen všem věřitelům, kteří evidují nezaplacené faktury po splatnosti. Registrace věřitele dle všeobecných obchodních podmínek je po splnění základních podmínek umožněna zdarma s možností oznámit dlužníkovi zápis do registru dlužníků. Právním titulem ke zpracování osobních údajů byl kontrolovaným stanoven výslovný souhlas dlužníka s tímto zveřejněním. Za odstranění záznamu je vždy dlužníkovi účtována platba ve výši 2–6 % z uvedené dlužné částky. Internetové stránky projektu „Dlužíš.cz“ jsou provozovány za účelem podnikání kontrolovaného.

Kontrolou bylo zjištěno, že jsou zpřístupňovány informace o údajném dlužníkovi v rozsahu jméno, příjmení, identifikační číslo, adresa (ulice, číslo popisné, obec a poštovní směrovací číslo), dále identifikace věřitele v rozsahu název, sídlo, resp. místo podnikání, identifikační číslo, bankovní účet, variabilní symbol, popis pohledávky (např. faktura za odebrané služby – připojení k internetu), dále číslo faktury, počet dnů po splatnosti, výše dlužné částky a výše penále. Seznamy dlužníků obsahují současně informace o jménu/názvu věřitele. Je-li věřitelem fyzická osoba podnikající, jsou v seznamu dlužníků zveřejněny osobní údaje v rozsahu jméno, příjmení, identifikační číslo, sídlo, resp. místo podnikání. V rámci kontroly bylo prokázáno, že kontrolovaný nedisponuje souhlasem ani jednoho subjektu údajů, tedy zpřístupňoval jejich osobní údaje na www.dluzis.cz bez právního titulu v rozporu se zákonem č. 101/2000 Sb. Na základě kontrolního zjištění byla kontrolovanému uložena příslušná opatření k nápravě a v návazném správním řízení mu byla za spáchání správního deliktu uložena pokuta ve výši 19 000 Kč.

2.

Dalším kontrolovaným subjektem, u něhož byla provedena opakovaná kontrola, bylo Zájmové sdružení právníků osob SOLUS (dále jen „sdružení SOLUS“), které vede tzv. negativní registr dlužníků. Jednalo se o mnohočetné stížnosti stěžovatelů, kteří se bránili proti tomu, že jsou vedeni, dle svého přesvědčení neoprávněně, v negativním registru fyzických osob. Součástí předmětu kontroly byla skutečnost, že sdružení SOLUS stále nerespektuje pravomocná rozhodnutí Úřadu vydaná na základě dřívějších zjištění a odmítá změnit své postupy při zpracování osobních údajů klientů svých členských společností.

Ilustrací problematiky, kterou se inspektor Úřadu zabýval v případech kontrol zpracování osobních údajů v negativním registru sdružení SOLUS, je kontrola, která byla ukončena kontrolním protokolem, z něhož vyplývá, že kontrolovaný zpracovával v případě stěžovatele J. R. v negativním registru sdružení SOLUS osobní údaje v rozsahu jméno, příjmení, rodné číslo, úplná adresa bydliště, výši dlužné částky po splatnosti, datum vzniku prodlení, datum registrace v informačním systému, datum zaplacení dlužné částky, datum poslední změny a jméno věřitele. Tyto údaje byly zpracovávány na základě souhlasu J. R., který udělil v souvislosti s uzavřením smlouvy o osobní půjčce u společnosti Raiffeisenbank a. s. Vzhledem k tomu, že se dostal do prodlení se splacením poskytnutého úvěru, byly jeho osobní údaje předány ke dni 3. července 2009 kontrolovanému. Prodlení J. R. trvalo do 26. října 2009, kdy svůj dluh splatil (k vymazání údaje mělo na základě podmínek sdružení SOLUS dojít po třech letech, tj. k 26. říjnu 2012). Dne

16. listopadu 2011 zaslal J. R. bance (Raiffeisenbank a. s.) výpověď souhlasu s nakládáním s osobními údaji, včetně vyjádření nesouhlasu se zpracováním svých osobních údajů v negativním registru sdružení SOLUS. Jeho žádosti nebylo bankou vyhověno.

Další stěžovatel (R. L.) dne 20. února 2012 prostřednictvím elektronické pošty vyjádřil svůj nesouhlas se zpracováním osobních údajů v negativním registru SOLUS a požádal, aby jeho jméno, rodné číslo, datum narození a adresa byly vymazány. Uvedené osobní údaje kontrolovaný zpracovával na základě smlouvy mezi R. L. a společností Home Credit a.s. Pohledávky z této smlouvy nebyly v té době uhrazeny. Za kontrolovaného odpověděla stěžovateli Společnost pro informační databáze, a.s., která uvedla, že zdrojem informací o klientech jsou jednotliví členové sdružení SOLUS a informace zpracovávají s výslovným souhlasem dotčené osoby pouze oprávnění členové sdružení; dále uvedla, že bylo zjištěno od společnosti Home Credit a.s., že jeho osobní údaje byly do registru fyzických osob zařazeny v souladu s Pravidly pro vytváření, správu a využívání databáze spotřebitelů neplnících své povinnosti vztahující se k činnosti řádných členů sdružení, a to na podkladě prokazatelného souhlasu se zpracováním osobních údajů v případě porušení smluvního vztahu a za splnění kritérií pro zařazení. R. L. se se stejnou žádostí obrátil dne 20. února 2012 na společnost Home Credit a. s., která mu sdělila, že eviduje záznam o neuhrazené pohledávce, a dále sdělila, že jeho osobní údaje jsou zpracovávány v souladu a za podmínek uděleného souhlasu, včetně podmínek pro jeho odvolání. Jelikož nedošlo k úhradě závazku, je odvolání souhlasu se zpracováním osobních údajů neúčinné. Uvedená evidence je taktéž v souladu se zákonnou povinností společnosti o odpovědném úvěrování.

Tato zjištění kontrolující inspektor posoudil tak, že kontrolovaný nepochybně zpracovává osobní údaje J. R. a R. L. ve smyslu § 4 písm. a) a e) zákona č. 101/2000 Sb. Tyto údaje jsou shromažďovány v negativním registru sdružení SOLUS, přičemž kontrolovaný rozhodl o účelu a prostředcích zpracování, provádí zpracování a odpovídá za něj, a je proto správcem osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb.

J. R. i R. L. udělili při uzavření příslušných smluv s Raiffeisenbank a.s., resp. Home Credit a.s. souhlas se zpracováním osobních údajů, mimo jiné za účelem předání informace o porušení smluvní povinnosti včetně rozsahu a povahy tohoto porušení, kontrolovanému. Předání osobních údajů kontrolovanému tedy bylo učiněno na základě platného právního titulu, kterým byl souhlas ve smyslu § 5 odst. 2 zákona č. 101/2000 Sb.

Kontrolou bylo také zjištěno, že v registru dlužníků sdružení SOLUS byly ve dvou dalších konkrétních případech zpracovávány osobní údaje osob, které nikdy neuzavřely žádnou smlouvu s žádnou členskou společností sdružení SOLUS, neboť vinou právě členské společnosti byly shromážděny nepřesné osobní údaje (v jednom případě se jednalo o krádež identity, ve druhém případě se jednalo o nesprávně uzavřenou smlouvu na základě nesprávné identifikace klienta), přičemž i v těchto případech sdružení SOLUS odmítlo likvidovat osobní údaje těchto osob. Oba stěžovatelé se o tom, že jsou zapsáni v registru dlužníků sdružení SOLUS, dozvěděli v okamžiku, kdy jim byly zamítnuty jejich žádosti o hypoteční úvěr z důvodu, že jsou evidováni jako dlužníci.

V dalším případě sdružení SOLUS zpracovávalo osobní údaje subjektu údajů, který uzavřel smlouvu v době, kdy smluvní společnost nebyla členem sdružení SOLUS, resp. dluh vznikl v době, kdy společnost nebyla členem sdružení SOLUS. Jednalo se o dluh ve výši 139 Kč, který vznikl členské společnosti v roce 2004.

Ve dvou případech byla odmítnuta žádost stěžovatelů o likvidaci zápisu v registru sdružení SOLUS, přestože se jednalo o osoby, které pouze žádaly o uzavření smlouvy nebankovní, přičemž

ani jedna z členských společností s nimi žádnou smlouvu neuzavřela. V tomto případě si sdružení SOLUS přivlastnilo rozhodovací pravomoc, která se vztahuje k bankovnímu registru.

V jednom z případů bylo zjištěno, že sdružení SOLUS odmítlo likvidovat osobní údaje i po lhůtě, kterou samo stanovilo jako dobu uchovávání, tedy po třech letech, kdy stěžovatel plně uhradil svůj dluh.

Odvoláním souhlasu se zpracováním osobních údajů, který J. R. předal kontrolovanému, resp. jeho neakceptováním kontrolovaným, nastal stav, kdy kontrolovaný zpracovával tyto osobní údaje v rozporu s § 5 odst. 2 zákona č. 101/2000 Sb. Současně tím dle kontrolujícího inspektora porušil kontrolovaný povinnost vyplývající z § 10 zákona č. 101/2000 Sb., protože svým jednáním nezajistil ochranu subjektů údajů před neoprávněným zasahováním do jejich soukromého a osobního života.

Inspektor Úřadu konstatoval, že zpracování osobních údajů za účelem informování členů kontrolovaného o porušení smluvní povinnosti je zpracováním, které nelze podřadit ani pod jednu z výjimek uvedených v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb.; tato povinnost nevyplývá z žádného právního předpisu, není nezbytná pro naplnění smlouvy, jejíž smluvní stranou je subjekt údajů a kontrolovaný, a dokonce ani pro naplnění smlouvy mezi subjektem údajů a členem kontrolovaného.

Inspektor Úřadu dále uvedl, že souhlas je podle § 4 písm. n) zákona č. 101/2000 Sb. svobodný a vědomý projev vůle, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů; jedná se tedy o jednostranný právní úkon, a ne smlouvu mezi správcem a subjektem údajů. Souhlas se zpracováním osobních údajů tedy není nezbytný pro uzavření příslušné smlouvy se společnostmi poskytujícími úvěrové produkty a služby a je poskytován nad rámec vlastního smluvního závazku. Je tedy pouze na rozhodnutí subjektu údajů, zda svůj souhlas udělí či neudělí, a současně také, kdy a zda svůj souhlas odvolá. Takové odvolání souhlasu je správce povinen respektovat a má za následek dle § 5 odst. 2 zákona č. 101/2000 Sb. nejen ukončení zpracování osobních údajů, ale také podle § 20 odst. 1 tohoto zákona povinnost osobní údaje zlikvidovat.

Podle právního názoru Úřadu lze osobní údaje klientů – fyzických osob zpracovávat pro účely vzájemného informování věřitelských subjektů pouze s jejich souhlasem. Zpracování (tj. zejména zařazování či aktualizace) informací v nebankovních registrech je v případě klientů – fyzických osob podmíněno poskytnutím souhlasu se zpracováním údajů. Zákon č. 101/2000 Sb. lidem umožňuje, aby svůj předchozí souhlas se zpracováním osobních údajů kdykoliv odvolali. Pokud zákonodárce neupravil zvláštním zákonem činnost provozovatelů nebankovních registrů dlužníků (na rozdíl od bankovního registru), musí se dlužnické registry řídit obecnou právní úpravou, tedy zákonem č. 101/2000 Sb.

S tímto právním názorem sdružení SOLUS nesouhlasí a podalo dne 12. února 2013 žalobu proti rozhodnutí Úřadu u Městského soudu v Praze, kterou napadlo rozhodnutí Úřadu.

V rámci kontroly bylo zjištěno, že sdružení SOLUS jako celek, tedy kancelář sdružení i zpracovatelská společnost Společnost pro informační databáze, a. s., a jednotlivé členské společnosti sdružení, nemají jednotnou metodiku a řízení k vyřizování žádostí podávaných subjekty údajů v rámci přístupu subjektu údajů k informacím a při vyřizování žádostí v rámci ochrany práv subjektů údajů a likvidaci osobních údajů. Absence pravidel má za následek nesystematické a rozdílné rozhodování jak sdružení SOLUS, tak jednotlivých členských společností při vyřizování zcela shodných žádostí klientů.

Kontrolou bylo zjištěno, že sdružení SOLUS, resp. členské společnosti sdružení SOLUS, v rámci svých všeobecných obchodních podmínek získávají souhlas se zpracováním osobních údajů v registrech sdružení SOLUS, ale podávají rozdílné informace o právu na odvolání souhlasu nebo o době zpracování v registrech sdružení SOLUS. V posledním čtvrtletí roku 2014 zahájil Úřad řešení řady dalších stížností na neoprávněné zpracování osobních údajů sdružením SOLUS.

K dané problematice je nezbytné doplnit, že Úřad při aplikaci zákona č. 101/2000 Sb. nemá zájem chránit ty osoby, které neplní své povinnosti dlužníka vůči věřitelské společnosti, tedy chránit osoby, které neplní své povinnosti, ale chránit osoby, jejichž osobní údaje jsou zpracovány bez zákonného právního titulu, čímž dochází k zásahu do jejich soukromého a osobního života.

D. POSKYTOVATELÉ ENERGETICKÝCH SLUŽEB A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ KLIENTŮ

Dodržování povinností správce osobních údajů se zaměřením na náležitosti souhlasu subjektů údajů při uzavírání smlouvy za využití všeobecných obchodních podmínek

Kontrola byla zaměřena na obchodní společnosti, jejichž činnost je regulována zvláštním zákonem. Byly kontrolovány tři subjekty: RWE Energie, s.r.o., ČEZ Prodej, s.r.o., a O2 Czech Republic a.s.

Kontrola společnosti RWE energie, s.r.o., byla zahájena již v roce 2013 a dokončena v roce 2014. Kontrolou bylo konstatováno, že společnost RWE Energie, s.r.o., tím, že informuje zákazníky prostřednictvím uzavírané smlouvy dle Obchodních podmínek sdružených služeb dodávky plynu a v Obchodních podmínkách sdružených služeb dodávky elektřiny v neúplném a nepřesném rozsahu a neposkytuje informace o tom, zda je zpracování osobních údajů k uzavření smlouvy povinné či dobrovolné, a rovněž zákazníky nepoučuje o tom, jaké následky má odmítnutí poskytnutí osobních údajů, bylo inspektorem Úřadu konstatováno, že společnost RWE Energie, s.r.o., porušila ustanovení § 11 odst. 2 zákona č. 101/2000 Sb.

Ve společnostech ČEZ Prodej, s.r.o., a O2 Czech Republic a.s. kontrola dosud probíhá.

Společným jmenovatelem všech zjišťovaných nedostatků z pohledu plnění zákona č. 101/2000 Sb. je nepřehlednost a formulační nejasnosti v informování subjektů údajů o právech a povinnostech při uzavírání smluv a udílení (neudílení) souhlasu se zpracováváním osobních údajů k účelům, ke kterým to zákon vyžaduje, a dále vyžadování souhlasu klientů v případech, kdy společnost má právo zpracovávat osobní údaje bez souhlasu ze zákona.

E. SAMOSTATNÉ PŘÍSPĚVKY

Kontrola společnosti www.scio.cz, s.r.o.

V polovině roku 2014 proběhla kontrola společnosti www.scio.cz, s.r.o. (dále také „Kontrolovaná“), která byla zahájena na základě stížnosti. Stěžovatelka uváděla, že v únoru 2014 podala přihlášku na jednu z vysokých škol (dále jen „Univerzita“). V březnu stěžovatelka obdržela e-mailem nabídku externího testování odeslanou Kontrolovanou s tím, že je oslovena na základě databáze uchazečů, poskytnuté Kontrolované Univerzitou, na kterou podala přihlášku, a to bez jejího souhlasu.

Inspektor Úřadu zahájil ve společnosti kontrolu, jejímž předmětem bylo dodržování povinností správce/zpracovatele osobních údajů stanovených v Hlavě II zákona č. 101/2000 Sb. a zákona č. 480/2004 Sb., o některých službách informační společnosti v souvislosti se zpracováním osobních údajů uchazečů o studium na vysokých školách.

Na základě Smlouvy o dílo, uzavřené dle ustanovení § 536 a násl. zákona č. 513/1991 Sb., obchodní zákoník (dále jen „smlouva o dílo“) s Univerzitou se Kontrolovaná jako zhotovitel zavázala k vytvoření strukturovaných databází výsledků Národních srovnávacích zkoušek – Obecné studijní předpoklady (dále jen „NSZ-OSP“) těch účastníků, kteří se přihlásili k přijímacímu řízení do bakalářského studia v oborech zohledňujících výsledky NSZ-OSP a k vytvoření databáze výsledků Národních srovnávacích zkoušek – Přijímací test pro navazující magisterské studium.

Podle obsahu smlouvy o dílo se Univerzita zavázala, že zhotoviteli předá seznam uchazečů, kteří jsou evidováni jako uchazeči, kteří si podali e-přihlášku do bakalářských a navazujících magisterských oborů pro akademický rok 2014/2015 a uhradili poplatek za podanou přihlášku.

Jako právní povinnost v kontextu podmínek zpracování osobních údajů lze označit právem očekávané nebo vynucované chování odpovědného subjektu, přičemž za takovou právní povinnost lze označit konkrétní ustanovení zvláštního zákona, ze kterého zákonné zmocnění vyplývá, tudíž zpracování dat zákon výslovně ukládá, anebo správci takovou povinnost stanoví.

Podle § 50 zákona č. 111/1998 Sb., o vysokých školách, se přijímací řízení zahajuje doručením přihlášky ke studiu na vysoké škole nebo její součástí, která uskutečňuje příslušný studijní program. V přihlášce uchazeč vždy uvede jméno, popřípadě jména, příjmení, rodné číslo, bylo-li přiděleno, a adresu místa trvalého pobytu na území České republiky, popřípadě bydliště mimo území České republiky.

Byť zákon č. 111/1998 Sb. zpracování osobních údajů uchazečů o studium předpokládá, stanoví tak výslovně jen pro subjekty uvedené v § 2 téhož zákona. Nelze tedy a priori dovozovat, že ke zpracování osobních údajů uchazečů o studium je oprávněn kterýkoliv soukromoprávní nebo veřejnoprávní subjekt, nevyplývá-li oprávnění (zmocnění) z jiného zvláštního zákona, smlouvy o zpracování nebo ze souhlasu uděleného subjektem údajů. Z dokumentů zaslaných Kontrolovanou a z přihlášky stěžovatelky ke studiu bylo zřejmé, že správce (Univerzita) ani zpracovatel (Kontrolovaný) nedisponovali souhlasem stěžovatelky k předání jejich osobních údajů Kontrolované.

Podle § 7 zákona č. 101/2000 Sb. povinnosti stanovené v § 5 platí obdobně také pro zpracovatele. Z dikce § 7 však nelze dovodit, že by se na zpracovatele vztahovaly všechny povinnosti, jelikož dodržování všech povinností stanovených § 5 zákona č. 101/2000 Sb. nelze bez dalšího na zpracovatele požadovat. Ze smlouvy o dílo, která odpovídá požadavkům obsaženým v ustanovení § 6 zákona č. 101/2000 Sb., tedy zpracovatelské smlouvě, vyplývá, že pro daný případ, předání osobních údajů za účelem vytvoření strukturovaných databází, je správcem Univerzita, která nese primární odpovědnost za prokázání právního titulu zpracování osobních údajů uchazečů o studium, tj. předání osobních údajů třetímu subjektu.

Kontrolou tedy nebylo zjištěno porušení ustanovení § 5 odst. 2 zákona č. 101/2000 Sb. Kontrolovanou.

Nicméně zákon č. 480/2004 Sb. v § 7 poskytuje ochranu před neoprávněným šířením obchodních sdělení. Podle § 10 odst. 1 písm. a) zákona č. 480/2004 Sb. je dohled nad dodržováním tohoto zákona pro šíření obchodních sdělení svěřen Úřadu pro ochranu osobních údajů. Pojem šíření obchodních sdělení se vztahuje na všechny formy sdělení určené k přímé či nepřímé podpoře zboží nebo služeb konkrétnímu subjektu, pokud tento subjekt je tzv. ekonomickým subjektem, tedy subjektem vykonávajícím podnikatelskou činnost. Podle § 7 odst. 2 zákona č. 480/2004 Sb. podrobnosti elektronického kontaktu lze za účelem šíření obchodních sdělení elektronickými prostředky využít pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.

S účinností od 1. srpna 2006 došlo ke změně právní úpravy, spočívající v novém znění ustanovení § 7 zákona č. 480/2004 Sb. provedené zákonem č. 214/2006 Sb. Tato změna se projevuje v zavedení tzv. principu opt-out, pokud jde o obchodní sdělení zaslaná elektronickými prostředky na adresy zákazníků neboli subjektů již existujících obchodních vztahů. Nově tedy fyzická či právnická osoba, která získala podrobnosti elektronického kontaktu od svého zákazníka v souvislosti s prodejem výrobku nebo služby, může tento elektronický kontakt využít pro potřeby šíření obchodních sdělení, týkajících se jejich vlastních obdobných výrobků nebo služeb, aniž by si opatřovala předchozí souhlas s využitím elektronického kontaktu, za účelem šíření obchodních sdělení, od svých zákazníků. Termín obdobný výrobek či služby je nutno vykládat vždy v konkrétním případě podle jeho okolností, neboť není možné určit jednoznačně hranice tohoto pojmu.

Z kontrolních zjištění vyplynulo, že Kontrolovaná shromažďuje údaje pro zasílání obchodních sdělení z různých zdrojů. Zdrojem pro rozeslání e-mailových zpráv, které byly předmětem kontroly, byly databáze přebírané od fakult jednotlivých vysokých škol obsahující osobní údaje.

Dnem 1. ledna 2012 nabyl účinnosti zákon č. 468/2011 Sb., jímž došlo ke změně zákona č. 480/2004 Sb. Konkrétně došlo k úpravě definice obchodního sdělení ve smyslu § 2 písm. f), kdy byla původní dikce rozšířena tak, že za obchodní sdělení se považují i všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku osoby, která je podnikatelem nebo vykonává regulovanou činnost. Aby byla zpráva považována za obchodní sdělení, je nutné vyhodnotit její faktický obsah, a to v jejím celém kontextu. Pokud zpráva obsahuje informace o určitém nabízení služeb, tedy možnost přijetí bez přijímacích zkoušek na základě výsledku Národních srovnávacích zkoušek, které nahrazují nebo doplňují přijímací zkoušky na desítkách vysokých škol v České republice a na Slovensku za úplatu, slouží taková zpráva k přímé či nepřímé podpoře zboží či služeb nabízených Kontrolovanou, a ve smyslu § 2 písm. f) zákona č. 480/2004 Sb. je tedy obchodním sdělením. Z e-mailové zprávy, obchodního sdělení zaslaného stěžovatelce, jakož i z prohlášení Kontrolované dále vyplývá, že v patičce e-mailové zprávy je obsažen text, jakým způsobem lze zrušit zasílání informačních e-mailů. Z uvedeného je tedy zřejmé, že byt Kontrolovaná e-mailové zprávy považuje pouze za „informační e-mail“, jsou takové zprávy obchodním sdělením sloužícím k přímé či nepřímé podpoře služeb a zboží Kontrolované. Kontrolovaná v písemném vyjádření potvrdila, že takovou zprávu skutečně rozeslala a rozesílání pro ni nezajišťuje jiná firma.

Kontrolovaná pro šíření obchodního sdělení s předmětem „možnost přijetí na univerzitu bez přijímaček“ neměla od uživatelů, kterým bylo obchodní sdělení zasláno, ve smyslu ustanovení § 7 odst. 2 zákona č. 480/2004 Sb. předchozí souhlas. Kontrolou bylo zjištěno porušení ustanovení § 7 odst. 2 zákona č. 480/2004 Sb.

Seznamy členů sdružení

Inspektorka Úřadu na základě podnětu provedla kontrolu, jejímž předmětem bylo dodržování povinností stanovených zákonem č. 101/2000 Sb. se zaměřením na ochranu osobních údajů členů Sdružení hasičů Čech, Moravy a Slezska (dále také „SH ČMS“). Podnět odkazoval na zpřístupnění seznamu členů SH ČMS na www.ulozto.cz. Kontrola byla s SH ČMS jako správcem osobních údajů jeho členů zaměřena na dodržování § 13 zákona č. 101/2000 Sb., tj. technicko-organizační zabezpečení osobních údajů.

Z podnětu vyplývalo podezření, že na internetovém portálu www.ulozto.cz byl volně ke stažení databázový soubor SH ČMS obsahující cca 359 000 osobních údajů členů sdružení. Databáze členů byla uložena na <http://ulozto.cz/xgbGFok/seznam-clenu-xlsx>. Tento soubor byl na webových stránkách [www.ulozto.cz](http://ulozto.cz) uložen dne 21. března 2013 a neprodleně po upozornění ze strany médií byl téhož dne odstraněn. Soubor ve formátu Excel o velikosti 72,99 MB obsahoval osobní údaje týkající se 359 690 členů SH ČMS v rozsahu příslušnost k okresnímu sdružení, příslušnost k obci, jméno, příjmení, datum narození, věk, pohlaví, název klubu, evidenční číslo, rodné číslo, příspěvky ústředí, příspěvky klubu a zařazení dle funkce (trenér, rozhodčí, registrovaný sportovec, funkcionář, technicko-organizační pracovník nebo ostatní).

Dle zástupců SH ČMS byl datový soubor uložen na www.ulozto.cz pověřenou osobou, aby si jej mohl správce, z důvodu velikosti souboru, stáhnout, jelikož soubor o cca 70 MB nebylo možné poslat přes e-mail. Osobní údaje byly pověřené osobě (dále také „zpracovatel“) poskytnuty pro zkompletování, resp. provedení takových úprav, aby soubor (osobní údaje) vyhovoval požadavkům Ministerstva školství, mládeže a tělovýchovy (dále jen „MŠMT“) v rámci žádosti SH ČMS o udělení státní podpory sportu, resp. databázový soubor, vytvořený zpracovatelem bylo potřeba před odesláním na MŠMT zkontrolovat a s ohledem na velikost souboru a rychlost předání dat zvolili jak zpracovatel, tak zástupce kanceláře SH ČMS formu předání souboru přes webový portál www.ulozto.cz.

SH ČMS vyhodnotilo data umístěná v souboru jako nezávadná, protože podle SH ČMS informace v nich nevedly k možnosti atakovat osobu telefonem, e-mailem ani místem bydliště. Konkrétním údajem bylo jméno a datum narození. Dále SH ČMS uvedlo, že ve sdružení není ani pravidlem, že osoba je členem toho spolku, kde má bydliště. A v případě SH ČMS uvedený název města není sídelní adresou člena, ale organizace. Zástupci SH ČMS dále uvedli, že na základě vlastních zkušeností vyhodnotili znění zákona o ochraně osobních údajů tak, že se jedná o zamezení zveřejnění údajů vedoucích k přímé možnosti oslovení osoby, dále že údaje v celém souboru nebyly poskytnuty třetí osobě a měly být na serveru jen po dobu několika hodin, než došlo k jejich stažení a smazání. Zástupce SH ČMS dále sdělil, že *„k této politováníhodné události došlo proto, že programátor, který umísťoval data na VPN – virtuální privátní síť, která v tomto případě slouží k přenosu dat mezi zpracovatelem a osobou pověřenou za správu programu z hlediska potřeb SH ČMS, nebyl k dispozici. Celý soubor dat jsme potřebovali pro kontrolu urychleně přeposlat a vzhledem k obsáhlosti jsme zvolili metodu přes server Uložto.“*

Zástupci SH ČMS dále uvedli, že *„soubor obsahující evidenci členů byl vyhotoven zpracovatelem na jeho počítači, v místě jeho podnikání a bydliště. Po vyhotovení jej v otevřené podobě zaslal jako nešifrovaný a nekryptovaný dokument prostřednictvím webového portálu ulozto.cz. Takto jej odeslal, protože si neuvědomil, že by mohlo dojít ke zneužití tohoto dokumentu. Neprodleně po upozornění, že se o věc zajímají novináři, přístup k souboru zablokoval a z webových stránek [www.ulozto.cz](http://ulozto.cz) odstranil.“*

Soubor byl vytvořen z primární databáze členů SH ČMS, která je uložena na serveru v USA, a to prostřednictvím cloudových služeb.

Evidenční program členské základny je potřebný rovněž i pro získávání finančních prostředků z grantů ministerstev a krajů, kdy ministerstva vyloženě požadují k žádostem o grant výpisy z evidence členské základny v elektronické podobě. MŠMT například bude od roku 2014 požadovat údaje o členské základně v elektronické podobě povinně, což vyplývá z dokumentu

„Státní podpora sportu pro rok 2013“ kapitola B – Pokyny pro předkládání žádostí – neinvestiční prostředky, odst. 3.

Kontrolující inspektorka v kontrolním protokolu konstatovala, že evidence členské základny je založena na základě přihlášky, která je současně využívána jako evidenční karta člena. Informace shromažďované a dále zpracovávány v evidenci SH ČMS jsou informacemi, jejichž účelem je bez jakýchkoliv pochyb identifikovat konkrétního jednotlivého člena sdružení. Informace shromažďované a dále zpracovávány v souvislosti s vedením evidence členů SH ČMS jsou osobními údaji dle § 4 písm. a) zákona č. 101/2000 Sb., neboť tyto informace se týkají určeného subjektu údajů, který je na základě shromážděných informací přímo určitelný.

SH ČMS údaje o svých členech shromažďuje od zájemců o členství, ukládá je ve své evidenci, přiřazuje k nim dále informace vzniklé z činnosti člena sdružení. Dále je systematicky ukládá v listinné podobě a prostřednictvím softwarového programu „členská evidence“ je shromažďuje, třídí, ukládá na nosiče, vyhledává a používá a využívá v rámci své činnosti, resp. činnosti jednotlivých organizačních složek, tedy zpracovává je ve smyslu ustanovení § 4 písm. e) zákona č. 101/2000 Sb., přičemž současně SH ČMS rozhodlo nejen o účelu zpracování, ale prostřednictvím stanov, organizačního řádu a smluv o prostředcích zpracování osobních údajů svých členů, a je tedy správcem osobních údajů dle § 4 písm. j) zákona č. 101/2000 Sb. a za toto zpracování odpovídá.

SH ČMS uzavřelo s fyzickou osobou podnikající podle živnostenského zákona smlouvu, jejímž předmětem bylo vytvoření elektronické databáze evidence členské základny a jejího následného zpracování. Z hlediska zákona č. 101/2000 Sb. byla tato fyzická osoba zpracovatelem osobních údajů, neboť jako samostatný subjekt na základě pověření SH ČMS zpracovával osobní údaje členů sdružení. SH ČMS tedy rozhodlo o předání a následném zpracování osobních údajů členů sdružení zpracovateli, a to za účelem dodávky webové aplikace členské základny a následném zajištění provozu této aplikace. SH ČMS, jako správce osobních údajů, se zpracovatelem uzavřelo písemnou smlouvu, jejímž obsahem je i převod osobních údajů členů sdružení ze stávající členské evidence do nové, centralizované členské databáze členů SH ČMS. Sdružení, jako správce osobních údajů, uzavřelo se zpracovatelem písemnou smlouvu o rozsahu, účelu i době, na kterou je uzavřena. Smlouva neobsahuje žádnou záruku zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů. Smlouva obsahuje závazek zpracovatele provést dílo na svůj náklad a na své nebezpečí, včetně toho, že při určení způsobu provedení díla není vázán pokyny objednatele a při provádění díla jinou osobou má zhotovitel odpovědnost, jako by dílo prováděl sám, dále že na svůj náklad a nebezpečí zajistí ochranu datových souborů a dat objednatele před poškozením, zničením, zneužitím a odcizením. Takto uzavřenou smlouvu nelze považovat za splnění povinnosti správce osobních údajů dle § 6 zákona č. 101/2000 Sb., a to i přesto, že obsahem smlouvy je migrace dat ze stávajících dílčích systémů do nově vytvořeného databázového souboru, neboť smyslem ustanovení § 6 je povinnost správce osobních údajů prověřit a smlouvou de facto schválit záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů u zpracovatele. SH ČMS se rovněž, jako správce osobních údajů, nemůže touto formou zbavit své povinnosti, a bez jakékoliv znalosti a záruk umožnit zpracovateli předávání osobních údajů svých členů třetím osobám, neboť tímto správcem krátí subjekt údajů na jeho právu mít pod kontrolou své osobní údaje, které je zahrnuto nejen v § 11 odst. 1 zákona č. 101/2000 Sb., dle kterého je správce osobních údajů povinen subjekt údajů informovat mimo jiné i o tom, kdo a jakým způsobem bude osobní údaje

zpracovávat a komu mohou být osobní údaje zpřístupněny, ale zejména v § 12 zákona č. 101/2000 Sb., tedy právu přístupu subjektu údajů k informacím.

SH ČMS tím, že předalo zpracování osobních údajů členů sdružení zpracovateli, aniž by svého zpracovatele zavázalo k ochraně osobních údajů a aniž by si smluvně vyhradilo kontrolní právo, se spokojilo s obecnou informací, že celá databáze členské základny je uložena v cloudovém úložišti na serverech v USA, bez smluvního zabezpečení ze strany provozovatele cloudu. Proti takto zcela nezabezpečenému zpracování osobních údajů neučinilo SH ČMS žádná opatření. Správce osobních údajů je podle § 13 odst. 2 zákona č. 101/2000 Sb. povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy. Základní činnost SH ČMS se řídí stanovami sdružení a organizačním řádem. Oba tyto právní dokumenty upravují pouze základní povinnosti v oblasti odpovědnosti za provoz a zabezpečení informací jednotlivým organizačním složkám SH ČMS. SH ČMS vydalo metodický pokyn starosty k nakládání s osobními údaji (č. 3/2009), který v obecné rovině upravuje nekonkrétní a neosobní povinnost při zpracování osobních údajů členů sdružení. V rámci tohoto metodického pokynu byl správně stanoven účel zpracování osobních údajů členů SH ČMS, a to evidence členské základny. V další části jsou podávány obecné informace o fungování programu evidence, včetně informace o přenesení odpovědnosti administrátorských práv na zpracovatele osobních údajů. Jeho obsahem je postup při přidělování přístupových práv v rámci jednotlivých organizačních jednotek sdružení se zjednodušeným prohlášením o odpovědnosti držitelů vstupních hesel. Součástí metodického pokynu je informace o tom, že bude zřízena virtuální privátní síť a bude mezi zpracovatelem a pověřenou osobou, pro správu dat za SH ČMS, instalován software umožňující zabezpečení ochrany dat při přenosu.

SH ČMS nepředložilo žádný dokument, vnitřní předpis či jiná přijatá opatření, ze kterých by vyplývalo, jakým způsobem byla organizačně začleněna a komu je odpovědná osoba pověřená správou dat ve SH ČMS. Dále nedokumentovalo žádná opatření v oblasti kontroly dodržování přenosu dat, jejich předávání mezi jednotlivými organizačními jednotkami, kontroly přístupu k datům, ale ani kontroly zabezpečení IT technologie, zejména zajištění kontroly dodržování povinností smluvního zpracovatele osobních údajů. SH ČMS nepřijalo žádná opatření pro předání a uchování osobních údajů členů sdružení v cloudovém úložišti na serveru v USA ani neučinilo žádná opatření proti svému zpracovateli.

Z uvedeného je zřejmé, že SH ČMS nesplnilo jako správce osobních údajů povinnost dle § 13 odst. 2 zákona č. 101/2000 Sb. zpracovat a dokumentovat přijatá technicko-organizační opatření k zajištění ochrany osobních údajů.

Důsledkem skutečnosti, že SH ČMS v rámci smlouvy o zpracování osobních údajů podle § 6 zákona č. 101/2000 Sb. nesplnilo povinnost přijmout a schválit záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů, a skutečnosti, že SH ČMS nesplnilo povinnosti přijmout a dokumentovat přijatá a provedená technicko-organizační opatření, a skutečnosti, že v rámci SH ČMS nebyla prováděna žádná kontrola v oblasti ochrany osobních údajů, bylo neoprávněně zpřístupnění kompletní databáze členské základny sdružení v nezajištěné podobě na webových stránkách www.ulozto.cz.

SH ČMS tím, že prostřednictvím webových stránek www.ulozto.cz zpřístupnilo osobní údaje 359 690 členů SH ČMS v nezajištěné formě po dobu nepřesahující jeden den, porušilo povinnost správce osobních údajů podle § 13 odst. 1 zákona č. 101/2000 Sb. přijmout taková opatření, aby

nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům. SH ČMS tím, že nezajistilo ani jako správce osobních údajů, ani prostřednictvím svého zpracovatele, pořizování elektronických záznamů (logování), které by umožnily určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány v databázi členů sdružení, porušilo povinnost uloženou § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

SH ČMS byla následně v rámci správního řízení za výše uvedená porušení zákona č. 101/2000 Sb. uložena pokuta ve výši 80 000 Kč.

Na základě výše uvedené kontroly byla v rámci kontrolního plánu Úřadu pro rok 2014 zahájena kontrola MŠMT, jejímž předmětem je dodržování povinností správce osobních údajů stanovených v Hlavě II zákona č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů v dokumentační agendě dotačních titulů realizovaných MŠMT vyhlášených jako Státní podpora sportu pro roky 2013 a 2014. Uvedená kontrola dosud probíhá.

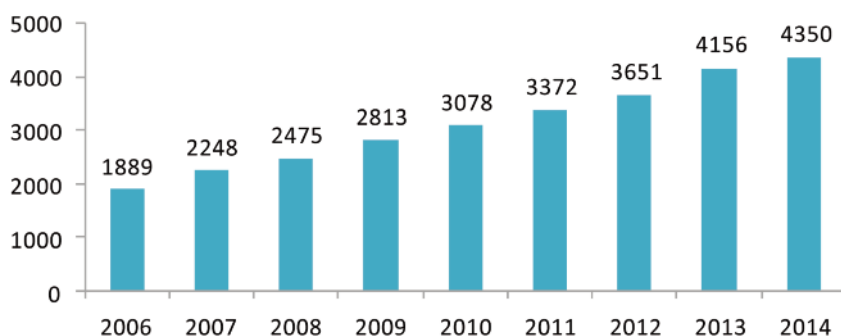
Ostatní dozorová činnost

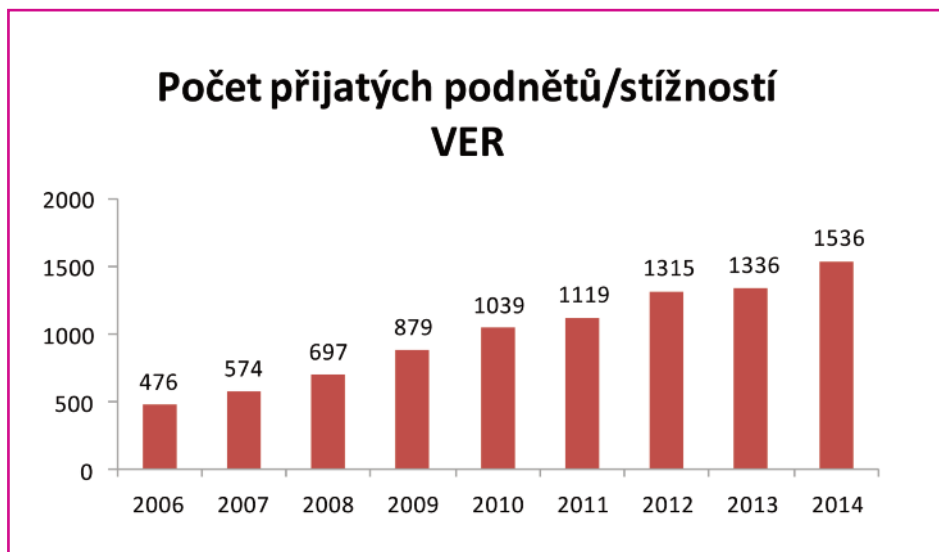
• VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ

Na základě poznatků získaných při vyřizování stížností a konzultační agendy Úřadu, která je vykonávána zejména Odborem pro styk s veřejností (VER), je možné s blížícím se výročím patnáctileté účinnosti zákona č. 101/2000 Sb. konstatovat zvýšené společenské povědomí o ochraně osobních údajů a činnosti Úřadu, jak mezi veřejností, tak i správci osobních údajů a dalšími zainteresovanými subjekty. Tento fakt je zřejmý nejen ze stále se zvyšujícího počtu přijatých podání (stížností/podnětů a dotazů), které Odbor pro styk s veřejností za rok 2014 oproti minulým letům vyřídil, ale i z charakteru a komplexnosti těchto podání a konzultovaných témat.

Za nárůstem v počtu podání stojí v tomto roce zejména nárůst počtu přijatých stížností, kdy oproti minulému roku, kdy byla zaznamenána stagnace v počtu přijatých stížností, došlo opět k nárůstu počtu přijatých stížností, jak dokresluje níže uvedený graf.

Celkový počet vyřízených dotazů a stížností/podnětů VER





Zvýšený počet přijatých stížností se odrazil mimo jiné i v počtu případů, které byly Odborem pro styk s veřejností postoupeny k dalším opatřením, tj. ke kontrole (237) nebo správnímu řízení (49). 21 podání bylo v souladu s § 12 zákona č. 500/2004 Sb., správní řád, postoupeno příslušným správním orgánům k dalšímu vyřízení.

Jako aktuální téma stížností a konzultační agendy lze zmínit tzv. right to be forgotten, tj. právo být zapomenut, které bylo v roce 2014 významným tématem ochrany osobních údajů na internetu, a to v důsledku rozhodnutí Soudního dvora Evropské unie ve věci Google v. Costeja. V tomto rozhodnutí Soudní dvůr Evropské unie vyslovil názor, že lidé mají právo na odstranění neaktuálních či nerelevantních výsledků vyhledávání týkajících se jejich osob, tj. rozhodnutí je nutné aplikovat na všechny vyhledávače, nikoli pouze na vyhledávač společnosti Google Inc. Rozhodnutí Soudního dvora Evropské unie však nepřináší absolutní možnost odstranění všech výsledků vyhledávání o konkrétní osobě, tak jak je někdy veřejností mylně vykládáno.

V ostatních aspektech byla stížnostní agenda co do předmětu podání obdobná jako v minulém roce, tj. nejčastěji přijaté stížnosti se tradičně týkaly provozování kamerových systémů (na pracovišti, v bytových domech, na veřejnosti), dále dlužnických registrů, a to především registru SOLUS a Centrálního registru dlužníků České republiky. Nelze opominout ani např. podněty týkající se nabídek prodeje databází e-mailových kontaktů a dalších osobních údajů nebo problematiku zpracování osobních údajů v pracovněprávních vztazích a zdravotnictví. Podstatnou stížnostní agendou jsou též stížnosti týkající se zpracování osobních údajů územně samosprávnými celky, zejména obcemi.

V rámci vyhodnocení přijatých stížností byla nejčastěji shledávána podezření z porušení zákona č. 101/2000 Sb. týkající se neexistence právního titulu ke zpracování osobních údajů či nedodržení jiných podmínek zpracování osobních údajů stanovených zákonem č. 101/2000 Sb. Jednalo se například o shromažďování nadbytečných osobních údajů, zpracování osobních údajů k jinému účelu, než ke kterému byly shromážděny, a v neposlední řadě lze zmínit nedostatečné zabezpečení osobních údajů, resp. jejich únik.

V případě konzultační činnosti Úřadu, prováděné zejména v písemné podobě, ale i telefonicky a osobně v prostorách Úřadu, se jednoznačně nejvíce konzultací týká podmínek pro používání kamerových systémů, kde je nutné zohledňovat rozdíly u kamerových systémů spadajících do režimu zákona č. 101/2000 Sb., a kamer instalovaných pro osobní potřebu v rodinných domech – nezaznamenávajících veřejné prostranství a zákonem upravené používání především policejních kamerových systémů. Zohledňována je i odlišnost kamer používaných v autech pro monitorování prostoru při provozu vozidla.

Velmi časté byly dotazy na zákonné podmínky pro pořizování kopií osobních dokladů, zejména občanského průkazu v souvislosti s uzavřením smlouvy o poskytování služeb elektronických komunikací či bankovních služeb. Časté byly i dotazy na oprávněnost požadavku na sdělení rodného čísla v různých životních situacích.

Úřad se setkával i s dotazy na zveřejňování osobních údajů občanů na internetových stránkách obce, kdy jde často o zveřejnění na základě zvláštního zákona, tedy bez souhlasu občana, a dále na zveřejňování audiovizuálních záznamů z jednání zastupitelstva s anonymizováním údajů týkajících se soukromého života občanů.

Dalším tématem konzultací je odlišnost bankovních a nebankovních registrů dlužníků.

Tazatelům je obvykle třeba vysvětlit odlišnost při vedení těchto registrů z hlediska podmínek (právního titulu) pro zpracování osobních údajů podle zákona č. 101/2000 Sb. Zatímco v případě bankovních registrů jde o zpracování osobních údajů stanovené zákonem č. 21/1992 Sb., o bankách, a je tak prováděno bez souhlasu klientů banky v souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., v případě nebankovních registrů, jestliže jde o zpracování osobních údajů zákonem nestanovené, jde o zpracování prováděné na základě souhlasu subjektu údajů, od čehož se odvíjejí i jiné možnosti pro uplatnění některých práv subjektu údajů, zejména pokud jde o dobu uchovávání osobních údajů.

Pokud jde o informační systémy veřejné správy, je častým předmětem dotazů veřejnost insolvenčního rejstříku a možnosti, jak tuto veřejnost omezit, zejména pokud jde o osobní údaje věřitelů, např. zaměstnanců. Dotazy se týkají i možnosti využívání osobních údajů z dalších veřejně přístupných rejstříků, živnostenského, obchodního a také katastru nemovitostí.

Obce se často dotazují na poskytnutí osobních údajů svých zástupců nebo zaměstnanců na základě žádosti podle zákona o svobodném přístupu k informacím, zejména údajů o platech a odměnách s ohledem na nejnovější rozhodnutí Nejvyššího správního soudu sp. zn. 8 As 55/2012 v této věci.

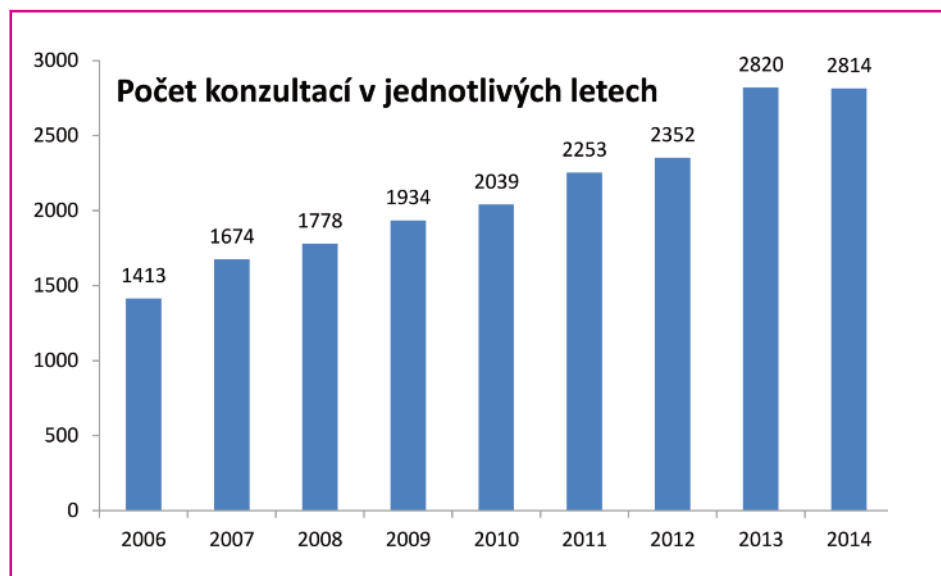
Nelze opominout ani dotazy pracovníků zařízení sociálních služeb na zpracování osobních údajů jejich klientů a na výjimky podle příslušných ustanovení zákona č. 101/2000 Sb. a podle zákona č. 108/2006 Sb., o sociálních službách.

Zodpovídány byly i dotazy týkající se použití či zneužití osobních údajů (zejména v prostředí internetu) mimo režim zákona č. 101/2000 Sb., kdy je zpravidla konstatováno, že ne každé nakládání s osobními údaji je zpracováním osobních údajů dle definice zákona č. 101/2000 Sb. a je doporučován občanskoprávní postup či postup dle § 5 zákona č. 480/2004 Sb.

Jak ukazuje níže uvedený graf, počet písemných konzultací se ve srovnání s minulým rokem ustálil.

Úřad v roce 2014 obdržel několik dotazů a stížností týkajících se využívání kamerových systémů pro ochranu budov zastupitelských úřadů na území České republiky. Proto byla v součinnosti s Ministerstvem zahraničních věcí připravena stručná metodika obsahující popis

základních pravidel pro takovéto zpracování osobních údajů. Tato metodika byla v listopadu 2014 formou cirkulární nóty rozeslána všem zahraničním zastupitelstvím v České republice.



• NĚKTERÉ POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

Správní řízení vede v Úřadu podle jeho organizačního řádu především (avšak nikoli výlučně) Odbor správních činností. Jedná se přitom v případě Odboru správních činností v podstatě o dva typy řízení: řízení o správních deliktech a řízení v případech, kdy z Úřadu oznámeného zpracování vyplyne obava, že při zpracování osobních údajů by mohlo dojít k porušení zákona č. 101/2000 Sb. (viz § 17 tohoto zákona). Oba typy řízení vede Úřad z moci úřední, tedy ex officio.

V roce 2014 získal na základě novelizace zákona č. 101/2000 Sb. Úřad možnost upustit od uložení pokuty mj. v případech, kdy dojde k nápravě protiprávního stavu bezprostředně poté, kdy bylo zjištěno porušení povinnosti (viz § 40a tohoto zákona).

1. K řízením podle § 17 zákona č. 101/2000 Sb.

K těmto řízením, která navazují na oznamovací povinnost správce upravenou v § 16 zákona č. 101/2000 Sb., je třeba především zdůraznit, že se nejedná o řízení sankční. Jejich cílem je, zjednodušeně řečeno, upravit oznámené parametry zpracování osobních údajů do podoby, která odpovídá zákonným požadavkům. Těžiště těchto řízení je tedy v ústním jednání s účastníkem řízení (tj. osobou, která je ve vztahu k oznámenému zpracování správcem), na němž účastník řízení poskytne Úřadu veškeré podrobnosti zamýšleného zpracování, a pracovníci Úřadu mu v návaznosti na tyto informace objasní podmínky, za kterých lze zpracování provádět. Následuje pak obvykle změna oznámeného zpracování, kterou účastník řízení provede právě na základě informací vyplývajících z ústního jednání. Je třeba současně uvést, že tato řízení se týkají téměř ve 100 % případů oznámených zpracování osobních údajů prostřednictvím kamerových systémů. Dále lze konstatovat, že (jak vyplývá z příslušných statistik) v posledních třech letech je více než 95 % těchto řízení zastaveno se závěrem, že oznámeným zpracováním nebude správce porušovat povinnosti stanovené zákonem č. 101/2000 Sb. a zpracování je na základě tohoto rozhodnutí zapsáno do registru, který Úřad vede. Ve zbylých případech Úřad zpracování nepovolí (v roce 2014 se jednalo například o kamerový systém umístěný v bytovně, uvnitř autobusů a v bytovém domě).

Základním problémem, se kterým se Úřad při těchto řízeních setkává, je skutečnost, že byť je povinnost oznámit zpracování správce povinen plnit předtím, než začne zamýšlené zpracování provádět, je někdy kamerový systém, jehož prostřednictvím jsou osobní údaje zpracovávány, již v provozu, příp. sice v provozu není, ale byl již správcem v příslušných prostorách umístěn. Změny v nastavení jednotlivých kamer, ke kterým v průběhu řízení často dochází, tak pro správce mohou znamenat dodatečné finanční náklady spojené právě se skutečností, že podmínky provozu celého systému začal řešit v nevhodné fázi projektu (tj. nikoli před samotnou instalací systému). Byť se jedná obvykle o technologie, které umožňují provést řadu dodatečných opatření (jako je například využití rastru), je nepochybné, že je pro správce výhodnější otázkou zákonnosti zamýšleného zpracování, do které patří i konkrétní nastavení jednotlivých kamer, řešit co nejdříve.

2. K možnosti upustit od uložení pokuty

Zákonem č. 64/2014 Sb., kterým se mění některé zákony v souvislosti s přijetím kontrolního řádu, bylo do zákona č. 101/2000 Sb. s účinností od 1. května 2014 doplněno zcela nové

ustanovení § 40a, podle kterého, dojde-li k nápravě protiprávního stavu v souladu s uloženým opatřením nebo bezprostředně poté, kdy bylo zjištěno porušení povinnosti, může Úřad upustit od uložení pokuty.

Jedná se o ustanovení, které je nepochybně třeba uvítat. Je třeba vzít v úvahu, že sankce, které zákon č. 101/2000 Sb. za porušení jím upravených povinností stanoví, mají velmi vysoké horní sazby (tj. 100 000 Kč za porušení povinnosti mlčenlivosti a 1 000 000 až 10 000 000 za porušení povinností správce či zpracovatele). Naštěstí v zákoně není a nikdy nebyla stanovena dolní hranice, protože by s ohledem na uvedené nastavení horní hranice sankce musela být poměrně velmi vysoká a pro řadu správců, kterými mohou být v řadě případů i fyzické osoby nepodnikající, až likvidační.

Do konce dubna 2014 přitom neexistovala možnost, jak při zjištění porušení zákonem stanovených povinností, které je současně správním deliktem, sankci neuložit. Takový postup nebyl možný ani u relativně bagatelních jednání, kde odpovědná osoba svoje pochybení napravila neprodleně poté, co na něj byla upozorněna. Tuto situaci nové ustanovení § 40a zákona č. 101/2000 Sb. mění.

To samozřejmě neznamená, že by Úřad mohl při používání tohoto ustanovení postupovat zcela libovolně, neboť je povinen mj. dodržet základní zásady činnosti správních orgánů upravené v § 2 a násl. zákona č. 500/2004 Sb., správní řád, zejména pak zásady ochrany legitimního očekávání upravené v § 2 odst. 4 tohoto zákona. Aby tyto své povinnosti Úřad dodržel, upravil možnosti aplikace § 40a zákona č. 101/2000 Sb. vnitřním předpisem, kterým je směrnice č. 5/2014, jíž se stanoví podmínky pro upuštění od uložení pokuty. Podle této směrnice lze upustit od uložení pokuty, dojde-li k nápravě protiprávního stavu v souladu s uloženým opatřením nebo bezprostředně poté, kdy se zjistí porušení povinnosti, a současně jsou kumulativně splněny tyto podmínky:

- jednání nesouvisí s porušením povinnosti při zpracování citlivých údajů,
- jednání nezasahuje do práv vysokého počtu subjektů údajů,
- jednání nepředstavuje podstatný zásah do práv subjektu údajů,
- souhrn okolností stanovených v § 46 zákona č. 101/2000 Sb. by odůvodňoval uložení pokuty do výše 5 000 Kč.

Že se jedná o ustanovení, které je v praxi Úřadu využitelné, dokládá statistika Odboru správních činností, který od 1. května do 31. prosince 2014 upustil na základě uvedeného ustanovení od uložení pokuty v 17 případech. Příkladem se jednalo o porušení povinnosti stanovené v § 12 zákona č. 101/2000 Sb., tj. povinnosti správce osobních údajů předat bez zbytečného odkladu na žádost subjektu údajů informaci o zpracování jeho osobních údajů, dále porušení § 5 odst. 1 písm. f) zákona č. 101/2000 Sb., tedy povinnosti správce zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny (zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6 uvedeného zákona, nebo pokud k tomu dal subjekt údajů předem souhlas), a to zveřejněním údajů na webových stránkách obce (dokonce v několika případech).

Závěrem k této problematice lze konstatovat, že se jedná o z hlediska praxe Úřadu velmi vhodnou legislativní změnu, která potlačuje jeho sankční funkci a soustředí se na nápravu protiprávního stavu, což by mělo být vždy hlavním cílem činnosti Úřadu (pokud je to samozřejmě možné, protože nepochybně existuje řada případů, kdy nelze následky protiprávního jednání odpovědných subjektů již nijak napravit).

• POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

Některá rozhodnutí Úřadu jsou předmětem soudního přezkumu. Pokud jde o konkrétní poznatky ze soudní praxe za rok 2014, lze poukázat na několik dále uvedených významných rozsudků, týkajících se zejména kamerových systémů, zpřístupnění provozních a lokalizačních údajů, realizace nápravných opatření, zpracování osobních údajů v rámci televizního vysílání a povinností při zabezpečení osobních údajů.

1. Dohled zajišťovaný pomocí videokamer na pracovišti je aplikovatelný pouze v případě, kdy stanovený účel nelze naplnit prostřednictvím mírnějších prostředků; tomuto účelu je nutno přizpůsobit i stanovení lhůty pro zpracování záznamů. Plnění informační povinnosti dle § 11 zákona č. 101/2000 Sb. je závislé na okruhu monitorovaných osob. V případě pochybností má správce osobních údajů požádat o konzultaci podle § 29 odst. 1 zákona č. 101/2000 Sb.

V rozsudku čj. 8A 182/2010-69 ze dne 2. září 2014 Městský soud v Praze především vyjádřil názor, že zaměstnanci mají i na pracovišti právo na jistou míru soukromí, byť je z povahy zaměstnaneckého vztahu nižší než např. ve vlastních obytných prostorách, neboť soukromý a pracovní život nelze zcela oddělit; určitou soukromou sféru člověk nosí neustále s sebou a zásah do ní je v případě zaměstnance monitorovaného kamerovým systémem významný v tom, že je sledován každý den neustále po celou pracovní dobu či její převážnou část. Dále pak Městský soud v Praze odkázal na rozsudek Nejvyššího správního soudu sp. zn. 5 As 158/2012, v němž bylo ohledně použití kamerového systému jako prostředku sledování zaměstnanců konstatováno, že „k instalaci kamerových systémů, s ohledem na jejich povahu a zásah do osobní integrity osob, je možné přistoupit až tehdy, pokud už veškeré méně invazivní prostředky selhaly anebo by nebyly schopny naplnit vytyčený účel, který je sledován. Je zcela nepochybné, že kamerový systém ve srovnání s jinými prostředky (např. personálními, mechanickými), které mohou dosáhnout naplnění účelů žadatelem sledovanými, zasahuje základní lidská práva, a to právo na soukromí a na soukromý rodinný život [...], a tudíž i do lidské důstojnosti, z které tato práva vyplývají.“

K tomu ovšem Městský soud v Praze v rámci rozsudku čj. 8A 182/2010-69 ze dne 2. září 2014 dodal, že skryté sledování je v tomto ohledu významnějším zásahem do soukromí než sledování, o němž osoby vědí, zásah do soukromí však představují oba tyto způsoby sledování. V posuzovaném případě byla rozlišovací schopnost kamer natolik vysoká, že bylo možno rozpoznat jednotlivé osoby (zaměstnance), včetně drobných detailů, a vzhledem k intervalům 5–10 vteřin mezi pořízením jednotlivých snímků bylo možno podrobně sledovat jejich činnost, a to po převážnou část pracovní doby; k významnému zásahu do jejich soukromí tedy došlo. Pokud jde o deklarované účely spočívající v kontrole otevírací doby, monitorování pracovní doby a rozložení pracovní zátěže, zvolený způsob byl k jejich dosažení způsobilý, neboť umožnil zjistit, kdy a který zaměstnanec se v prodejně nacházel, avšak je zřejmé, že zaměstnavatel mohl zvolit mírnější prostředky, např. čipové karty nebo kameru snímající výhradně prostor vstupu do

prodejny, a nebylo třeba sledovat přímo zaměstnance u prodejního pultu; výkon zaměstnanců pak bylo možno měřit i podle dosažených výsledků.

Následně však zaměstnavatel za účel kamerového systému označil výhradně ochranu majetku, konkrétně herních konzolí umístěných po obvodu prodejen a obzvláště ochranu před neoprávněným poskytováním slev zaměstnanci. V této souvislosti Městský soud v Praze konstatoval, že z archivovaných snímků vyplynulo, že v každé z 20 prodejen patřících zaměstnavateli se nacházela právě jedna kamera. Kamery s jedinou výjimkou vždy snímaly pouze část prodejny, a to pouze malý několikametrový úsek, pokaždé však byly zaměřeny na prostor prodejního pultu a pokladny. Kamerový systém tedy nemohl sloužit k účinné ochraně proti krádežím herních konzolí, neboť nemonitoroval místa, kde měly být umístěny. Ve sledovaném prostoru prodejního pultu jakékoli případné krádeži naopak předcházela přítomnost prodávče. Městský soud v Praze k tomu uvedl, že vzhledem k velikosti těchto přístrojů by byla dostatečným prostředkem ochrany kamera snímající prostor východu z prodejny.

Zároveň ale bylo také připomenuto, že nezbytnost sledování prodejního pultu byla zaměstnavatelem původně zdůvodněna tak, že zaměstnanci často poskytují slevu neexistujícím zákazníkům, a jen takto lze zpětně ověřit, zda se v době prodeje nacházel u pultu skutečný zákazník. V tomto ohledu Městský soud v Praze ovšem uvedl, že takovému zneužívání bylo možno zabránit patřičnou úpravou svého slevového programu; i kdyby však byla taková úprava z hospodářského hlediska příliš tíživá, mohl zaměstnavatel nastavit kamery tak, aby snímaly prostor před prodejním pultem, avšak nikoli prostor za ním, v němž se po většinu pracovní doby zdržují zaměstnanci; takovým způsobem by zaměstnavatel mohl ověřit přítomnost zákazníka u pultu a zároveň by bylo chráněno soukromí zaměstnanců. Městský soud v Praze tak i v tomto případě konstatoval, že zaměstnavatel mohl užít z hlediska ochrany soukromí zaměstnanců mírnějších prostředků, tudíž zpracovával osobní údaje v rozporu s § 5 odst. 2 zákona č. 101/2000 Sb.

Městský soud v Praze se dále zabýval problematikou týkající se doby uchování osobních údajů. Podle § 5 odst. 1 písm. e) zákona č. 101/2000 Sb. je správce povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Zaměstnavatel, tedy správce osobních údajů tuto dobu stanovil na jeden rok, během něhož uchovával veškeré pořízené záběry. To odůvodňoval výhradně tak, že podezření ohledně neoprávněně poskytnutých slev lze pojmout až dodatečně, a pro zjištění, zda byla sleva poskytnuta skutečnému zákazníkovi, je třeba porovnat pokladní údaje (čas poskytnutí slevy) s příslušnými kamerovými záběry. Z uvedeného je zřejmé, že správce osobních údajů evidoval veškeré časy poskytnutí slev, tudíž mu nic nebránilo, aby při převádění záběrů z počítačových jednotek na CD či DVD, k němuž docházelo po jednom měsíci od pořízení záběrů, uchovával pouze záběry pořízené v době, kdy podle údajů z pokladny byly ze strany zaměstnanců poskytnuty slevy. Vzhledem k tomu, že u naprosté většiny zpracovaných záběrů postačovalo uchování po dobu nanejvýš několika týdnů, muselo být správcem osobních údajů zřejmé, že doba jednoho roku přesahuje dobu nezbytnou. V této souvislosti neobstojí ani poukaz správce osobních údajů na neurčitost ustanovení § 5 odst. 1 písm. e) zákona č. 101/2000 Sb.

Co se týče informační povinnosti podle § 11 odst. 1 a 5 zákona č. 101/2000 Sb., je třeba zohlednit skutečnost, že ve vztahu k nahodilým kolemjdoucím (např. zákazníkům) je úplné splnění této povinnosti prakticky nereálné, a za postačující je třeba považovat poskytnutí základní informace o tom, že v daném místě dochází k monitorování kamerovým systémem se

záznamem, kdo je správcem systému, popřípadě kde lze získat informace o probíhajícím zpracování osobních údajů. Zvláště důležité ovšem je sdělení o tom, kdo kamerový systém provozuje. Naopak v případě předem známého okruhu osob (typicky zaměstnanců) je třeba trvat na úplném poskytnutí informací.

Správce osobních údajů ostatně mohl v případě pochybností o přiměřenosti jím přijatého opatření požádat podle § 29 odst. 1 zákona č. 101/2000 Sb. o konzultaci, to však neučinil.

2. Provozní a lokalizační údaje evidované a uchovávané podle ustanovení § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, není možno zpřístupnit s odkazem na ustanovení § 40 odst. 1 písm. a) zákona č. 121/2000 Sb., autorský zákon

Městský soud v Praze svým rozhodnutím čj. 31C 1/2014-88 ze dne 21. srpna 2014 zamítl žalobu, již bylo požadováno s odkazem na ustanovení § 40 odst. 1 písm. a) zákona č. 121/2000 Sb. zpřístupnit provozní a lokalizační údaje evidované a uchovávané podle ustanovení § 97 odst. 3 zákona č. 127/2005 Sb. primárně z toho důvodu, že předmětné údaje již byly zlikvidovány. Nicméně zároveň v zásadě uznal za správnou argumentaci, podle níž nakládání s provozními a lokalizačními údaji je přísně upraveno zákonem č. 127/2005 Sb., přičemž tato úprava je ve vztahu k zákonu č. 121/2000 Sb. lex specialis. Poskytovatelé služeb internetového připojení sdělují předmětné údaje jen na základě této speciální normy, a to navíc pouze nastanou-li v okolnosti touto speciální normou předvídané. Tato povinnost se tudíž nijak nevztahuje k osobám uplatňujícím svá autorská či jim obdobná práva, přičemž obecného ustanovení § 40 odst. 1 písm. c) zákona č. 121/2000 Sb. nelze použít. Dále pak je třeba vzít v úvahu, že v jednom konkrétním okamžiku může být přidělena jediná IP adresa více uživatelům. Stejně tak je nutno připomenout, že Soudní dvůr Evropské unie dospěl k závěru, že evropská legislativa jen nebrání (a nikoli příkazuje) přijetí takové národní úpravy, dle níž by bylo možno splnit, co bylo požadováno žalobou, ovšem v rámci České republiky žádná taková konkrétní úprava dosud přijata nebyla.

3. Pokud kontrolovaný hodlá poukazovat na to, že mu byly uloženy povinnosti, které již neodpovídají aktuálnímu stavu věcí, je třeba, aby toto učinil již v námítkách proti protokolu o kontrole

Nejvyšší správní soud ve svém rozsudku čj. 3 As 124/2013-34 ze dne 30. července 2014 uvedl, že k upuštění od vytýkané praxe (v tomto případě provozu daného kamerového systému) ze strany správce osobních údajů reálně mohlo dojít teprve poté, co bylo jasné, co se po něm požaduje, tj. poté, co byla daná opatření k nápravě poprvé formulována protokolem o kontrole, resp. po podání námitek proti protokolu o kontrole až poté, co o nich bylo rozhodnuto, kdy byla většina z uložených opatření v nezměněné podobě potvrzena rozhodnutím předsedy Úřadu. V takové situaci však již ze strany správce nemohlo jít o nic jiného než neprodlenou nápravu zjištěného závadného stavu, byť náprava, jejíž způsob si zvolil sám správce, šla převážně nad rámec jmenovitě ukládaných povinností v předmětných opatřeních (opatření neukládala od záznamů a zpracování osobních údajů zcela upustit, ale kamerový provoz toliko stanoveným způsobem determinovat a o daném provozu také řádně a úplně informovat). I s přihlédnutím k této úvaze Nejvyšší správní soud konstatoval, že mu nezbyvá než zopakovat, že jestliže správce

opravdu mínil vážně své tvrzení, že mu za jím takto předestíraného stavu věci byly kontrolním protokolem ukládány povinnosti, které již neodpovídaly aktuálnímu stavu věci, potom je zcela nepochopitelné, a také nelogické, že toto neuplatnil v námitkách proti protokolu o kontrole, neboť to bylo zcela zjevně v jeho prvořadém zájmu. Později se však nemůže daná námitka jevit jinak než zcela účelová. O tom svědčí i fakt, že vzdor tomu, že správce namítal, že včasným upuštěním od pořizování záznamů a zpracování osobních údajů pominuly důvody pro uložení jakýchkoliv opatření, zároveň uložená opatření rozporoval i věcně.

4. Příprava televizní reportáže směřující ke zveřejnění osobních údajů prostřednictvím televizního vysílání je zpracováním osobních údajů ve smyslu zákona č. 101/2000 Sb.

Nejvyšší správní soud v rozhodnutí čj. 6 As 144/2013-34 ze dne 20. srpna 2014 uvedl, že nemá pochybnosti o tom, že jednání spočívající v odvysílání televizní reportáže, v níž bylo uvedeno, že osoba identifikovaná mj. jménem a příjmením trpí přenosnou chorobou, náleží pod pojem zpracování osobních údajů ve smyslu zákona č. 101/2000 Sb. Podstatou televizního vysílání totiž jsou aktivity, které jsou při přípravě i samotném vysílání prováděny cíleně, organizovaně a pravidelně. Získání a zveřejnění předmětné informace zahrnovalo množství na sebe navazujících kroků počínaje procházením policejních internetových stránek přes investigativní aktivity pro opatření doplňujících informací o chování subjektu údajů od třetích osob, vlastní úvahu nad charakteristikou způsobu přenosu nemoci či další pátrání ve snaze ji přesně označit až po technické zpracování reportáže, zařazení do programu zpravodajské relace a odvysílání. V tomto procesu zakončeném zveřejněním diagnózy subjektu údajů v celorepublikovém vysílání v tzv. *prime time* není pro nahodilost žádný prostor. Že byla citlivá informace odvysílána jen jednou, neznamená, že neoddělitelným předpokladem pro takové uveřejnění nebyla systematická práce přičitatelná správci. Na předmětný skutek je třeba pohlížet komplexně, neboť činnosti předcházející zveřejnění ve vysílání bytostně a neoddělitelně souvisejí s finálním počinem. Nahodilé zveřejnění údaje o zdravotním stavu osoby by takové pozadí nemělo.

5. Vynaložení veškerého úsilí, které bylo možno požadovat ve smyslu § 46 zákona č. 101/2000 Sb., neznamená jakékoliv úsilí, které správce osobních údajů vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit. Jako liberační důvod tudíž nemůže postačovat fakt, že uzavřená smlouva o dílo obsahovala detailní popis postupu od převzetí specifického odpadu od správce další odpovědnou osobou

V rozsudku čj. 11A 107/2013-28 ze dne 26. května 2014 Městský soud v Praze především uvedl, že pravidla ochrany osobních údajů platí v zásadě za všech okolností. Není podstatné, zda se jedná o soubor osobních údajů zpracovávaných výpočetní technikou nebo například o soubor listin, na nichž jsou osobní údaje uvedeny. Vynaložení veškerého úsilí, které bylo možno požadovat ve smyslu § 46 zákona č. 101/2000 Sb., pak 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. Došlo-li tedy k uzavření

smlouvy o dílo, týkající se dalšího bezprostředního nakládání s předměty, obsahujícími citlivé osobní údaje, přičemž uvedené předměty byly posléze nalezeny na veřejné skládce, která jistě není běžným místem pro uložení dokumentů s osobními údaji, jednoznačně nelze hovořit o vynaložení veškerého úsilí, aby nedošlo k neoprávněnému přístupu k těmto údajům. Pro splnění podmínek ochrany osobních údajů a případnou liberaci v případě nějakého konfliktu ve vztahu k ochraně osobních údajů je třeba mít na paměti, že dosažení, respektive prokázání liberačního důvodu není samo sebou, a že tento důvod musí být správcem či zpracovatelem nejen jednoznačně prokázán, ale také musí vycházet z toho, že ne jakákoliv opatření, ale opatření maximálně možná mohou být za liberační důvod uznána. Pro případnou liberaci tudíž nemůže postačovat fakt, že uzavřená smlouva o dílo obsahovala detailní popis postupu od převzetí specifického odpadu od správce další odpovědnou osobou. To lze považovat za jedno z opatření, zajišťující ochranu osobních údajů ve smyslu ustanovení § 13 zákona č. 101/2000 Sb., nicméně přesto došlo k incidentu, tedy úniku osobních údajů mimo sféru správce. Došlo tudíž k zapracování pokynů do smluvního textu, ale nedošlo prokazatelně k jejich dostatečnému provedení, které by fakticky zabránilo úniku osobních údajů, což znamená, že správce nevynaložil veškeré úsilí, které bylo možné požadovat, přičemž nepochybně existovaly další možnosti, jak by bylo možno postupovat, aby se zveřejnění osobních údajů zabránilo. Účelem povinnosti podle ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. není primárně to, aby správce osobních údajů přijal formálně bezpečnostní předpisy, ale zajištění toho, aby nedošlo k neoprávněnému přístupu k osobním údajům, a tím naplnění práva subjektu údajů na ochranu jeho soukromí.

S ohledem na shora uvedený výklad ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. Městský soud v Praze vyslovil názor, že použití pojmů „nepřijme nebo neprovede“ nic nemění na charakteru odpovědnosti správce za nesplnění povinnosti podle uvedeného právního ustanovení. Uvedení bezpečnostních opatření v život tak, aby plnila svůj smysl a účel, nelze jiným způsobem než jejich přijetím a provedením, přičemž tyto dva pojmy současně plně pokrývají a vystihují všechny možné způsoby naplnění účelu bezpečnostních opatření. S bezpečnostními opatřeními nelze dělat nic jiného než je přijmout a provést; dikce ustanovení § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. pak nedává prostor k tomu, aby bylo prokazováním preventivního jednání popřeno, že k naplnění skutkové podstaty deliktu došlo, byl-li přístup neoprávněné osoby k osobním údajům nepochybně prokázán.

● REGISTRACE

Trend nárůstu počtu registračních oznámení pokračoval i v roce 2014. V tomto roce Úřad přijal 7686 oznámení o zpracování podle § 16 zákona č. 101/2000 Sb. Oproti minulému roku se jednalo o 15% nárůst. Vedle registračních oznámení Úřad vyřídil v letošním roce rovněž 845 žádostí týkajících se změny či doplnění stávajících registrací, které se nejčastěji týkaly adresných údajů, doplnění rozsahu zpracovávaných osobních údajů, kategorií subjektu údajů, doplnění účelů zpracování a míst zpracování. Vedle posuzování přijatých registračních oznámení vydává Úřad rozhodnutí o zrušení registrace podle § 17a odst. 2 zákona č. 101/2000 Sb. V letošním roce bylo zrušeno celkem 132 zpracování na žádost správce, nejčastěji z důvodů zániku či sloučení společnosti, zrušení podnikatelské činnosti nebo ukončení zpracování osobních údajů. Jednalo se o nárůst 27 %. Informace o zrušených registracích Úřad zveřejňuje ve Věstníku.

V případech, že oznámení neobsahuje všechny náležitosti, které jsou nezbytné pro samotné posouzení zpracování, je správci zaslána výzva k doplnění informací. V roce 2014 Úřad zahájil celkem 1001 řízení o registraci podle § 16 odst. 4 zákona č. 101/2000 Sb. Z velké části se řízení týkala zpracování prostřednictvím kamerových systémů se záznamovým zařízením, zpracování citlivých údajů, zpracování osobních údajů bez jasného právního titulu atd. Pokud v rámci tohoto řízení vznikne, resp. trvá důvodná obava z porušení zákona, zahajuje Úřad správní řízení ve smyslu § 17 zákona č. 101/2000 Sb., jehož závěrem může být i rozhodnutí o nepovolení oznámeného zpracování. V roce 2014 bylo takové řízení zahájeno u celkem 131 podaných oznámení o zpracování, což představuje nárůst oproti loňskému roku o 31 %.

Nejčastěji oznamovaným druhem zpracování, podobně jako v letech minulých, bylo zpracování osobních údajů prostřednictvím kamerových systémů se záznamovým zařízením (cca 21 % ze všech podaných oznámení). Celkem je v registru zpracování osobních údajů zapsáno 13 711 subjektů, které podaly oznámení o zpracování osobních údajů kamerovými systémy (rozdíl oproti součtu jednotlivých let v tabulce je dán tím, že jeden subjekt mohl podat oznámení ve více letech). V roce 2014 podalo oznámení 2716 subjektů, což je nárůst oproti roku 2013 o 12 %.

Tabulka 1

Přehled počtu subjektů, které podaly oznámení o zpracování osobních údajů, ke kamerovým systémům

| Rok | Počet subjektů |
|---------------|----------------|
| do 2005 | 32 |
| 2006 | 386 |
| 2007 | 890 |
| 2008 | 1399 |
| 2009 | 1255 |
| 2010 | 1268 |
| 2011 | 1505 |
| 2012 | 1887 |
| 2013 | 2373 |
| 2014 | 2716 |
| Celkem | 13 711 |

Kamery v automobilech

Úřad zaznamenal zvýšený počet oznámení fyzických osob hodlajících zpracovávat osobní údaje prostřednictvím kamer umístěných uvnitř automobilu a monitorujících prostor před jedoucím automobilem za účelem následného využívání získaných záběrů jako důkazního materiálu pro případ mimořádné události (nehody nebo jiné pojistné události). Takové zpracování je z hlediska zásahu do práva na ochranu soukromí a osobních údajů subjektů údajů z pohledu Úřadu považováno za nerizikové (oproti stacionárním kamerovým systémům například není způsobilé zajistit provozovateli pravidelný přehled o výskytu a chování lidí v konkrétním prostoru ani nezasahuje do práva na obydlí) a současně se nepředpokládá využití záznamu z kamerového systému v motorovém vozidle za jiným účelem (např. zveřejnění), nemusí být předmětem předběžného šetření dozorového orgánu, a tudíž se na takové zpracování oznamovací povinnost dle § 16 zákona č. 101/2000 Sb. vztahovat nebude.

Zpracování prostřednictvím biometrických technologií

V souvislosti s rozvojem informačních technologií se stále častěji objevují zvláštní způsoby zpracování prováděné prostřednictvím těchto nových technologií. Týká se např. technologií zabezpečujících vstup do režimových pracovišť, nejčastěji na základě snímání otisku prstů, duhovky oka či krevního řečiště. Právě posledně jmenovaná biometrická technologie se v praxi začíná prosazovat ve stále větší míře. Úřad zaznamenal několik dotazů a oznámení o zpracování společností hodlajících zavést tuto technologii za účelem zabezpečení vstupu do chráněných prostor. Vstupní systém obsahuje biometrický snímač, který dokáže rozpoznat jednotlivé osoby na základě obrazu krevního řečiště dlaně. Pokud je vzniklý obraz krevního řečiště dále automaticky v systému konvertován do biometrické šablony, která je redukcí biometrického obrazu, a představuje pouze číselnou veličinu, ze které nelze biometrický údaj zpětně rekonstruovat, nejedná se o zpracování citlivých údajů. Biometrická šablona – bezrozměrný číselný kód je „pouze“ osobním údajem ve smyslu stanoviska Úřadu č. 3/2009.

V letošním roce Úřad rovněž zaznamenal několik oznámení týkajících se použití dynamického biometrického podpisu. Konkrétně se jedná o údaje týkající se jeho velikosti a dynamiky, tlaku při podepisování a časové délce podpisu, a to za účelem zajištění a uplatnění právních nároků v případě pochybností nebo sporů o pravost podpisu. Úřad vydal stanovisko č. 2/2014 k problematice jeho využití v souvislosti s aplikací zákona č. 101/2000 Sb. Z hlediska plnění oznamovací povinnosti je podstatné, že zpracování dynamického biometrického podpisu podléhá oznamovací povinnosti, jedná se o zpracování citlivých údajů, a je tedy potřeba získat výslovný souhlas subjektu údajů s jeho zpracováním.

Zpracování osobních údajů nezbytných pro využívání zdrojů z evropských fondů

Vzhledem k tomu, že poměrně čteně přicházejí oznámení o zpracování nezbytných osobních údajů v souvislosti s realizací projektů využívajících zdrojů z evropských fondů, jsou oznamovatelé upozorňováni na uplatnění výjimky z oznamovací povinnosti (blíže na webu Úřadu, rubrika Názory Úřadu / Na aktuální téma ze dne 24. 2. 2014), a to vzhledem k tomu, že evropská nařízení jsou v členských státech přímo aplikovatelnými právními předpisy, a lze tedy na zpracování nezbytných údajů v souvislosti s řešením takových projektů uplatnit výjimku dle § 18 odst. 1 písm. b) zákona č. 101/2000 Sb.

Zpracování osobních údajů cestujících osob dopravními podniky

Dopravní podniky jednotlivých měst oznamují Úřadu zpracování spočívající v instalaci kamerového systému do vozidel MHD, případně kamer zabírajících prostor před dopravním prostředkem za účelem vyšší ochrany zaměstnanců před napadením, ochranou majetku před poškozováním a vandalismem, zvýšení bezpečnosti cestujících a prevence, při využití záznamu jako důkazního materiálu o trestné činnosti nebo o způsobení škody, případně k objasnění příčin a dořešení mimořádných událostí. Z pohledu zákona č. 101/2000 Sb. je třeba říci, že plošné zavádění kamer do MHD v zásadě přípustné není a vždy je třeba postupovat v souladu s principem proporcionality a minimalizovat zásah do soukromí, v tomto případě cestujících.

V souvislosti s činností dopravních podniků se objevují zpracování, jejichž podstatou je pořizování audiozáznamů při výkonu přepravní kontroly za účelem zvýšení ochrany zaměstnanců přepravní kontroly při případných konfliktních situacích, ke kterým může dojít při řešení zjištěného porušení smluvních přepravních podmínek ze strany cestujících v průběhu přepravní kontroly a rovněž pro ověření správnosti postupu zaměstnance přepravní kontroly. Pokud se jedná pouze o incidenční záznam, a nikoliv o plošné nahrávání každé situace, pak je v takovém případě možné zpracování provádět bez souhlasu na základě ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Narušení ochrany osobních údajů (tzv. data breaches)

S účinností zákona č. 127/2005 Sb., o elektronických komunikacích, byla Úřadu svěřena kompetence související s přijímáním a posuzováním zaslaných oznámení týkajících se narušení ochrany osobních údajů (tzv. data breaches).

V roce 2014 obdržel Úřad dvě oznámení týkající se narušení bezpečnosti osobních údajů. První oznámení se týkalo zpřístupnění souboru s osobními údaji přibližně 380 000 zákazníků jedné neoprávněné osobě. Vzhledem k charakteru dat uplatněným technicko-organizačním opatřením a tomu, že data již nebyla v držení neoprávněné osoby, neuplatnil Úřad jiná opatření.

Druhé oznámení se týkalo využití osobních údajů přibližně 300 zákazníků bývalými společníky po jejich odchodu ze společnosti. Vzhledem k tomu, že oznamovatel zasažené subjekty informoval, neuplatnil Úřad jiná opatření.

Cloud computing

V poslední době Úřad obdržel několik oznámení o zpracování osobních údajů s využitím cloud computingu. Při posuzování takových oznámení je zásadní, zda je oznamovatel v pozici poskytovatele cloudových služeb, nebo jeho zákazníka. Vzhledem k tomu, že oznámení o zpracování osobních údajů podávají také společnosti poskytující cloud computing (cloudové služby), je nutné uvést, i s odkazem na stanovisko WP29 č. 5/2012 ke cloud computingu (je dostupné i v češtině), že obvykle je poskytovatel cloudových služeb v pozici zpracovatele. Oznámení o zpracování osobních údajů podává ve smyslu § 16 odst. 1 zákona č. 101/2000 Sb. vždy pouze správce. V tomto případě je správcem zákazník poskytovatele cloudových služeb; správce je povinen přijmout taková opatření, aby nemohlo dojít k zneužití osobních údajů. Vzhledem k charakteru zpracování osobních údajů však lze v některých případech uplatnit výjimku z oznamovací povinnosti např. u docházkového systému, v personalistice apod. zajišťované tímto způsobem.

• PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Ustanovení § 27 zákona č. 101/2000 Sb. upravuje zvláštní režim pro předání osobních údajů z České republiky do třetích zemí. Třetí zemí se v tomto smyslu rozumí všechny země mimo Evropský hospodářský prostor. Účelem a smyslem tohoto ustanovení je zajištění ochrany osobních údajů subjektů údajů, které mají být předány a následně zpracovávány ve třetích zemích. V zásadě mohou být osobní údaje předávány do země mimo Evropskou unii, pokud tato země zaručuje „odpovídající úroveň ochrany“. Odpovídající úroveň ochrany ve třetí zemi mohou zajišťovat buď obecné právní předpisy, nebo odvětvová pravidla dotyčné třetí země, nebo tuto ochranu může garantovat sám správce (vývozce údajů) prostřednictvím odpovídajících ochranných opatření, která zajistí, že úroveň ochrany předávaných osobních údajů bude v zemi příjemce srovnatelná se standardy ochrany obsaženými v zákoně č. 101/2000 Sb. Takové záruky mohou vyplývat zejména ze smlouvy mezi správcem a příjemcem dat, jejíž nedílnou součástí budou standardní smluvní doložky vytvořené rozhodnutím Evropské komise. Pokud správce osobních údajů zvolí variantu vytvoření jiných druhů odpovídajících ochranných opatření, musí tato svá vlastní ochranná opatření „obhájit“ v rámci povolovacího řízení podle § 27 odst. 4 zákona č. 101/2000 Sb.

Jako nejefektivnější a svým způsobem nejjednodušší nástroj k vytvoření takovýchto garancí se osvědčily tzv. standardní smluvní doložky, které byly určeny pro použití v privátním sektoru a definovány několika rozhodnutími Evropské komise.

Pro případ předání osobních údajů zpracovateli osobních údajů do třetích zemí jsou určeny standardní smluvní doložky, které jsou přílohou rozhodnutí Evropské komise ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES.

Pro případ předání osobních údajů novému správci osobních údajů do třetích zemí lze použít buď standardní smluvní doložky obsažené v rozhodnutí Evropské komise ze dne 15. června 2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice Evropského parlamentu a Rady 95/46/ES; nebo standardní smluvní doložky obsažené v rozhodnutí Evropské komise ze dne 27. prosince 2004, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavádění alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí.

V případě, kdy správce osobních údajů uzavře s příjemcem osobních údajů ve třetí zemi smlouvu, jejíž součástí budou standardní smluvní doložky podle některého z výše uvedených rozhodnutí Evropské komise, proběhne předání osobních údajů v režimu ustanovení § 27 odst. 2 zákona č. 101/2000 Sb. „na základě rozhodnutí orgánu Evropské unie“. V takovém případě správce nemusí žádat Úřad o povolení ve smyslu § 27 odst. 4 zákona č. 101/2000 Sb.

Vývozci osobních údajů se často obracejí na Úřad s otázkou, zda lze upravovat text standardních smluvních doložek a za jakých podmínek bude i změněný text považován za standardní smluvní doložky. Pokud budou zachovány právní záruky dané původním textem doložek, lze pozměněný text považovat nadále za standardní smluvní doložky. Zároveň je třeba poznamenat, že Úřad neposkytuje posudky, které by potvrzovaly, že předložená smlouva splňuje náležitosti standardních smluvních doložek.

Na žádost společnosti Microsoft o posouzení smlouvy se tohoto úkolu v jednom případě zhostila pracovní skupina WP29, poradní orgán Evropské komise pro otázky ochrany osobních údajů. Avšak tento případ se ukázal ve výsledku problematický vzhledem k tomu, že skupina WP29 je poradním orgánem Evropské komise a nemá v kompetenci vydávání posudků privátním korporacím, a zároveň vyvolal vlnu žádostí o posouzení smluv ze strany dalších korporací. Takové posudky mohou vydat pouze jednotlivé národní dozorové úřady. Proto vznikla potřeba stanovit procedurální pravidla, podle kterých budou dozorové úřady v takových případech postupovat. WP29 v současné době pracuje na vytvoření Kooperační procedury zhodnocení, zda je předloženou smlouvu možné považovat za standardní smluvní doložky podle rozhodnutí Evropské komise. V tomto okamžiku lze říci jen tolik, že tato procedura se vytváří podle vzoru kooperační procedury schvalování závazných podnikových pravidel. Přitom bude na rozhodnutí společnosti, zda si vyžádá u konkrétního dozorového úřadu zhodnocení upravených standardních smluvních doložek touto procedurou nebo jiným způsobem; rovněž požádaný dozorový úřad bude samozřejmě moci žádost odmítnout.

Úspěšná aplikace stávajících standardních smluvních doložek určených pro privátní sektor vyvolala iniciativu směřující k vytvoření vzorových smluvních doložek pro předání osobních údajů mezi veřejnými institucemi Evropské unie a veřejnými institucemi třetích zemí. Této iniciativy se chopil úřad Evropského komisaře pro ochranu osobních údajů (EDPS), podle jehož analýzy mezinárodní smlouvy zpravidla neobsahují evropské zásady ochrany osobních údajů, nanejvýš obecné ustanovení o adekvátní ochraně osobních údajů. EDPS vypracoval návrh vzorových smluvních doložek pro předání osobních údajů mezi veřejnými institucemi v Evropské unii a ve třetích zemích. Je jasné, že jakkoliv veřejná instituce vyjádří svůj záměr řídit se danými vzorovými smluvními doložkami, nikdy pro ni nebudou striktně právně závazné, takže se nemohou stát standardními smluvními doložkami ve výše uvedeném smyslu. Cílem EDPS je tedy prostřednictvím těchto vzorových smluvních doložek vytvořit obecné doporučení, podle kterého by se orgány veřejné moci mohly řídit a které by mohlo být využíváno při formulaci mezinárodních dohod.

Cestou vytvoření vzorových smluvních doložek se ubírá také snaha nějakým způsobem ošetřit případy, kdy do třetích zemí předává osobní údaje zpracovatel osobních údajů, klasicky v rámci poskytování cloudových služeb. V současné chvíli vyhlásila skupina WP29 veřejnou konzultaci ke stanovisku skupiny WP29 č. 1/2014 „Návrh Ad hoc standardních smluvních doložek pro předání evropským zpracovatelem dílčím zpracovatelům do třetích zemí“ (WP 214). Této konzultace se účastní mj. Konfederace evropských organizací ochrany dat (Confederation of European Data Protection Organisations, CEDPO) a neziskové asociace European Digital Rights (EDRi) a European CIO Association (EuroCIO). Návrh doložek vychází z konkrétního textu upravených „standardních smluvních doložek“ uzavřených mezi španělským zpracovatelem a dílčími zpracovateli ve třetích zemích, na jehož základě a na základě smlouvy uzavřené mezi správcí osobních údajů a uvedeným španělským zpracovatelem španělský dozorový úřad autorizoval předání do třetích zemí.

Je pochopitelné, že Evropská komise v době přípravy nového nařízení nehodlá přijmout svým rozhodnutím za standardní ani výše zmíněné vzorové doložky pro předání osobních údajů mezi veřejnými institucemi Evropské unie a veřejnými institucemi třetích zemí, ani vzorové doložky pro předání evropským zpracovatelem dílčím zpracovatelům do třetích zemí. Přesto tyto doložky jsou dalším krokem k rozšíření evropských standardů ochrany osobních údajů i do dosud opomíjených oblastí.

Adekvátní ochranu osobních údajů v případě předání osobních údajů do Spojených států amerických bylo dosud možné zajistit rovněž tím způsobem, že se příjemce osobních údajů ve Spojených státech přihlásil k dodržování zásad systému „bezpečný přístav“ („Safe Harbor“), definovanému rozhodnutím Evropské komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států amerických.

Odhalení sledovacích programů Spojených států (PRISM), v rámci kterých docházelo k plošnému předávání údajů občanů Evropské unie prostřednictvím internetových společností americkým veřejným orgánům, však vyvolalo v rámci Evropské unie diskusi o tom, zda institut „bezpečného přístavu“ je v současné době schopen zajistit efektivní ochranu osobních údajů ve Spojených státech amerických.

K problémům spojeným s předáváním osobních údajů do USA se vyslovila Evropská komise ve svém Sdělení Evropskému parlamentu a Radě ze dne 27. listopadu 2013 („Obnovení důvěry v toky údajů mezi EU a USA“) a dále také Usnesení Evropského parlamentu ze dne 12. března 2014 o programu agentury NSA (USA) pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů Evropské unie a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí (2013/2188(INI)). Podle Sdělení Evropské komise mnoho společností zapsaných na seznamu bezpečného přístavu jeho zásady v praxi nedodržuje. Usnesení Evropského parlamentu pak v bodě 38 přímo konstatuje, že „zásady nástroje Safe Harbor neposkytují za stávajících okolností dostatečnou ochranu občanům Evropské unie, a proto by tato předávání měla probíhat na základě jiných nástrojů, například smluvních doložek nebo závazných podnikových pravidel, pokud tyto nástroje stanoví konkrétní záruky a mechanismy ochrany a nejsou obcházeny jinými právními rámci.“

Úřad proto doporučuje správcům osobních údajů zajistit předání osobních údajů do Spojených států amerických, které se ukáže být nezbytně nutným k naplnění stanovených účelů, smlouvou, jejíž součástí budou příslušné standardní smluvní doložky. Tyto standardní smluvní doložky zajišťují v současné době nepochybně lepší úroveň ochrany osobním údajům ve třetí zemi než institut „bezpečného přístavu“.

Neošetří-li správce předání osobních údajů do třetí země s nedostatečnou ochranou osobních údajů standardními smluvními doložkami nebo jiným způsobem podle § 27 odst. 2 zákona č. 101/2000 Sb., musí požádat o povolení k předání osobních údajů do třetích zemí podle § 27 odst. 4 zákona č. 101/2000 Sb.

Úřad přijal za rok 2014 celkem 40 žádostí o povolení k předání osobních údajů do třetích zemí. V osmi případech Úřad věc odložil, a to zpravidla z důvodu, že žadatel dal nakonec přednost ošetření předání smlouvou, jejíž součástí jsou standardní smluvní doložky.

Z 30 v roce 2014 vydaných povolení (dvě žádosti jsou v řízení) bylo opět nejčastějším právním titulem, na jehož základě Úřad povolení vydal, ustanovení § 27 odst. 3 písm. b) zákona č. 101/2000 Sb., neboť žadatel vytvořil ve třetí zemi dostatečné zvláštní záruky ochrany osobních údajů, a to vždy prostřednictvím schválených závazných vnitropodnikových pravidel (Binding Corporate Rules, BCR). Stalo se tak v osmnácti případech. Institutem závazných vnitropodnikových pravidel se poměrně podrobně zabývala výroční zpráva za rok 2013. Sedmkrát bylo právním titulem povolení ustanovení § 27 odst. 3 písm. a), tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů. Čtyřikrát bylo právním titulem povolení

ustanovení § 27 odst. 3 písm. e), tedy předání údajů nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů.

Geograficky šlo jako obvykle především o předání do Spojených států amerických, Indie a oblasti jihovýchodní Asie a Pacifiku (Japonsko, Čína, Filipíny, Austrálie) a také ve dvou případech cestovních kanceláří do Turecka a Egypta.

• SCHENGENSKÁ SPOLUPRÁCE

Obdobně jako v předchozích letech se také v roce 2014 Úřad aktivně podílel na činnostech spojených s dozorem v oblasti schengenské spolupráce týkající se především sdílení osobních údajů v mezinárodních informačních systémech. V postavení dozorového orgánu České republiky Úřad zajišťoval dohled nad dodržováním relevantní právní úpravy, a to primárně za účelem ochrany osobních údajů subjektů, jejichž data jsou zpracovávána v rámci schengenského prostoru. Stěžejní postavení mezi informačními systémy na evropské úrovni zaujímá Schengenský informační systém druhé generace (SIS II), který eliminuje bezpečnostní rizika související s volným pohybem osob a věcí uvnitř Schengenského prostoru. V agendě zpracovávané Úřadem rovněž figuruje dohled nad řádným zpracováváním osobních údajů ve Vízovém informačním systému (VIS), Celním informačním systému (CIS) či EURODACu (mezinárodní systém pro evidenci otisků prstů žadatelů o azyl či ilegálních přistěhovalců). S ohledem na uvedené se Úřad tomuto tématu věnoval jak výkonem vlastní dozorové činnosti na národní úrovni, tak i v rámci jednání příslušných pracovních skupin zahrnujících zástupce jednotlivých členských států Evropské unie, resp. států podílejících se na využívání příslušného informačního systému.

• Kontroly informačních systémů a jejich výsledky

Jelikož zpracování dat subjektů ve výše zmíněných systémech může potenciálně ohrozit jejich práva včetně práva na řádné zpracování osobních údajů, Úřad se zaměřuje na systematické prověřování daných informačních systémů. V roce 2014 tak došlo k vnitrostátní kontrole orientované na přechod na nový Schengenský informační systém druhé generace. Kontrola prověřila především dodržení všech bezpečnostních aspektů operací s osobními daty subjektů, jež provádí Policie ČR jako pověřený správce osobních údajů v národní součásti Schengenského informačního systému.

Z poznatků získaných v průběhu kontroly a na základě vyžádaných dokladů a dokumentů byl zjištěn skutkový stav a následně provedeno právní hodnocení, jak ve věci přechodu ze SIS 1+ na systém SIS II, tak hodnocení postupu při vyřizování žádosti konkrétní dotčené osoby a prověření zpracování jejích osobních údajů v SIS. Právní posouzení vycházelo z příslušných vnitrostátních právních předpisů v oblasti ochrany osobních údajů i ze závazných předpisů Evropské unie týkajících se zpracování osobních údajů v informačních systémech provozovaných v rámci schengenské spolupráce. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb., opatření k nápravě tedy nebyla uložena. Inspektorka Úřadu v závěru kontrolního protokolu kontrolovanému doporučila vypracovat aktualizovanou bezpečnostní studii národní součásti SIS II a gestoru problematiky (Policejnímu prezidiu ČR), aby při vyřizování žádostí přímo vyhledával žádosti dotčené osobní údaje v systému a ve spise výsledek úkonu dokumentoval tak, aby byla zajištěna přezkoumatelnost postupu k úkonu oprávněného subjektu, včetně zachování informace o osobních údajích dotazovaných na základě žádosti v národní součásti SIS II.

Úřad dále prověřil činnost Ministerstva zahraničních věcí v postavení jednoho ze správců osobních údajů v souvislosti se zpracováním osobních údajů ve Vízovém informačním systému (dále také „VIS“), mimo jiné kontrolou Velvyslanectví v Káhiře. Smyslem VIS je především výměna vízových údajů mezi členskými státy s cílem zlepšit provádění společné vízové politiky a konzultací spolupráce. Ačkoli nebylo v tomto ohledu kontrolou shledáno porušení povinností

vyplývající z zákona č. 101/2000 Sb. Ministerstvem zahraničních věcí, Úřad přesto upozornil na problematický aspekt zpracování osobních údajů. Jde zejména o využívání outsourcingových služeb soukromých společností. Jmenované společnosti provádějí příjem žádostí o udělení schengenských víz včetně skenování otisků prstů žadatelů z odlehlých míst teritoriálně velkých států a následnou distribuci dat společně s osobními a citlivými údaji na zastupitelské úřady České republiky. Ministerstvo zahraničních věcí je dosud zapojeno do činnosti těchto tzv. vízových center jen v Ruské federaci. V průběhu kontroly byl z otevřených zdrojů zjištěn záměr rozšířit uvedenou spolupráci se soukromými společnostmi i do dalších států, konkrétně Číny a též do oblasti severní Afriky. Jelikož se uvedené společnosti nacházejí v postavení zpracovatele osobních údajů, musí Ministerstvo zahraničních věcí přistoupit k důslednému dodržování povinností plynoucích z ustanovení § 6 zákona č. 101/2000 Sb. a uzavřít s těmito subjekty smlouvu o zpracování osobních údajů. Největší pozornost je přitom nutné věnovat zárukám zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů zpracovávaných ve VIS a následné kontrolní činnosti.

V neposlední řadě prošel kontrolou rovněž Celní informační systém, jehož účelem je zejména napomáhat předcházení, šetření a odhalování operací, které jsou v rozporu s celními nebo zemědělskými předpisy Evropské unie nebo jsou závažnými porušeními vnitrostátních předpisů členských států Evropské unie. Mezi jeho součásti patří i speciální identifikační databáze celních spisů (FIDE). Se závěry kontroly je možné se seznámit v části výroční zprávy Z kontrolní činnosti Úřadu.

• Judikatura

Úřad soustavně zabezpečoval informovanost o aktivitách a novinkách ve vztahu k schengenské spolupráci, například zajišťováním informačních kampaní. Ačkoli obecné seznamování dotčených orgánů probíhalo bez problémů, jisté nedostatky byly zaznamenány v souvislosti s povědomím veřejnosti, odbornou nevyjímaje, o některých procesních aspektech zpracování dat v informačních systémech. Uvedené prokazuje zejména aktuální judikatura Nejvyššího správního soudu.

Nejvyšší správní soud v rozsudku ze dne 25. června 2014, č.j. 1 Aps 15/2013-33 mimo jiné konstatoval: „*Ten, o němž je veden záznam v Schengenském informačním systému (SIS), musí v případě nesouhlasu s tímto záznamem nejprve podat žádost o výmaz či opravu záznamu v SIS u Policie České republiky, Policejního prezidia (§ 84 zákona č. 273/2008 Sb., o Policii České republiky). Na tom nic nemění ani to, že záznam samotný byl učiněn nikoliv českou stranou, ale naopak jiným státem Schengenského systému (čl. 106 Úmluvy k provedení Schengenské dohody ze dne 14. června 1985 mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích). Policie České republiky je povinna učinit vše, aby údaje žadatele byly vymazány, pokud snad jsou v SIS vedeny v rozporu se zákonem (čl. 106 odst. 3 a čl. 115 citované úmluvy). To platí navzdory tomu, že za jejich správnost a aktuálnost sama Policie České republiky neodpovídá (čl. 105 téže úmluvy).*“ Příklad se týkal vložení záznamu jiným členským státem, přičemž stěžovatel po vydání rozhodnutí žádal o odstranění svého záznamu v SIS II Policii České republiky. Následně podal Úřadu žádost o výmaz záznamu ze SIS II, ačkoli k danému kroku není na základě relevantní právní úpravy příslušný ani Úřad, ani Policie ČR, ani žádný jiný český orgán. Ustanovení čl. 34 odst. 2 Nařízení o SIS II (dříve čl. 106 odst. 1 Prováděcí úmluvy k Schengenské dohodě) totiž explicitně stanoví, že pouze členský stát, který záznam vložil, je oprávněn měnit, doplňovat, opravovat, aktualizovat nebo mazat zpracovávané údaje. S ohledem na

řečené žádný členský stát Evropské unie, a tedy ani Česká republika, nedisponuje pravomocí odstranit záznam, který do SIS II vložily orgány jiného členského státu. I přesto, že se Úřad podílí na šíření informací v otázkách zpracování osobních údajů v informačních systémech, v následujících letech bude účelné dále pracovat na prohloubení znalostí odborné i laické veřejnosti o sféře schengenské spolupráce.

• Počty podnětů, stížností, dotazů a jejich vyřízení

V průběhu roku 2014 Úřad obdržel celkově deset podnětů týkajících se zpracování osobních údajů v SIS II. Předmětem žádostí bylo především poskytnutí informací o zpracování osobních údajů žadatele v národní součásti SIS II, dále rovněž vyřízení požadavků na opravu či výmaz zde zpracovaných osobních údajů. Část podnětů směřovala k prošetření zamítavých rozhodnutí v rámci vízového řízení anebo řízení o povolení k pobytu v ČR. V jednom případě byl Úřad požádán o spolupráci francouzským dozorovým orgánem ve věci záznamu, který do SIS II vložil příslušný orgán České republiky. Shodně jako v předchozích letech Úřad v těchto případech spolupracoval s orgány Policie ČR.

Jde-li o otázky vízové politiky České republiky, Úřad nadále eviduje množství dotazů a žádostí spadajících do působnosti Ministerstva zahraničních věcí. Za rok 2014 jde konkrétně o 66 takových případů. Úřad při vyřizování těchto podnětů přistupoval k objasnění rozdělení pravomocí orgánů vízového sektoru, poučení o možnosti kontaktovat Ministerstvo zahraničních věcí, jakož i k osvětlení svých dohledových kompetencí.

Legislativní činnost

V roce 2014 se činnosti Úřadu zásadně dotknuly dvě nové právní úpravy:

Procesní novela zákona č. 101/2000 Sb., účinná od 1. května 2014, přijatá v návaznosti na nový kontrolní řád, uvedla dosavadní procesní pravidla pro kontrolu ochrany osobních údajů do souladu s novými postupy podle kontrolního řádu, přitom současně zohlednila definici nezávislého dozoru stanovenou směrnicí 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Novela odstranila všechna ustanovení, která byla vyhodnocena jako duplicitní s kontrolním řádem. V zákoně č. 101/2000 Sb. však bylo ponecháno výslovné zákonné oprávnění kontrolujících na přístup ke všem potřebným informacím, zejména informacím chráněným zvláštními režimy, u nichž zvláštní právo přístupu kontrolní řád neupravuje. Tato pravomoc je založena směrnicí 95/46/ES, která požaduje pro orgány dozoru jednak pravomoc přístupu k údajům, které jsou předmětem zpracování, jednak pravomoc shromažďovat veškeré informace nezbytné pro splnění dozoru. Po vzoru jiných kontrolních úřadů byla do zákona zavedena pravomoc uvážit, zda a v jakých případech je možno upustit od uložení pokuty za porušení povinností při zpracování osobních údajů. Konečně novela nastavila pravidla pro souběh kontrolního procesu nad probíhajícím zpracováním osobních údajů s dalšími dozorovými procedurami – předběžným posuzováním zpracování oznamovaných Úřadu podle § 16 zákona č. 101/2000 Sb.

Změnový zákon navazující na zákon č. 234/2014 Sb., o státní službě zařadil Úřad do výčtu ústředních správních úřadů a spolu s tím byl upraven § 2 odst. 2 zákona č. 101/2000 Sb., který s účinností od 1. ledna 2015 stanoví, že Úřad je ústředním správním úřadem pro oblast ochrany osobních údajů v rozsahu stanoveném zákonem č. 101/2000 Sb., zvláštními právními předpisy, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropské unie. Pravidla státní služby budou dopadat na většinu zaměstnanců Úřadu, předseda Úřadu je služebním orgánem a je oprávněn dávat státnímu zaměstnanci příkazy k výkonu státní služby podle zákona č. 234/2014 Sb. Zákon o státní službě výslovně stanoví, že se nevztahuje na předsedu a inspektory Úřadu, nevyřešil však důsledně, a to ani v doprovodném

zákonu, vztah Úřadu jako nezávislé dozorové instituce k vládě. Podle článku 28 směrnice 95/46/ES má být Úřad „zcela nezávislý“. Ačkoliv § 28 zákona č. 101/2000 Sb. nezávislost Úřadu deklaruje, není v ustanoveních kompetenčního zákona, mj. ukládajících úkoly ústředním úřadům, rozlišována skupina nezávislých dozorových úřadů nepodřízených vládě. Tento přetrvávající problém může definitivně vyřešit až nový kompetenční zákon.

Příkladem nevhodného zapojení Úřadu do státní správy je návrh na začlenění zástupce dozorového úřadu do mezirezortní pracovní skupiny ke Sčítání lidu, domů a bytů kolem roku 2020. Není vhodné, aby Úřad jako nezávislý dozorový úřad byl zastoupen v pracovní skupině; jako takovému mu nelze ukládat úkoly v rámci pracovní skupiny týkající se definování potřeby administrativních zdrojů dat, návrhu nových administrativních zdrojů dat, vyčíslení rozpočtových výdajů a výdajů na vlastní provedení cenzu nebo stanovení harmonogramu prací nezbytných pro dosažení těchto cílů. Odpovídajícím organizačním opatřením k zajištění náležitého promítnutí ochrany osobních údajů do návrhových prací může být předložení návrhu na provedení sčítání 2020 Úřadu k posouzení v souladu s působností Úřadu na úseku ochrany osobních údajů, a to i opakovaně.

V oblasti **připomínkování právních předpisů** se k trendům a místy problematickým otázkám zpracování údajů z uplynulých let, jako vyhodnocování dopadů do soukromí či tvorba nových státních databází, přiřadilo nově velmi populární **zveřejňování osobních údajů s deklarovaným cílem transparentnosti veřejné správy a boje proti korupci**. U tohoto trendu Úřad upozorňoval na vhodný a přiměřený způsob zveřejňování a na zákonný požadavek, aby stát pracoval s daty strukturovaně a účelně, stejně jako na skutečnost, že v řadě případů ani průběžné nebo následné zveřejňování všech údajů z veřejné správy, včetně údajů osobních, nemůže nahradit chybějící standardy a kontrolní pravidla.

Úřad poskytl konzultaci ve věci uvažované **úpravy zákona č. 159/2006 Sb., o střetu zájmů**, týkající se zejména zavedení centralizovaného vedení přehledu oznámení podle zákona č. 159/2006 Sb. a o způsobech zpřístupňování informací z takového registru veřejnosti. Důvodová zpráva ke změně zákona musí jasně vysvětlit, jaká vybraná, zákonem daná kritéria zpracování a zpřístupňování údajů považuje stát za nejúčinnější tak, aby byl naplněn účel stanovený zákonem č. 159/2006 Sb. Je vhodné přesně definovat data, která by měla být v centrálním registru (bez omezení) veřejně dostupná. Řadu údajů o působení veřejného funkcionáře je možné již dnes podle zákona č. 101/2000 Sb. zveřejnit. Oproti tomu variantu neomezené, „plošné“ publikace všech podrobných údajů a dokumentů z registru oznámení veřejných funkcionářů na internetu považuje Úřad za silně problematickou, a to i s ohledem na závěry judikátů Soudního dvora Evropské unie týkající se střetu oprávnění na informace a oprávnění na soukromí, zejm. u případů *Rechnungshof v. Österreichischer Rundfunk* a *Schecke a Eifert v. Hesensko*. Aktuální je přitom rovněž debata o způsobu realizace „práva být zapomenut“ na internetu, které nyní vydefinoval Soudní dvůr Evropské unie ve věci *Google v. Costeja*.

V několika případech zásadních nebo objemných legislativních změn Úřad zaznamenal záměr odpovědných ministerstev předkládat přímo **návrh novel právních předpisů bez vypracování věcného záměru**, aniž by byl vyhotoven podrobný rozbor problematiky a posouzení alternativního rozsahu právní regulace. Tento postup nezbavuje ministerstva povinnosti věnovat se aspektům ochrany osobních údajů ještě před vypracováním paragrafovaného znění novely.

V případě **změny zákona č. 561/2004 Sb., školský zákon**, kterou má být zaveden registr učitelů, Úřad upozornil na povinnost stanovenou legislativními pravidly vlády vyhodnotit

dopady do soukromí, které by zřízení a provoz zamýšleného registru vyvolalo. To znamená, že pro Ministerstvo školství, mládeže a tělovýchovy je dána povinnost popsat a vyhodnotit možné varianty registru: decentralizovanou, která je spojena se zpřístupněním souhrnných dat ze škol a ministerstvu by to umožňovalo pravidelně získávat aktuální statistické přehledy; variantu centralizovaného celostátního registru uchovávajících údaje o učitelích a jiných pedagogických pracovnících, která by umožnila pracovat s daty sledujícími celou pracovní kariéru učitelů. Zejména pro variantu, zahrnující centrální shromažďování a uchovávání osobních údajů z informačních systémů škol, která znamená zvýšený zásah do soukromí, je třeba vypracovat pečlivé odůvodnění potřebnosti registru pro účel plánování (personálního zabezpečení) školství.

Nejen v případě registru učitelů se Úřad domnívá, že školám mají být k dispozici konkrétní technologie splňující požadavky zpracování a ochrany osobních údajů. Souběžně je třeba řešit související otázky, jako např. vhodné napojení na systémy e-Governmentu (základní registry) a dopad záměru ministerstva na školy a jiná školská zařízení. I v tomto případě tedy Úřad poukázal na **povinnosti ministerstev metodicky usměrňovat postupy v nasazení prostředků ICT v regulovaných nebo zákonem upravených oblastech**, mj. tak, aby údaje bylo možné získávat bez zvýšené administrativní zátěže. Úřad nabízí spolupráci při definování standardů sdílení a předávání dat.

Věcný záměr zákona byl citelně postrádán u návrhu **nové právní úpravy hazardních her** předložené do připomínkového řízení Ministerstvem financí. V materiálu nebyl řádně popsán účel a sledovaný cíl evidence osob vyloučených z účasti na hazardních hrách, ani vyhodnocena jeho legitimita a přiměřenost zpracování osobních údajů. Úřad navíc upozornil na možný střet právní úpravy se zákazem rozhodování o lidech prováděným výlučně na základě automatizovaného zpracování osobních údajů, kdy by zápis do rejstříku byl pouze odvozován od jiné právní skutečnosti – pobírání sociálních dávek či úpadku. Jedná se o paušální a diskriminační řešení. Úřad má za to, že o každém člověku lze rozhodnout individuálně, na základě daných kritérií, příp. na stanovenou dobu a ve stanovené oblasti. Úřad navíc upozornil na protiústavnost celého řešení, jelikož takové automatizované opatření mělo být vyloučeno z řádného správního přezkumu.

Obdobně nedostatečně byly v materiálu zmiňovány mechanismy zpracování osobních údajů popisované v části týkající se naplňování evidence vyloučených osob údaji (vč. způsobu předávání dat z resortu Ministerstva práce a sociálních věcí), odůvodněnost vedení evidence Ministerstvem financí, rozdělení přístupů do ní. Za odůvodnění dopadů do soukromí nebylo možno ani považovat stručnou větu v důvodové zprávě ospravedlňující identifikaci v herně a kasinu tvrzením, že přístup do herny či kasina vyžadující povinnou identifikaci představuje „společenskou ochranu“ sázejících. Návrh předložený do připomínkového řízení dále ani nijak neobjasňoval, zda a jak hodlá právní úprava (i v podzákoně podobě) převzít dosavadní úpravu monitorování.

Jelikož důvodová zpráva k návrhu zákona neobsahovala popis většiny základních náležitostí zpracování osobních údajů, vznesl Úřad v připomínkovém řízení v závěru roku řadu zásadních připomínek. Ilustrativní je, že Ministerstvo financí se v materiálu „pochlubilo“ konzultací s Úřadem z května t. r., do vlastního materiálu však nepromítlo ani jediný postoj Úřadu, který byl zástupcům ministerstva na tomto jednání sdělen.

V roce 2014 se Úřad také vyjadřoval k **problematice zákona č. 106/1999 Sb., o svobodném přístupu k informacím**, kde mj. navrhoval vyjasnění úpravy zveřejňování údajů o platech,

o nichž často a zásadním způsobem rozhodovaly v poslední době soudy, stanovením zákonných hranic, aby obce nadále nebyly ve své každodenní praxi zatěžovány prováděním tzv. testu proporcionality při považování vztahu veřejného zájmu k zájmu na ochraně soukromí osob. Úřad proto Ministerstvu vnitra navrhoval zpřesnění právní úpravy v §§ 8a a 8b zákona č. 106/1999 Sb.

Za nezbytnou otázku k řešení Úřad také považuje právní úpravu modelových způsobů zveřejnění informací osobní povahy z veřejné správy. Jedná se o problém, který má závažné dopady i na soukromý sektor. V současnosti je již snad více zřejmé, že každý, kdo informace zveřejňuje, musí zvažovat vhodnost a přiměřenost technologie zveřejnění a dále související rizika týkající se zejména překročení doby potřebné pro dostupnost osobních údajů, udržení jejich aktuálnosti, přesnosti apod. Ze stávajících zákonných pravidel ochrany osobních údajů již dnes vyplývá, že povinný subjekt musí zvolit takový způsob zveřejnění, který je přiměřený povaze zveřejňovaných informací, se zvláštním zřetelem k soukromí dotčených fyzických osob.

Úřad se také vyjádřil k možnosti **zřízení informačního komisaře** nebo svěření této role nějakému úřadu. Úřad vyjádřil přesvědčení, že takový orgán by představoval určitý přínos, neboť z řady konzultací, které Úřad vyřizuje, je zjevná bezradnost povinných subjektů, především obcí. Minimálně jim by metodická a poradní činnost v oblasti přístupu k informacím mohla jednoznačně pomoci a předejít porušování zákona. Přitom z analýzy provedené Ministerstvem vnitra vyplývá, že role infokomisaře je v jiných evropských zemích celkem běžná.

Jedním z méně častých případů legislativních prací je připomínkování návrhu změny právního předpisu v průběhu kontroly vedené Úřadem. Úřadu byla předložena k vyjádření **novela vyhlášky o zdravotnické dokumentaci** s novou podobou kartičky s novorozeneckým screenin- gem. Úřad nezpochybil potřebnost novorozeneckého screeningu a nezbytnou administrativu s ním spojenou. Upozornil však, že metodický pokyn Ministerstva zdravotnictví, podle něhož se doposud postupovalo, není dostatečnou právní úpravou pro naplnění zákonného účelu a pro další uchovávání údajů. Zpracování citlivých údajů je totiž možné pouze na základě výslovné zákonné úpravy a jakákoliv podzákoná právní úprava neodůvodňuje další zpracování, vč. uchovávání vzorků, která překračují původní účel zpracování. Z tohoto důvodu Úřad uplatnil připomínky k vyjasnění právního titulu a doby dalšího uchovávání a zpracování vzorků krve.

Nevyjasněné dopady do soukromí Úřad spatřoval i v **novele čerstvého občanského zákoníku**, která od některých osob zúčastněných na fungování svěřenských fondů měla vyžadovat zápis vybraných údajů do evidence svěřenských fondů. Tvzení, že „případné dopady nicméně ve svém souhrnu nepřekračují mez únosnosti“, Úřad nepovažoval za odůvodněné.

Pozitivně Úřad hodnotí **evidenci přestupků**, jejíž zákonná podoba byla delší dobu pečlivě připravována a diskutována, na výsledné podobě zákonné úpravy je to znát. Ve vztahu k ochraně soukromí a specificky osobních údajů se při hledání rovnováhy mezi významným společenským zájmem na ochraně všech a individuálně vymezovaným právem a zájmem na ochraně vlastních osobních údajů podařilo dosáhnout přijatelného řešení. Sledovány – tedy evidovány a při projednávání brány v úvahu – budou vybrané přestupky podle zákona č. 200/1990 Sb., o přestupcích; postihuje se recidiva a pro posouzení spolehlivosti osob se budou evidovat kromě vybraných přestupků podle zákona č. 200/1990 Sb. také přestupky podle zvláštních zákonů. Současně se podařilo dosáhnout takového vymezení podmínek, že přístup do registru má být dostatečně omezen a vázán na jednoznačně vymezený důvod. Přístup oprávněných orgánů k údajům je striktně vázán na potřebu těchto údajů pro plnění konkrétního úkolu při výkonu jejich působnosti a nezakládá pravomoc je využít, pokud to pro danou věc není nezbytné.

Úřad byl příslušný také vyjádřit se výjimečně k novelizaci právní úpravy, která nepodléhá jeho doзору. Jedná se o **úpravu dozoru nad zpracováním osobních údajů získaných zpravodajskou službou**. Úřad poukázal na její nedostatečnost, neboť stávající zákonná forma kontroly vylučuje použití standardních dozorových pravomocí při zpracování osobních údajů, avšak současně nelze srovnatelné míry kontroly dosáhnout prostřednictvím institutu individuálního povolování soudem a potřebám účinné kontroly neodpovídá ani stávající model kontroly Parlamentem České republiky. Potřeba stálého a kompetentního dozoru nad zpracováním osobních údajů je dána již jen tím, že zpravodajským službám je umožněno zpracování osobních údajů o mimořádně velkém počtu lidí, přičemž tyto údaje jsou primárně zpracovávány k jiným účelům a není v možnostech dotčených subjektů údajů druhotnému zpracování předcházet nebo mu bránit. Rovněž možnost subjektu údajů naplnit smysluplně svá práva je za stávající právní úpravy vyloučena.

Styky se zahraničím a mezinárodní spolupráce

Oblast zahraniční spolupráce v ochraně osobních údajů byla v roce 2014 ovlivněna jednak intenzivní diskusí nad sledováním elektronických komunikací občanů ve světě (téma „postsnowdenovského“ světa), jednak několika rozhodnutími Soudního dvora Evropské unie v Lucemburku přímo se týkajícími zpracování osobních údajů podle evropské směrnice 95/46/ES. Obojí mělo jisté dopady nejen do praxe národních dozorových úřadů, ale také podstatný vliv na dosud neukončenou přípravu nového evropského nařízení o ochraně osobních údajů. V řadě případů se zřetelně ukazuje globální povaha ochrany osobních údajů, a tak je přirozené, že i z tohoto důvodu byly klíčové otázky a aktuální trendy dozoru v oblasti ochrany osobních údajů v poslední době nejčastěji řešeny společně, na celoevropské úrovni, v rámci poradního orgánu Evropské komise, Pracovní skupiny pro ochranu osobních údajů (WP29).

Zasedání skupiny WP29 se pravidelně účastní předseda Úřadu a další zástupci Úřadu pracují na vybraných tématech v podskupinách WP29. V roce 2014 se stanoviska WP29 věnovala tématům porušení bezpečnosti osobních údajů, anonymizačních technik na internetu a zařízení pořizujících otisky prstů. Stanoviska obvykle vznikají na základě sdílených poznatků dozorových úřadů a konzultací se zainteresovanými subjekty, nicméně poprvé byl v rámci technologické podskupiny WP29 realizován i vlastní průzkum zaměřený na využívání cookies na webech internetových médií, soukromého sektoru (zejm. e-shopy) i veřejné správy. Zástupce Úřadu se podílel jak na tvorbě metodologie a výběru rozsahu průzkumu, tak na vlastním průzkumu, a získaná data za Českou republiku jsou prezentována ve výsledné zprávě. Úřad rovněž aktivně přispěl k několika dokumentům WP29 pro zpracování osobních údajů ve zvláštních oblastech výkonu práva a sledování elektronických komunikací za účelem národní bezpečnosti, jakož i k vyjádření ohledně zneplatnění dlouhodobě kritizované evropské směrnice o data retention. Na jednání WP29 v roce 2014 navazovala většina odborných setkání, kde zástupci Úřadu prezentovali praktické zkušenosti či stanoviska Úřadu týkající se civilního použití bezpilotních letounů (setkání organizované Evropskou komisí) či snímání veřejných prostranství kamerami a kopírování dokladů v rámci boje proti praní špinavých peněz (26. setkání zástupců úřadů pro ochranu dat, Case Handling Workshop).

Nad rámec obvyklých stanovisek a pracovních dokumentů upozornilo plénum WP29 v závěru roku na nutnost širší debaty o budoucnosti ochrany soukromí a o zachování evropských hodnot ochrany osobních údajů prohlášením zdůrazňujícím nutnost prosazovat evropské hodnoty v ochraně soukromí zejména s ohledem na postupující digitalizaci každodenního života (<http://europeandatagovernance-forum.com>).

Úřad se podílel na vytvoření společné znalostní báze WP29, vzniklé v reakci na rozsudek Soudního dvora Evropské unie ve věci „předběžné otázky“ **C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González**. Soud rozhodl, že „provozovatel internetového vyhledávače je odpovědný za zpracovávání osobních údajů, které se nacházejí na internetových stránkách zveřejněných třetími osobami“, a potvrdil existenci práva na odstranění výsledku vyhledávání (práva na výmaz, práva na tzv. de-listing či šířeji **práva být zapomenut**) také v prostředí internetu a zejména v prostředí služeb internetového vyhledávače. Zatímco na národní úrovni vydal k této otázce Úřad po projednání se zástupci průmyslu doporučení, ve věci postupu vůči globálním poskytovatelům internetových služeb, usazeným jako správci osobních údajů v jiném členském státu Evropské unie, koordinoval společný postup a výměnu poznatků s dalšími dozorovými úřady, čehož výsledkem byl společný dokument skupiny WP29 pojednávající o aplikaci závěrů soudního rozhodnutí.

Další aktuální rozhodnutí lucemburského soudu v záležitostech ochrany osobních údajů se přímo dotýká Úřadu. Ve věci **předběžné otázky C-212/13 František Ryneš v. Úřad pro ochranu osobních údajů** vystoupil na ústním jednání u Soudního dvora Evropské unie zástupce Úřadu a polemizoval zde mj. s názorem (vlády) České republiky ohledně vyjmutí určitého druhu kamerových systémů z mezí pravidel ochrany osobních údajů. V následném rozhodnutí dal soud za pravdu názoru Úřadu, že „na obrazový záznam pořízený prostřednictvím kamerového systému nainstalovaného osobou na jejím rodinném domě a zabírajícího veřejné prostranství se vztahuje směrnice o ochraně osobních údajů“ a že „nelze provozování kamerového systému, který zabírá veřejné prostranství, a je tudíž zaměřen mimo soukromou sféru osoby zpracovávající údaje, považovat za výlučně osobní či domácí činnost“.

Již od ledna 2012 se Úřad věnuje projednávání nového **evropského právního rámce ochrany soukromí** a pravidelně připomínkuje návrhy pozic (vlády) ČR na jednání v této věci. Obdobně se zástupce Úřadu věnoval **modernizaci Úmluvy Rady Evropy č. 108 – Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat** na výboru T-PD a ad hoc vytvořenému výboru (CAHDATA).

V posledních letech se Úřad častěji setkává s názory zástupců vlády České republiky, odchylnými od dlouhodobě zavedených pohledů na principy zpracování osobních údajů, a to jak na úrovni Evropské komise, tak v případech projednávaných u Soudního dvora Evropské unie. Typickým příkladem byl v závěru roku požadavek České republiky na omezení působnosti Úmluvy č. 108, ačkoliv v rámci harmonizačních prací byl dříve dostatečně vysvětlen a široce akceptován systém stávajících výjimek pro zvláštní zpracování osobních údajů. Proto Úřad oceňuje příležitost ke spolupráci, kdy je Ministerstvem zahraničních věcí ve věci tzv. soudních předběžných otázek osloven se žádostí o vyjádření a může včas přispět a usměrnit formulaci společného stanoviska.

Jednou z významných kauz roku 2014, k nimž se Úřad mohl vyjádřit, byl případ 362/14 (Scherms). Podstatou věci je tvrzení, že v právu Spojených států amerických a také v praxi neexistuje žádná výrazná **ochrana údajů předávaných do USA**. Irský soud se v rámci

pochybnosti o výkladu evropského práva v dané věci rozhodl Soudnímu dvoru Evropské unie položit předběžnou otázku ohledně problematiky předávání osobních údajů do třetích zemí upravené v článku 25 směrnice 95/46/ES. Osobní údaje v souladu s tímto článkem mohou být do třetí země předány, pokud třetí země zajišťuje odpovídající úroveň ochrany osobních údajů. Evropská komise dříve uznala, že USA tuto ochranu splňuje, členské státy Evropské unie jsou jím na základě článku 25 odst. 5 směrnice 95/46/ES vázány a již nemohou o této otázce rozhodnout samy. Lze doufat, že rozhodnutí lucemburského soudu o předběžné otázce by mohlo být zásadním argumentačním příspěvkem v debatě mezi Evropskou unií a USA o předávání osobních údajů, a to v průniku s problematikou údajů předávaných mezi Evropskou unií a USA za účelem prosazování práva (prevence, vyšetřování a stíhání trestných činů včetně terorismu), o níž vede Evropská komise od jara 2011 jednání s vládou Spojených států amerických.

Kromě spolupráce na centrální úrovni Úřad rozvíjel **vztahy bilaterální** a pokračoval v **projektech s partnerskými úřady**. Úřad dokončil ve spolupráci s partnery z Polska, Bulharska a Chorvatska projekt „Zvýšení povědomí o ochraně dat mezi zaměstnanci pracujícími v EU“ financovaný z programu Celoživotního učení / Leonardo da Vinci – Partnerství. Projekt byl zaměřen na společné evropské principy a pravidla pro ochranu osobních údajů a soukromí na pracovišti. Hlavním výstupem je příručka určená především zaměstnancům. Se zájmem se však tato publikace setkala také u zaměstnavatelů, odborů a personálních agentur.

Z nových nabídek na spolupráci Úřad přijal nabídku bulharských kolegů na přípravu projektů zaměřených na ochranu dětí. Se slovenskými kolegy se v polovině roku setkal na celodenním pracovním jednání. V rámci projektu „Právo do praxe, praxe do práva“, na němž Úřad spolupracuje s Právnickou fakultou Masarykovy univerzity v Brně, Úřad přijal studijní návštěvu z chicagské DePaul University.

V listopadu 2014 spolupořádal Úřad mezinárodní workshop, který se zabýval problematikou zpracování osobních údajů v souvislosti s odhalováním a vyšetřováním podvodů v zaměstnaneckém sektoru. Mezi účastníky workshopu byli jak zástupci z dozorových úřadů pro ochranu údajů z osmi evropských států (Polsko, Estonsko, Makedonie, Černá Hora, Albánie, Rumunsko, Bosna a Hercegovina a Česká republika), tak i zástupci českých a mezinárodních společností zabývajících se touto problematikou. Diskuse se velmi úzce dotýkala právních podmínek vyšetřování v kontextu ochrany práv vyšetřovaných zaměstnanců. Součástí programu workshopu byla část věnovaná problematice whistleblowingu.

Také v roce 2014 pokračovali zástupci Úřadu v práci ve zvláštních evropských kontrolních skupinách (a koordinačních skupinách pro dohled), v agendě Europolu, Schengenského informačního systému, Vízového informačního systému, Celního informačního systému a systému EURODAC, jakož i v hodnotící skupině schengenské evaluace.

Úřad, sdělovací prostředky a komunikační nástroje

Úřad informoval veřejnost o aktuální agendě průběžně prostřednictvím nově upravených webových stránek. Odpovědi na dotazy novinářů byly poskytovány v co nejkratší lhůtě, většinou v průběhu dne, maximálně do tří dnů. Dotazy novinářů se dosti často stávaly podnětem pro šetření prováděné Úřadem, eventuálně po doplnění faktických podkladů i podnětem ke kontrolní činnosti či správnímu řízení. V takových případech docházelo a lze předpokládat, že se vzrůstající znalostí ochrany osobních údajů či obav o ztrátu soukromí bude i v budoucnu docházet, k synergii práce Úřadu s informacemi z veřejných zdrojů.

Je zřejmé, že ani po čtrnácti letech, kdy je ochrana osobních údajů v České republice uzákoněna, nelze rezignovat na šíření znalostí o ochraně osobních údajů jako významném rysu hodnoty demokracie a je třeba trvale prosazovat hodnoty spojené s ochranou soukromí. V případech, kde je třeba uplatňovat subtilnější přístup – kupříkladu v případě nutného uvážení proporcí mezi ochranou soukromí a veřejným zájmem, je ze strany zejména některých novinářů zřetelný jednoznačný příklon k zveřejňování informací bez hlubšího rozmyslu. Ignorováním nutnosti vyvážené aplikace práva na ochranu soukromí a přístupu k informacím je občas napomáháno publikováním názorů, které ochranu osobních údajů nepovažují za nutnou.

Přehled aktivit Úřadu, nejsledovanějších případů i nejzávažnější problematiky spojené s ochranou osobních údajů je soustavně dostupný na webových stránkách v rubrikách „Tiskové zprávy a konference“ a „Názory Úřadu“. Zde jsou mimo jiné k dispozici Stanoviska Úřadu – nově za rok 2014 Stanovisko č. 1/2014 – Chytré měření a ochrana osobních údajů, Stanovisko č. 2/2014 Dynamický biometrický podpis z pohledu zákona o ochraně osobních údajů, Stanovisko č. 3/2014 – K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti a Stanovisko č. 4/2014 – Transparentní účty a ochrana osobních údajů.

ŠÍŘENÍ ZNALOSTÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

U příležitosti Dne ochrany osobních údajů 28. ledna Úřad vyhlásil 8. ročník soutěže „Moje soukromí! Nekoukat, nešťourat!“. Soutěž měla v tomto ročníku upoutat pozornost zejména na fakt, že o informacích, které jsou jednou umístěny na internetu, již nikdy nelze s jistotou říci, co se s nimi bude dále dít. Cílem bylo vzbudit zájem dětí a mladých lidí o tento problém s ohledem na to, že většinou jsou denními uživateli internetu a sociálních sítí. Výsledky soutěže byly vyhlášeny za přítomnosti doprovázejících učitelů. Jako běžná praxe se ukázalo pořádání jakéhosi předkola soutěže na jednotlivých školách, odkud na Úřad přicházejí už jen vybrané nejlepší práce. Je tedy zřejmé, že učitelé skutečně dovedou využít nabídnutou aktivitu a zprostředkovat znalosti, které lze nabyt zábavným způsobem ve prospěch širšího okruhu žáků než jen těch nejúspěšnějších a nejagilnějších. To je jistě příslibem pro eventualitu začlenění vzdělávání o ochraně osobních údajů do rámce prohlubování digitální gramotnosti. Příspěvky do soutěže jsou trvale publikovány na webových stránkách Úřadu a nejlepší výtvarné návrhy byly využity pro vytvoření předmětů propagujících odpovědné chování na sociálních sítích (tzv. placek, které mládež s oblibou nosí na svých batozích).

Jako poděkování za účast v soutěži obdrželi všichni její účastníci publikaci Web We Want, která vyšla za podpory společnosti UPC, od níž potřebné výtisky pro účastníky soutěže získal Úřad darem na konferenci České asociace elektronických komunikací, jíž poskytl záštitu předseda Úřadu.

Zájem studentů práv o ochranu osobních údajů se projevil žádostí členů společnosti ELSA Praha o setkání s odborníky. Seminář o evropských i domácích právních dokumentech i konkrétní kazuistice byl studenty navštíven v mezích kapacity, kterou nabízí zasedací místnost Úřadu, a setkal se s jejich zájmem i živou účastí v diskusi.

Zaměstnanci Úřadu jako každoročně přednášeli na velkém množství seminářů i konferencí pro státní instituce, samosprávu i podnikatelské subjekty.

Jako forma komunikace s odbornou veřejností se v práci Úřadu ustálilo pořádání kulatých stolů, například diskusní kulatý stůl na téma Inteligentní sítě a inteligentní měřicí systémy a zařízení v kontextu podmínek pro zpracování osobních údajů, jehož spolupořadatelem bylo Ministerstvo průmyslu a obchodu. Diskuse se zúčastnili i představitelé dalších zainteresovaných subjektů, především z řad výrobců a dodavatelů energií, ale i společností zabývajících se vyúčtováním dodávek energií, operátora trhu s energiemi, stejně jako zástupci výrobců a distributorů příslušných technologických řešení a rovněž představitelé akademické sféry. Zástupci oborů, od nichž je vyžadováno plnění povinností ukládaných zákonem č. 101/2000 Sb., tak dostávají přímo příležitost klást otázky přítomným expertům plynoucí z jejich každodenní praxe a pro Úřad je tak dána možnost vysvětlovat své aplikační přístupy k doзору nad dodržováním uvedeného zákona.

Na konci roku 2014 se uskutečnil seminář s mezinárodní účastí (Albánie, Bosna a Hercegovina, Černá Hora, Estonsko, Makedonie, Polsko, Rumunsko), jehož tématem bylo zpracování osobních údajů v souvislosti s odhalováním a vyšetřováním podvodů v zaměstnaneckém sektoru a problematika whistleblowingu. Spolupořadatelem byla kancelář bnt attorneys-at-law.

KNIHOVNA A PUBLIKACE ÚŘADU

Knihovnu Úřadu i nadále využívají především zaměstnanci Úřadu, ale také studenti pro své seminární a diplomové práce dotýkající se ochrany osobních údajů.

Fond této vysoce specializované knihovny se rozrostl v roce 2014 o 38 nových titulů a 5 knih získal Úřad darem.

V roce 2014 Úřad začal publikovat svou oficiální tiskovinu – Věstník výhradně v elektronické podobě. Nadále je tato publikace určena především odborné veřejnosti. Kromě náležitostí, které ukládá Úřadu zákon, což je přehled zrušených registrací, jsou ve Věstníku publikována stanoviska Úřadu, právní rozbor, informace z rozhodovací činnosti Úřadu a výsledky vybraných kontrolních šetření Úřadu. Dále se zde předkládají důležitá sdělení reflektující problémy dění ve společnosti, která nějakým způsobem souvisejí s ochranou osobních údajů. Důležitou součástí jsou dokumenty mezinárodního charakteru.

V roce 2014 vyšlo číslo Informačního bulletinu, které jednak informovalo o pořádaném kulatém stole a názorech, které zazněly k problematice chytrého měření, zejména ale soustředil pozornost na objasnění přijímání a vyřizování podnětů a stížností Úřadem v zájmu informování široké veřejnosti o postupech, které může využít, pokud se stětuje s problémy ochrany osobních údajů. Další číslo Informačního bulletinu je připravováno ve 4. čtvrtletí, aby informovalo o celosvětové konferenci o ochraně osobních údajů, o přístupech Úřadu k problematice cookies a v neposlední řadě přinese příspěvky k „žhavé“ problematice práva na zapomenutí. Je pravděpodobné, že distribuováno bude toto číslo až v roce 2015.

Úřad vydal v roce 2014 ve spolupráci s partnerskými úřady v Polsku, Bulharsku a Chorvatsku přehlednou brožuru týkající se ochrany osobních údajů zaměstnanců na pracovištích. Dvouletý projekt byl slavnostně uzavřen představením publikace veřejnosti. Předseda Úřadu RNDr. Igor Němec pozval k setkání zástupce velvyslanectví partnerských zemí, zástupce personálních agentur, odborových svazů, inspekce práce, advokátních kanceláří a médií. Publikace se setkala s ohlasem zejména v oblasti personálních agentur, odborových svazů, ale také některých odborných periodik, která se vyslovila pro možnost využití publikace v rámci své oblasti působnosti. Publikace vzbudila pozornost rovněž u zahraničních kolegů z rumunského úřadu pro ochranu osobních údajů, kteří projevíli zájem o překlad do rumunštiny. V rubrice Publikace na webových stránkách je výsledek projektu trvale dostupný všem zájemcům.

WEBOVÉ STRÁNKY ÚŘADU

Webové stránky Úřadu se proměnily jak co do grafické podoby, tak co do uživatelské přívětivosti a šíře vyhledávacích možností, a to u příležitosti přechodu na práci s redakčním systémem. Hlavní uživatelskou změnou je od začátku roku zavedená možnost vyhledávání podle konkrétních témat (např. zdravotnictví, školství, veřejná správa) nebo jednotlivých zákonných ustanovení, paragrafů zákona č. 101/2000 Sb. a dalších. Tato možnost, dostupná přímo z hlavní stránky webu, zjednodušuje a urychluje přístup k zásadním dokumentům k dané problematice. Ze statistik přístupů na jednotlivé stránky vyplynulo, že největší zájem nejširší veřejnosti je stále o problematiku kamerových systémů, což potvrdilo účelnost samostatné rubriky Kamerové systémy v rámci Poradny na hlavní stránce webu.

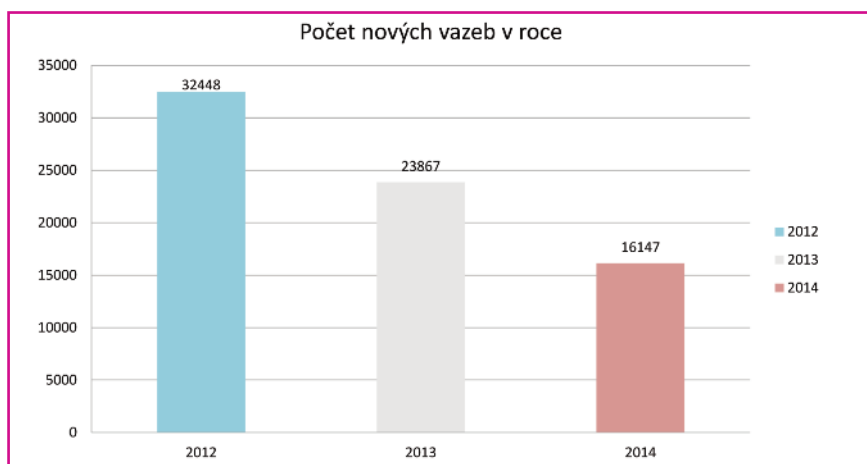
Informační systém ORG

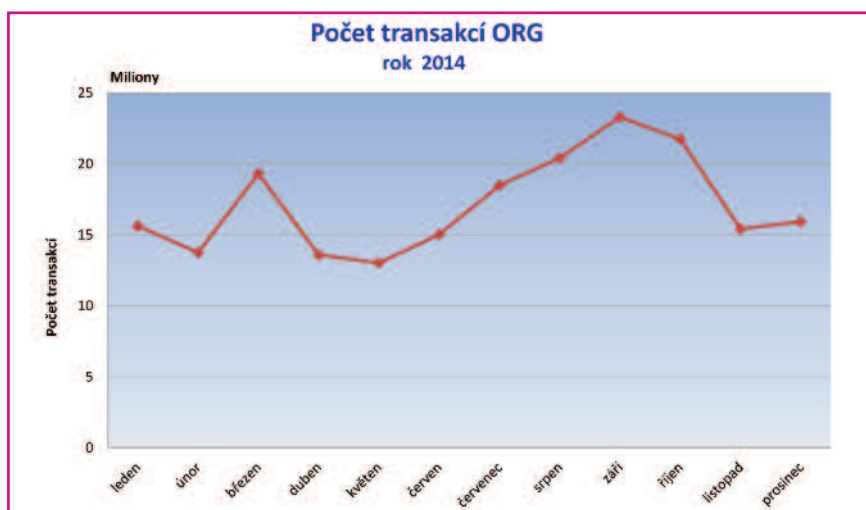
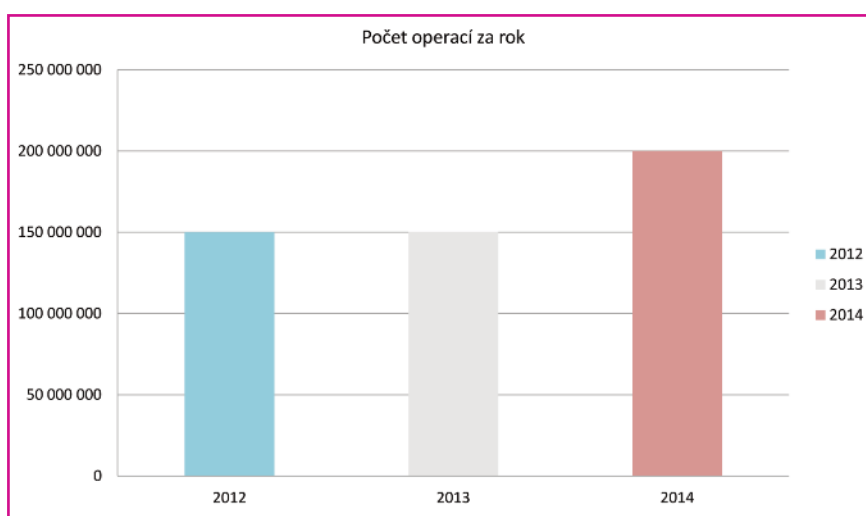
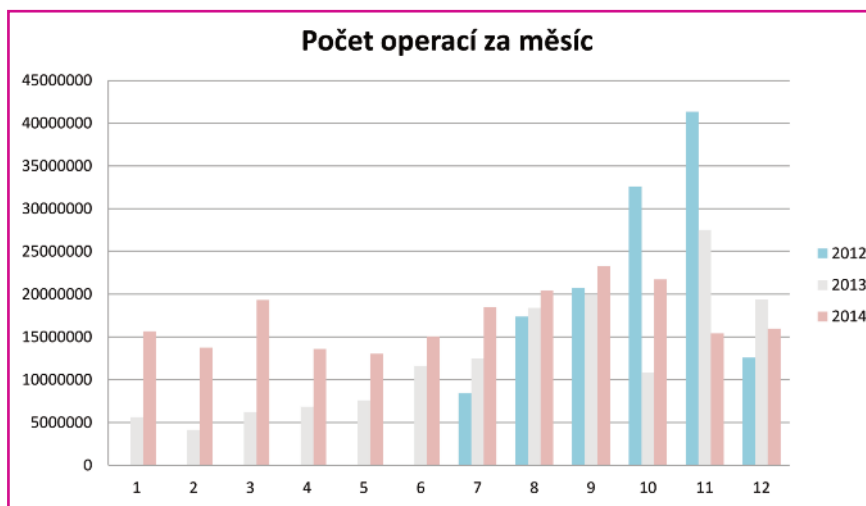
Informační systém ORG, který vytváří, vede seznam a překládá agendové identifikátory z jedné agendy do agendy druhé, je součástí „Informačního systému základních registrů“. Tento systém vznikl na základě zákona č. 111/2009 Sb., o základních registrech, a je využíván hlavně orgány veřejné správy. Zjednodušuje komunikaci mezi občany a úřady. V provozu je 24 hodin denně, 7 dní v týdnu.

Pracovníci ORG ve spolupráci s dodavatelem systému společností TESCO SW zajišťují bezchybný chod Informačního systému ORG a tím zabezpečují vysoké nároky na dostupnost služeb. Mimo jiné se podílejí i na přípravě rozvoje systému a zabezpečují administraci hardwarových prvků, spadajících pod ORG, v datových centrech.

O tom, že se systém každým dnem rozrůstá, svědčí to, že denně přicházejí požadavky na Správu základních registrů (dále „SZR“) na vytvoření nových vazeb mezi agendami a informačními systémy uživatelů. Informační systém uživatele musí být certifikován SZR a v systému zaveden. V systému je k 31. 12. 2014 zavedeno 377 agend a zhruba 72 000 vazeb na informační systémy koncového uživatele. Velké a známé agendy jsou např. Sociální zabezpečení, Zdravotní pojišťovny, Agenda řidičů, ale do skupiny agend patří např. i Ochrana chmele, Protidrogová politika nebo Podpora filmového průmyslu.

Pracovníci ORG pravidelně vytvářejí reporty o chodu a stavu systému a naplnění registru ORG daty.





Z grafů je vidět, že zatížení systému (počet operací) se během roku mění, avšak ani taková velká akce, jakou byly komunální volby v letošním roce, zdaleka nezatížila systém tak jako příprava prezidentských voleb v roce 2012, kdy se množství dat v systému ověřovalo, doplňovalo a aktualizovalo.

Pracovníci odboru ORG jsou pravidelně proškolení pracovníky dodavatelské společnosti TESCO SW a pracovníky SZR.

Pravidelně probíhá test DRP (Disaster Recovery Plan) – havarijní plán obnovy. Test potvrdil kontinuitu provozu i v případě výpadku jednoho datového centra.

Účinnost těchto školení a testů přechodu na záložní centrum byla ověřena při reálném výpadku napětí aktuálně připojeného datového centra. Přechod na záložní datové centrum proběhl ve stanovenou dobu a bez ztráty dat.

Provoz IS ORG je monitorován aplikací Service Desk, provozovanou SZR. Zde jsou zaznamenány všechny provozní požadavky a události související s provozem, testováním a rozšiřováním systému.

V roce 2014 byl ukončen audit, který v roce 2011 zahájil subjekt pověřený Ministerstvem financí a Ministerstvem pro místní rozvoj. Bylo vydáno stanovisko k auditu Finančním úřadem pro hlavní město Prahu s tím, že neshledal žádné pochybení ve financování ani realizaci projektu „Informační systém ORG v systému základních registrů“.

I letos se Úřad věnoval publicitě Informačního systému základních registrů.

Personální obsazení Úřadu

Počet funkčních míst je Úřadu určen státním rozpočtem a je od roku 2010 stanoven na 102. Fluktuace zaměstnanců v roce 2014 se ve srovnání s předchozími roky snížila z 10 % na necelých 6 %. Pracovní poměr uzavřelo 6 nových zaměstnanců, z toho dva pracovní poměry byly uzavřeny na dobu určitou na zástup za zaměstnankyně na mateřské dovolené. Pracovní poměr ukončili 4 zaměstnanci, z nichž jeden odešel do starobního důchodu.

Ke dni 1. 1. 2014 bylo v Úřadu ve stavu 99 zaměstnanců, ke dni 31. 12. 2014 byl jejich počet 99. Průměrný evidenční přepočtený počet zaměstnanců za rok 2014 byl 99.

Dalších 28 zaměstnanců pracovalo v Úřadu na základě uzavřených dohod mimo pracovní poměr. Na dlouhodobější činnosti, jako je členství v rozkladové komisi Úřadu, výpomoc se stále narůstajícím objemem pracovních úkolů, a to především v souvislosti se zákonem č. 480/2004 Sb., o některých službách informační společnosti (nevyžádaná obchodní sdělení), konzultační činnosti nebo příprava vnitřních předpisů, bylo uzavřeno 19 dohod o pracovní činnosti. Na krátkodobé činnosti, např. na přednáškovou činnost nebo na vyhodnocení soutěže „Moje soukromí! Nekoukat, nešťourat!“, bylo uzavřeno 9 dohod o provedení práce.

Z tabulky „Členění zaměstnanců Úřadu podle věku a pohlaví“ vyplývá, že v Úřadu pracují převážně zaměstnanci ve věku 50 let a výše (54 %), tito zaměstnanci mají kromě odpovídajícího vzdělání i dlouhodobou praxi a velké zkušenosti, většina z nich je v Úřadu zaměstnána od jeho vzniku a svoje zkušenosti předává novým zaměstnancům, většinou absolventům vysokých škol, kteří jsou přijímáni na uvolněná pracovní místa. Předpoklad vysokoškolského vzdělání je na dvě třetiny pracovních míst v Úřadu, na zbývající třetinu pracovních míst je předpoklad úplného středoškolského vzdělání. Z tabulky „Členění zaměstnanců Úřadu podle vzdělání a pohlaví“ je patrné, že zaměstnanci Úřadu splňují kvalifikační předpoklady vzdělání pro výkon své práce.

Úřad umožňuje a zabezpečuje odborný rozvoj svých zaměstnanců. Zajišťuje jim prohlubování odborné kvalifikace a v případě potřeby Úřadu i její zvýšení. Umožňuje zaměstnancům navštěvovat jazykové kurzy a jazykové znalosti uplatnit při výkonu práce. Absolventům středních a vysokých škol umožňuje absolvovat odbornou praxi a tím podporovat jejich zájem o problematiku ochrany osobních údajů a vychovávat si tak nové zaměstnance.

Členění zaměstnanců Úřadu podle věku a pohlaví – stav k 31. prosinci 2014

| Celý soubor | muži | ženy | celkem | % |
|-----------------|-----------|-----------|-----------|-------|
| do 20 let | 0 | 0 | 0 | 0,00 |
| od 21 do 30 let | 4 | 10 | 14 | 14,14 |
| od 31 do 40 let | 8 | 10 | 18 | 18,18 |
| od 41 do 50 let | 6 | 7 | 13 | 13,13 |
| od 51 do 60 let | 13 | 21 | 34 | 34,34 |
| 61 a více | 15 | 5 | 20 | 20,20 |
| Celkem | 46 | 53 | 99 | |

Členění zaměstnanců Úřadu podle vzdělání a pohlaví – stav k 31. prosinci 2014

| Celý soubor | muži | ženy | celkem | % |
|--------------------------------|-----------|-----------|-----------|-------|
| C – Základní | 0 | 1 | 1 | 1,01 |
| H – Střední odborné + VL | 1 | 1 | 2 | 2,02 |
| J – Střední odborné | 0 | 1 | 1 | 1,01 |
| K – Úplné střední všeobecné | 2 | 5 | 7 | 7,07 |
| L – Úplné střední odborné + VL | 1 | 1 | 2 | 2,02 |
| M – Úplné střední odborné | 4 | 15 | 19 | 19,19 |
| N – Vyšší odborné vzdělání | 0 | 1 | 1 | 1,01 |
| R – Bakalářské | 0 | 2 | 2 | 2,02 |
| T – Vysokoškolské | 38 | 26 | 64 | 64,64 |
| Celkem | 46 | 53 | 99 | |

Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 475/2013 Sb., o státním rozpočtu České republiky na rok 2014.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

| | v tisících Kč |
|--|---------------|
| Souhrnné ukazatele | |
| Příjmy celkem | 2 677,80 |
| Výdaje celkem | 124 767,14 |
| Specifické ukazatele – příjmy | |
| Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem | 2 677,80 |
| v tom: příjmy z rozpočtu Evropské unie bez SZP celkem | 702,54 |
| ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem | 1 975,26 |
| Specifické ukazatele – výdaje | |
| Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů | 124 767,14 |
| Průřezové ukazatele výdajů | |
| Platy zaměstnanců a ostatní platby za provedenou práci | 44 743,48 |
| Povinné pojistné placené zaměstnavatelem ^{*)} | 15 143,04 |
| Převod fondu kulturních a sociálních potřeb | 432,76 |
| Platy zaměstnanců v pracovním poměru | 35 179,95 |
| Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů | 8 032,78 |
| Výdaje spolufinancované z rozpočtu Evropské unie bez SZP celkem | 193,23 |
| v tom: ze státního rozpočtu | 0,00 |
| podíl rozpočtu Evropské unie | 1 93,23 |
| Výdaje vedené v informačním systému program. financování EDS/SMVS celkem | 7 210,05 |

^{*)} pojistné na sociální zabezpečení a příspěvek na státní politiku zaměstnanosti a pojistné na veřejné zdravotní pojištění

1. Příjmy

Příjmy pro rok 2014 nebyly schváleným rozpočtem stanoveny.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částkou 2 677,80 tisíc Kč.

Jednalo se především o refundace zahraničních cest zaměstnanců Úřadu Evropskou komisí a Europolem, o sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti, o sankce uložené podle zákona č. 101/2000 Sb., o ochraně osobních údajů a jiných zákonů, o náhrady nákladů řízení, o úroky z finančních prostředků uložených na bankovních účtech, o 85% podíl z rozpočtu Evropské unie za poslední etapu projektu „Informační systém ORG v systému základních registrů“, o 100% refundace výdajů týkající se komunitárního programu Leonardo da Vinci „Zvýšení povědomí o ochraně osobních údajů mezi zaměstnanci pracujícími v EU“, o refundace všech výdajů studijní návštěvy z Makedonie projektu TAIX, o příjmy vztahující se k roku 2013 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2013).

Úroky z finančních prostředků uložené na účtech u ČNB činily 1,30 tisíc Kč.

Přijaté sankční platby byly ve výši 1 460,80 tisíc Kč, neinvestiční dotace z Evropské unie ve výši 702,54 tisíc Kč, přijaté nekap. příspěvky a náhrady týkající se minulých let ve výši 399,09 tis. Kč, převody z ostatních vlastních fondů ve výši 114,07 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

2. Výdaje

Čerpání běžných výdajů ve výši 124 767,14 tisíc Kč odpovídá běžným provozním výdajům, které vyplývají z hlavní činnosti Úřadu; jde zejména o položky spojené s nákupem drobného hmotného majetku, materiálu, IT služeb, služeb spojených s provozem budovy a ostatních služeb, cestovního, vzdělávání, údržby a o výdaje související s neinvestičními nákupy.

Výdaje za vodu, plyn, el. energii a PHM činily v roce 2014 1 946,97 tisíc Kč.

Výše uvedené částky odpovídají požadavku na účelný a hospodárný provoz Úřadu.

3. Platby zaměstnanců a ostatní platby za provedenou práci, vč. souvisejících výdajů

Čerpání rozpočtu na platby zaměstnanců, ostatních výdajů za provedenou práci a souvisejících výdajů, vč. projektů a náhrady v době nemoci, ve výši 60 382,80 tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. 12. 2014 byl 99 zaměstnanců.

4. Výdaje vedené v informačním systému programového financování Ministerstva financí – EDS/SMVS

V souladu se schválenou dokumentací programu 143V01 „Rozvoj a obnova materiálně-technické základny Úřadu pro ochranu osobních údajů od r. 2007“ bylo celkem vyčerpáno 7 210,05 tisíc Kč.

V podprogramu 143V01100 „Pořízení, obnova a provozování ICT ÚOOÚ“ bylo v roce 2014 čerpáno celkem 6 242,05 tisíc Kč v **investičních** systémově určených výdajích SR na následující akce:

| | v tis. Kč |
|---|-----------|
| akci 143V011000052 „Technologická a technická obnova sítě LAN“ | 998,15 |
| akci 143V011000054 „Rozšíření spisové služby GINIS“ | 75,62 |
| akci 143V011000055 „Software 602 Print2“ | 204,73 |
| akci 143V011000056 „Úprava IS ORG 1.etapa“ | 1 350,36 |
| akci 143V011000057 „Úprava modulu Registr“ | 59,03 |
| akci 143V011000058 „Úprava IS ORG 2.etapa“ | 232,32 |
| akci 143V011000059 „Úprava IS ORG 3.etapa“ | 2 106,93 |
| akci 143V011000060 „Technologická a technická obnova WIFI“ | 292,88 |
| akci 143V011000061 „Upgrade Check Point“ | 502,76 |
| akci 143V011000062 „Rozšíření IS ÚOOÚ o nástroj pro centr. správu“ | 419,27 |
| akci 143V011000063 „Prodloužení smlouvy Enterprise na používání produktů Microsoft“ | 0,00 |

V podprogramu 143V01200 „Reprodukce majetku ÚOOÚ“ bylo v roce 2014 čerpáno celkem 968,00 tisíc Kč v **investičních** systémově určených výdajích SR na následující akce:

| | |
|---|--------|
| akci 143V012002014 „Obnova vozového parku 2014“ | 968,00 |
|---|--------|

Přehled čerpání rozpočtu v roce 2014

| Druh rozpočtové skladby | Název ukazatele | Schválený rozpočet 2014 v tis. Kč | Konečný rozpočet 2014 v tis. Kč | Skutečnost dle účetních výkazů k 31. 12. 2014 v tis. Kč | Skutečný konečný rozpočet v % |
|------------------------------|---|-----------------------------------|---------------------------------|---|-------------------------------|
| 4118 | Neinvestiční převody z Národního fondu | 0,00 | 0,00 | 509,31 | |
| 4135 | Převody z rez. fondů OSS | 0,00 | 0,00 | 193,23 | |
| 2141, 2211, 2212, 2324, 4132 | Ostatní nedaňové příjmy | 0,00 | 0,00 | 1 975,26 | |
| | Příjmy celkem | 0,00 | 0,00 | 2 677,80 | |
| 501 | Platy | 43 093,88 | 43 358,09 | 43 212,73 | 99,66 |
| 5011 | Platy zaměstnanců | 34 928,88 | 35 193,09 | 35 179,95 | 99,96 |
| 5013 | Platy státních úředníků | 0,00 | 0,00 | 0,00 | |
| 5014 | Platy zaměst. odvozov. od platů úst. činitelů | 8 165,00 | 8 165,00 | 8 032,78 | 98,38 |

| | | | | | |
|------|---------------------------------------|-------------------|-------------------|-------------------|--------------|
| 502 | Ostatní platby za provedenou práci | 2 075,70 | 2 078,10 | 1 530,75 | 73,66 |
| 5021 | Ostatní osobní výdaje | 1 775,70 | 1 778,10 | 1 469,06 | 82,62 |
| 5024 | Odstupné | 300,00 | 300,00 | 61,68 | 20,56 |
| 503 | Povin. pojist. plac. zaměstnavatelem | 15 357,66 | 15 447,49 | 15 143,04 | 98,03 |
| 5031 | Povin. pojist. na sociál. zabezp. | 11 292,40 | 11 358,45 | 11 120,47 | 97,90 |
| 5032 | Povin. pojist. na veřej. zdr. pojišť. | 4 065,26 | 4 089,04 | 4 022,57 | 98,37 |
| 513 | Nákup materiálu | 2 666,00 | 2 742,34 | 1 413,77 | 51,55 |
| 514 | Úroky a ost. fin. výdaje | 15,00 | 15,00 | 14,92 | 99,44 |
| 515 | Nákup vody, paliv a energie | 2 670,00 | 2 805,00 | 1 946,97 | 69,41 |
| 516 | Nákup služeb | 70 955,80 | 65 188,36 | 48 181,31 | 73,91 |
| 5169 | Nákup ostatních služeb | 68 260,07 | 62 096,43 | 45 721,65 | 73,63 |
| 517 | Ostatní nákupy | 4 487,00 | 5 133,11 | 3 099,68 | 60,39 |
| 5171 | Opravy a udržování | 2 414,00 | 2 414,00 | 1 042,25 | 43,18 |
| 5173 | Cestovné | 1 550,00 | 1 973,61 | 1 491,97 | 75,60 |
| 518 | Poskyt. zálohy, jistiny | 330,00 | 430,00 | 0,00 | 0,00 |
| 519 | Výdaje souvis. s neinv. nákupy | 2 453,00 | 2 825,00 | 2 500,01 | 88,50 |
| 5342 | Převody do FKSP | 433,94 | 436,58 | 432,76 | 99,13 |
| 536 | Ost. neinv. transf. jin. veřej. rozp. | 17,00 | 23,77 | 17,63 | 74,17 |
| 542 | Náhrady plac. obyvatelstvu | 300,00 | 300,00 | 63,52 | 21,17 |
| 5424 | Náhrady v době nemoci | 300,00 | 300,00 | 63,52 | 21,17 |
| | Běžné výdaje celkem | 144 854,97 | 140 782,84 | 117 557,09 | 83,50 |
| 611 | Pořízení dlouh. nehmot. majetku | 6 200,00 | 4 423,35 | 2 526,39 | 57,11 |
| 612 | Pořízení dlouh. hmot. majetku | 3 300,00 | 5 076,65 | 4 683,66 | 92,26 |
| | Kapitálové výdaje celkem | 9 500,00 | 9 500,00 | 7 210,05 | 75,90 |
| | VÝDAJE CELKEM | 154 354,97 | 150 282,84 | 124 767,14 | 83,13 |

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 12. 2014.

Přehled výdajů na projekty spolufinancované z rozpočtu EU v roce 2014

v tis. Kč

| Název projektu | Schválený rozpočet 2014 | Konečný rozpočet 2014 | Skutečnost dle účetních výkazů k 31. 12. 2014 | Skutečnost/konečný rozpočet v % |
|--|-------------------------|-----------------------|---|---------------------------------|
| Leonardo da Vinci „Zvýšení povědomí o ochraně osobních údajů mezi zaměstnanci pracujícími v EU“ | | 179,61 | 179,61 | 100,00 |
| TAIEX | | 13,62 | 13,62 | 100,00 |
| Celkem za projekty spolufinancované z EU | 0,00 | 193,23 | 193,23 | 100,00 |

Poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

V roce 2014 Úřad obdržel celkem 74 žádostí o informace. Jedná se o srovnatelné číslo s předchozím rokem, které potvrzuje zájem veřejnosti o informace vztahující se k působnosti Úřadu, resp. o oblast ochrany osobních údajů jako takovou.

Z celkového počtu žádostí o informace Úřad v roce 2014 zcela vyhověl 43 z nich, v 23 případech žádost o informace odmítl částečně a osm žádostí o informace odmítl zcela. Mezi nejčastější důvody pro částečné nebo celkové odmítnutí žádosti o informace patřila ochrana osobních údajů, které byly mezi požadovanými informacemi obsaženy, především ochrana údajů třetích osob, poškozených či svědků v řízeních vedených Úřadem, a ochrana informací získaných při výkonu dozorové činnosti, které jsou chráněné zákonem uloženou povinností mlčenlivosti. Průměrná doba vyřízení jedné žádosti o informace v roce 2014 činila zhruba šest dnů. Ani v jednom případě nedošlo k překročení zákonné patnáctidenní lhůty pro vyřízení žádosti o informace.

Rozhodnutí o částečném nebo úplném odmítnutí žádosti o informace byla jednou napadena za využití řádného opravného prostředku, tedy rozkladu. Předseda Úřadu jako odvolací orgán v tomto případě rozkladu nevyhověl a postup Úřadu při vyřizování žádosti o informace v tomto případě potvrdil. Předmětem řízení v této žádosti o informace byla žádost o zpřístupnění celého

spisu žadateli, který nebyl účastníkem řízení ani jinak neprokázal právní zájem o nahlédnutí do spisu. V souladu s rozhodovací činností správních soudů, které považují úpravu nahlížení do spisu podle správního řádu ve vztahu k zákonu č. 106/1999 Sb. za zvláštní právní úpravu, byla tato žádost odmítnuta. Postup při vyřizování žádosti o informace byl rovněž v jednom případě napaden stížností podle § 16a zákona č. 106/1999 Sb. Předmětem stížnosti byla skutečnost, že žadateli o informace nebyl zaslán jeden z požadovaných dokumentů, ač tomu tak být mělo. Toto pochybení bylo bezodkladně napraveno.

Postup Úřadu při vyřizování žádostí o informace podle zákona č. 106/1999 Sb. nebyl ani v roce 2014 předmětem soudního přezkumu, Úřadu tak nevznikly žádné související náklady.

Obsahově žádosti o informace nejčastěji směřovaly k rozhodovací praxi Úřadu a k jejímu soudnímu přezkumu. Žadatelé požadovali buď kontrolní závěry či správní rozhodnutí týkající se určité kategorie správců údajů či určité činnosti, informace o soudním přezkumu rozhodnutí Úřadu včetně samotných správních žalob a vyjádření Úřadu k nim, nebo více informací v případě řízení, které Úřad zahájil z moci úřední na základě jejich předchozího podnětu. Nikoliv nevýznamná část žádostí o informace se týkala hospodaření Úřadu. Obsah poskytnutých informací Úřad standardně zveřejňuje i pro další zájemce na svých webových stránkách.

Vyřizování stížností podle § 175 správního řádu

I v roce 2014 se Úřad zabýval stížnostmi podle § 175 správního řádu na základě podnětů dotčených osob, které mají podle tohoto ustanovení právo obrátit se na správní orgán se stížností v případě, pokud se domnívají, že správní orgán postupoval nesprávně, nebo v případě, že došlo k nevhodnému chování úředních osob. Tento institut správního řádu slouží k ochraně práv dotčených osob, pokud jim zákon neposkytuje jiný prostředek ochrany.

V roce 2014 Úřad vyřídil celkem 39 podnětů, které byly vyhodnoceny a následně řešeny jako stížnost podle § 175 správního řádu, kdy z tohoto celkového počtu stížností bylo 10 posouzeno jako důvodné a 5 stížností jako částečně důvodné. Zbýlých 24 stížností bylo shledáno bezdůvodnými. V porovnání s předchozím rokem celkový počet stížností zůstal zhruba stejný.

Zákonná lhůta pro vyřízení stížnosti dle § 175 správního řádu činí 60 dnů. V roce 2014 Úřad stížnosti vyřizoval v průměru za méně než třicet dnů, přičemž zákonem stanovená maximální hranice 60 dnů nebyla v žádném případě překročena.

V deseti případech se stěžovatelé obrátili na Úřad se stížností proti závěrům kontroly inspektorů Úřadu nebo postupu při vedení kontroly inspektory Úřadu, kdy z tohoto celkového počtu byla jedna stížnost posouzena jako důvodná a dvě jako částečně důvodné. V každém případě byl stěžovatel informován o zjištěném pochybení a jeho důsledcích pro konkrétní řešenou věc. Zbýlých sedm stížností bylo posouzeno jako bezdůvodné.

Dvacet pět stížností směřovalo proti postupu Odboru pro styk s veřejností, který prvotně analyzuje stížnosti a podněty, které Úřad obdrží. Stížnosti na postup Odboru pro styk s veřejností se obvykle týkají nesouhlasu stěžovatelů s vyřízením jejich předchozího podnětu, tedy především s jeho odložením bez dalšího opatření, žádná se netýkala stížnosti na nevhodné chování úředních osob. V takových případech dochází na základě podnětů stěžovatelů k prošetření daných stížností a postupu při vyřizování předchozích podnětů, kdy po jejich dalším posouzení bylo v deseti případech shledáno podezření z porušení

zákona č. 101/2000 Sb. s tím, že sedm stížností bylo posouzeno jako důvodných a ve třech případech jako částečně důvodné. Zbýlých patnáct stížností bylo posouzeno jako bezdůvodné. Pokud bylo po jejich přezkoumání shledáno podezření z porušení zákona č. 101/2000 Sb., byly tyto podněty postoupeny buď inspektorovi Úřadu k provedení kontroly, nebo Odboru správních činností k zahájení správního řízení pro podezření ze spáchání správního deliktu či přestupku.

V obou výše uvedených případech platí, že v případě, kdy je stížnost shledána důvodná nebo částečně důvodná, může tato skutečnost nasvědčovat i systémové chybě na straně Úřadu a být tak impulzem k širší diskusi o dané problematice, případně k vypracování obecného výkladového stanoviska či k přijetí jiného opatření ze strany Úřadu.

Tak jako v uplynulém roce ani v roce 2014 žádný z 39 podnětů, které Úřad od stěžovatelů obdržel, nesměřoval proti nevhodnému chování úředních osob. Na základě tohoto zjištění je možné konstatovat, že Úřad při vyřizování podaných podnětů komunikuje s veřejností na profesionální úrovni a v souladu s principy ochrany práv a zájmů adresátů veřejné správy.



Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2014

Úřad pro ochranu osobních údajů

Pplk. Sochora 27, 170 00 Praha 7

E-mail: posta@uoou.cz

Internetová adresa: www.uoou.cz

Na základě povinnosti, kterou mu ukládá zákon č. 101/2000 Sb.,

o ochraně osobních údajů, § 29 písm. d) a § 36,

zveřejnil Úřad pro ochranu osobních údajů tuto výroční zprávu

v únoru 2015 na svých webových stránkách.

Editoři a redakční zpracování: PhDr. Hana Štěpánková a PhDr. David Pavlát, telefon 234 665 286

Grafické řešení: Eva Lufferová

Jazyková korektura: Mgr. Eva Strnadová

Tisk: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno

Pro Úřad pro ochranu osobních údajů vydalo Nakladatelství MU Brno, 2015

ISBN 978-80-210-7758-4