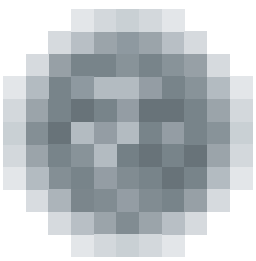
Výroční zpráva 2016



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-8507-7

Úvodní slovo předsedkyně Úřadu

Dámy a pánové,

dovoluji si předložit vaší laskavé pozornosti výroční zprávu Úřadu pro ochranu osobních údajů (dále Úřad) za rok 2016. Kromě toho, že to byl první rok, kdy jsem mohla začít prosazovat své názory na změny v činnosti Úřadu a začaly se objevovat výsledky těchto změn, byl to také iniciační rok z pohledu dalšího vývoje ochrany osobních údajů. Začala totiž platit, i když dosud není účinná, delší dobu připravovaná změna právního rámce ochrany osobních údajů v podobě nového evropského nařízení o ochraně osobních údajů a souvisejících předpisů, které sjednocuje ochranu osobních údajů ve 28 členských státech EU. Jedná se o zcela zásadní kvantitativní i kvalitativní změnu zachovávající původní právní základy a principy. Úřad se již začal na chystané změny systematicky a koncepčně připravovat, přičemž se jedná o aktuálně probíhající kontinuální a dynamický proces seznamování se s novou právní úpravou, rozbor a výklad nových právních institutů a přípravu na aplikační praxi. K tomuto procesu se odpovědně postavily i další subjekty na národní a evropské úrovni.

Nový právní rámec zakotvuje potřebu důslednější a efektivnější ochrany osobních údajů, případně v obecnějším pohledu ochranu soukromí vůbec.

Jedno z nejaktuálnějších témat současnosti navazuje na vývoj nových technologií a datových toků, které pracují s osobními údaji a vyvolávají nejistotu zejména fyzických osob, zda jsou jejich údaje chráněny dostatečně. Podle aktuálních statistik se 80 % Evropanů domnívá, že jejich údaje nejsou dostatečně chráněny. V tomto ohledu má význam právo na informační sebeurčení zakotvené jak na úrovni evropského práva, tak našeho ústavního pořádku, které spočívá v právu jednotlivce rozhodnout se, zda vůbec, v jakém rozsahu a komu zpřístupní své osobní informace. Toto právo může být omezeno pouze zákonem. Soukromí a ochrana osobních údajů jsou z podstaty věci protichůdné k právu na získávání a šíření informací, stejně jako lze obdobné napětí vnímat ve vztahu soukromí jednotlivce a bezpečnosti státu. K řešení těchto střetů práv je nutné proporcionální uvažování v procesu rozhodování, kdy je v několika krocích posuzováno, zda zásah do základního práva slouží legitimnímu cíli, zda je nezbytný a přiměřený. Situace přitom musí být vždy posuzována s ohledem na všechny souvislosti a specifika daného případu. Toto komplexní posuzování již také v některých případech vedlo k přehodnocení některých dřívějších přístupů Úřadu, včetně několika stanovisek. K vyjasňování sporných otázek také přispívá rozhodovací činnost soudů, která umožňuje zpřesnit některá východiska. Úřad přestal zaujímat negativní stanoviska, ani nezveřejňuje oponentní tisková vyjádření k rozhodovací činnosti soudů, jak se stávalo v minulosti. Praxi soudů Úřad respektuje a argumentačně ji rozpracovává, čímž náležitě reflektuje svoji funkci správního orgánu chránícího soukromí člověka jako základní právo. Změny se rovněž promítají ve vyhodnocování podnětů doručených Úřadu, provádění kontrol a ve správním řízení, zde mimo jiné i v přístupu k předmětu nejčastějších podnětů doručovaných Úřadu, totiž kamerovým systémům.

Pokud jde o konkrétní změny, již v roce 2015 byla připravena a zahájena částečná reorganizace Úřadu. Jejím důležitým cílem byla podpora práce inspektorů Úřadu; konkrétně došlo k soustředění kontrolních činností vykonávaných v systému státní služby do kontrolního odboru, což by mělo vést k vytvoření vhodných podmínek pro sjednocování rozhodovacích postupů. Kromě této organizační změny dovnitř Úřadu, která se plně projevila až v roce 2016, bych chtěla poukázat na viditelné změny politiky navenek Úřadu, zejména v oblasti informování veřejnosti. Jednoduše řečeno, snažíme se více a aktivněji komunikovat se zainteresovanou veřejností. V tomto ohledu jsou naším základním zprostředkovacím médiem webové stránky Úřadu. Od loňského roku jsou např. v půlročním intervalu zveřejňovány zprávy o všech kontrolách ukončených inspektory Úřadu, zatímco dříve takový úplný přehled nebyl poskytován.

Za zmínku nepochybně stojí, že odbor pro styk s veřejností, který je důležitým konzultačním orgánem pro odbornou i širokou veřejnost, obdržel v roce 2016 celkem 4721 podnětů, dotazů, stížností a žádostí o konzultace; z nich bylo 143 postoupeno ke kontrole nebo správnímu řízení.

K nejširší veřejnosti se z více než šedesáti správních řízení podle zákona o ochraně osobních údajů dostaly nepochybně i informace o pokutě 3,6 miliónů uložené společnosti T-Mobile za únik osobních údajů zákazníků.

Legislativní oddělení zaznamenalo, že přes obecně zlepšenou spolupráci s předkladateli (téměř dvou set) legislativních návrhů byl Úřad na rozdíl od minulosti jen několikrát opomenut jako připomínkové místo. To se stalo mj. s návrhem novely zákona o zpravodajských službách České republiky, v němž byla navrhována reforma dozoru nad zpravodajskými službami.

Pro úplnost také připomenu, že Úřadem byla vedena veřejná konzultace k online kamerám, která navázala na rozsáhlou diskusi u kulatého stolu. Jedná se o komplexní téma skrývající řadu

dílčích otázek při limitované možnosti použití stávajícího zákona o ochraně osobních údajů (při absenci speciálního zákona o kamerových systémech). Dále Úřad zveřejňuje všechny dostupné informace jako přípravu na účinnost nového obecného nařízení o ochraně osobních údajů. Využíváme rovněž i výsledky společné práce dozorových úřadů členských zemí EU, do níž se snažíme postupně stále více aktivně zapojovat a přispívat.

V neposlední řadě se podařilo naplnit také další z mých záměrů, kterým bylo zřízení analytického oddělení. Podstatou právně-analytické práce je pracovat se všemi dostupnými relevantními podklady, které představují zejména právní předpisy, vnitrostátní i mezinárodní soudní rozhodnutí, srovnávací studie a odborná literatura. Analytická práce dává prostor pro reflexi a vyhodnocení stávající i zamýšlené právní regulace ochrany osobních údajů včetně vztahu k jiným oblastem právní úpravy. Tato činnost v podstatě přispívá k vytyčení směrů rozhodování Úřadu při respektování rozhraní mezi analytickými závěry a kontrolní činností. Cílem je hledání optimálních řešení u složitých otázek ochrany osobních údajů.

Závěrem bych chtěla uvést, že zatímco v prvních měsících svého působení v čele Úřadu jsem vnímala, že problémy ochrany soukromí a osobních údajů se ve veřejné debatě promítaly spíše jako situačně podmíněné a izolované, po schválení evropského obecného nařízení, které se stane účinným v květnu 2018, se situace začíná měnit. Úřad již není osamocen, neboť „agendu" ochrany osobních údajů musí řešit i další subjekty.

Věřím, že tyto aktivity v konečném důsledku přispějí k zajištění cíle sledovaného Úřadem, jímž je ochrana osobních údajů a soukromí fyzických osob v digitálním a technologicky náročném věku, jehož středem musí zůstat služba člověku.

JUDr. Ivana Janů
předsedkyně Úřadu pro ochranu osobních údajů

Obsah

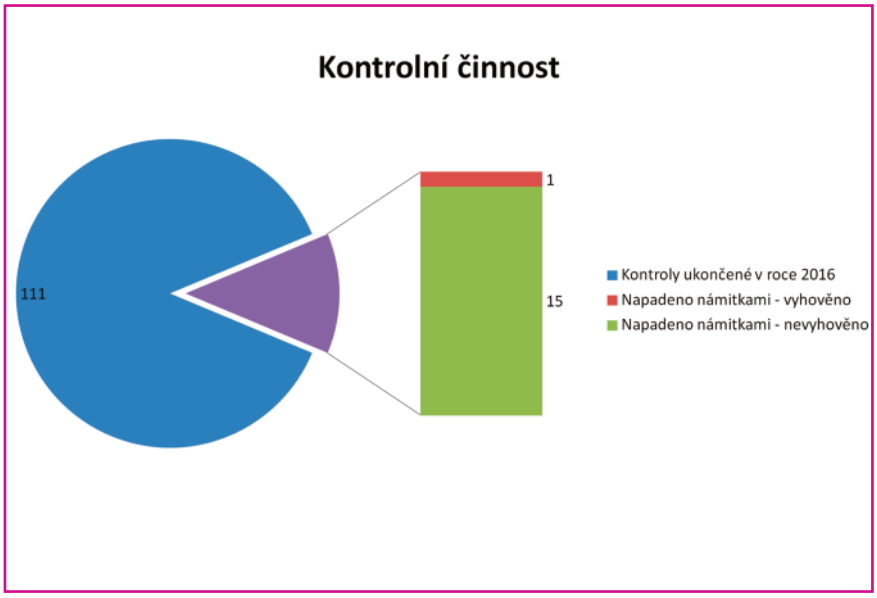
Úřad v číslech 2016

Dotazy a konzultace	ČR		3117
	zahraničí		19
	z toho		
	soukromá sféra		2079
	veřejná správa		751
Podání a stížnosti	přijaté podněty		1585
	informování správce o jeho povinnostech		52
	stížnosti předané ke kontrole nebo správnímu řízení		143
Kontrolní činnost (vyjma kontrol týkajících se zákona č. 480/2004 Sb.)	zahájeno		116
	ukončeno		111
	z toho z předchozích let	rok 2015	47
		rok 2014	1
	předáno jiným státním úřadům		1
	napadeno námitkami		16
	námitkám vyhověno		1
	nevyhověno		15
	převážně vyhověno		0
	převážně nevyhověno		0
	správní řízení o uložení opatření k nápravě		21
	předkontrolní úkony bez následného zahájení kontroly		43
Nevyžádaná obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem		3807
	vyřešených podnětů		3105
	zahájených kontrol		16
	ukončených kontrol		18
	z toho z předchozích let	rok 2015	9
	správních rozhodnutí o pokutě		15
	napadeno námitkami		1
	námitkám vyhověno		0
	nevyhověno		1
	převážně vyhověno		0
	převážně nevyhověno		0
	předkontrolní úkony bez následného zahájení kontroly		611

Správní trestání	správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb.	53
	přestupková řízení podle zákona č. 101/2000 Sb.	13
	přestupková řízení o porušení zákona č. 159/2006 Sb., o střetu zájmů	0
	upuštění od uložení pokuty podle § 40a zákona č. 101/2000 Sb.	33
Rozhodnutí o rozkladech	rozklady napadená rozhodnutí	22
	zamítnutých rozkladů	12
	zrušeno a vráceno k novému projednání	3
	zrušených rozhodnutí a zastaveno řízení	3
	změna rozhodnutí	4
Soudní přezkum (Pozn.: * *celkem od r. 2001*)	podaných žalob k soudu	5 (145*)
	zamítnutých žalob soudem	11
	zrušených rozhodnutí soudem	3
	ukončených/neukončených soudních řízení od roku 2001	114/31
Registrace	přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.)	9708
	zaregistrovaná zpracování	9594
	dosud v řízení	417
	zrušené registrace	153
	oznámení o změně zpracování	945
	řízení podle § 17	54
	zastaveno (nedochází k porušení zákona)	49
	zastaveno z procesních důvodů (např. oznámení vzato zpět)	4
	nepovoleno	0
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	26
	rozhodnutí o povolení předávání	24
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	0
Oznámení podle zákona č. 127/2005 Sb.	došlých oznámení	3
	vyřízených jako opodstatněné	3
	vyřízených jako neopodstatněné	0
Stížnosti podle § 175 správního řádu	přijatých stížností	33
	vyřízených jako důvodné	2

	vyřízených jako částečně důvodné	11
	vyřízených jako bezdůvodné	18
Žádosti podle zákona č. 106/1999 Sb.	přijatých žádostí	53
	zcela vyhověno	42
	částečně odmítnuto	8
	odmítnutých žádostí	3
Publikované materiály	Věstník Úřadu (počet částek)	2
Připomínkované legislativní návrhy	zákony	74
	prováděcí předpisy	92
	návrhy nařízení vlády	26
	návrhy vyhlášek	66
	ostatní	58
	zahraniční materiály	27

Kontrolní činnost Úřadu



• KONTROLNÍ PLÁN

Kontrolní činnost Úřadu je prováděna na základě plánu kontrolní činnosti, podnětů předsedkyně Úřadu a podnětů či stížností, které obsahují upozornění na porušování zákona č. 101/2000 Sb.

Všechny kontroly řídí inspektoři Úřadu, za podpory odboru kontrolního, který byl zřízen od 1. ledna tohoto roku rozdělením původní sekce dozorových činností.

Kontrolní záměry Úřadu se zaměřily na oblasti, v nichž bylo možné očekávat vyšší míru rizika při zpracování osobních údajů a na oblasti, kde se na základě předcházejících zkušeností ukázalo, že může jít o systémové pochybení nebo nesprávné nastavení podmínek při zpracování osobních údajů.

V roce 2016 se Úřad zaměřil na zpracování osobních údajů, které provádí veřejná správa v rámci velkého objemu dat (tzv. Big Data) a dále tato data využívá například pro účely marketingu. Cílem bylo u vybraného subjektu ověřit, zda osobní údaje pocházející ze zákonně zpracovávaných databází nejsou dále využívány za jiným účelem.

Úřad se dále zaměřil na dodržování povinností odpovědných subjektů při využívání služeb „cloud computingu". Zákazníci cloudových služeb by měli provést komplexní analýzu rizik v souvislosti s využíváním těchto služeb, včetně přeshraničního předávání osobních údajů, a to zejména do třetích zemí nezajišťujících přiměřenou úroveň ochrany. Všichni poskytovatelé cloudových služeb by měli svým zákazníkům podávat veškeré informace týkající se přenosu a umístění datových úložišť, aby zákazník mohl správně posoudit všechny výhody a nevýhody poskytované služby.

U vytipované developerské společnosti byla provedena kontrola podmínek ochrany osobních údajů v souvislosti s přípravou a realizací developerských projektů při instalaci a provozu dohledových systémů. Stranou pozornosti nezůstalo zpracování osobních údajů pomocí systémů využívajících biometrické údaje při vstupu zaměstnanců do prostor, kde probíhají práce. Při zpracování citlivých údajů, kam biometrické údaje patří, je třeba dodržovat některé zvláštní právní podmínky.

V oblasti elektronických komunikací bylo kontrolním záměrem prověřit, zda je technicky a organizačně zajišťována důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací.

Do kontrolního plánu byl rovněž zahrnut subjekt, vůči kterému byla již dříve vedena kontrolní nebo správní řízení v oblasti zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Kontrola se zaměřila na dodržování podmínek při zasílání obchodních sdělení a dále také na dodržování zákona o ochraně osobních údajů.

V roce 2016 provedli inspektoři v souladu s plánem kontrolní činnosti následující kontroly:

1. Zpracování osobních údajů v souvislosti **s využíváním provozních a lokalizačních údajů** předávaných Policii ČR, kdy kontrolovaným subjektem bylo Ministerstvo vnitra – Policie ČR – Krajské ředitelství policie hlavního města Prahy. Kontrolu řídí inspektor František Bartoš. Kontrolním záměrem je prověření všech skutečností souvisejících s využíváním provozních a lokalizačních údajů poskytovaných Policii ČR podle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), a dodržování podmínek pro jejich zpracování dle zákona č. 101/2000 Sb. a zákona č. 273/2008 Sb., o Policii České republiky.
   Kontrola nebyla v roce 2016 ukončena.

2. Zpracování osobních údajů, které provádí veřejná správa v rámci velkého objemu dat, tzv. **Big data**, a dále tyto údaje využívá například pro účely marketingu. Kontrolovaným subjektem byl Český statistický úřad (dále také „ČSÚ"). Kontrolu řídil inspektor František Bartoš. Předmětem kontroly bylo prověření dodržování zásady legality při zpracování osobních údajů zdrojově pocházejících z databází ČSÚ, které jsou, nebo mají být následně využívány k obchodním aktivitám tohoto subjektu.

Kontrola byla zahájena v květnu 2016 a ukončena v září 2016. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb.

3. **Využívání údajů z Registru obyvatel** na základě zákonného zmocnění.
   Kontrolovaným subjektem byla vytipovaná zdravotní pojišťovna – Zaměstnanecká pojišťovna Škoda. Kontrolu řídila inspektorka Božena Čajková. Kontrola byla zaměřena na dodržování podmínek stanovených zákonem č. 101/2000 Sb. při zpracovávání osobních údajů pojištěnců. Bylo zjištěno, že kontrolovaný zpracovává řadu osobních údajů pojištěnců, včetně dat získaných z informačních systémů veřejné správy, neboť působí i v oblasti veřejného zdravotního pojištění dle zákona č. 48/1997 Sb., o veřejném zdravotním pojištění. Kontrola prověřila, že na veškeré zpracování osobních údajů, které bylo kontrolou dotčeno, lze aplikovat právní titul dle § 5 odst. 2 písm. a) nebo b) zákona č. 101/2000 Sb., tedy lze zpracovávat osobní údaje pojištěnců bez jejich souhlasu. Kontrolou bylo současně prověřeno řádné plnění povinností dle § 13, § 14 a § 15 zákona č. 101/2000 Sb. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb. V průběhu kontroly došlo ze strany kontrolovaného k úpravě přístupu k datům v základních registrech při využití tzv. služby e20, kterou nabízí Správa základních registrů.

4. **Zpracování v oblasti samosprávy** – oprávněnost přístupů do Registru obyvatel.
   Kontrolovaným subjektem byla vytipovaná obec, v daném případě se jednalo o město Říčany. Kontrolu provedla s kontrolním týmem inspektorka Božena Čajková. Bylo kontrolováno plnění povinností města při zpracování osobních údajů subjektů údajů z Informačního systému základních registrů – konkrétně z registru obyvatel (a dále z agendového informačního systému evidence obyvatel, na základě zákona č. 128/2000 Sb., o obcích (obecní zřízení), a zákona č. 111/2009 Sb., o základních registrech). Kontrolou bylo zjištěno, že město je ve vztahu k předmětným registrům v postavení zpracovatele osobních údajů, přičemž osobní údaje zpracovává za účelem výkonu přenesené působnosti obce dle zvláštních právních předpisů. Kontrolovaný tedy postupoval na základě právního titulu dle § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. Dále bylo kontrolou prověřeno, že kontrolovaný přijal přiměřená opatření k zabezpečení osobních údajů dle § 13 zákona č. 101/2000 Sb. a že upravil povinnost mlčenlivosti zaměstnanců ve vnitřních předpisech města a v pracovní smlouvě v souladu s požadavky § 15 zákona č. 101/2000 Sb.

5. **Monitorovací systémy v developerských projektech**
   Kontrolovanými subjekty byly vytipované společnosti – developerská a stavební. Kontrolu vedly inspektorky Božena Čajková a Jiřina Rippelová.
   Kontrolním záměrem bylo prověření podmínek ochrany osobních údajů v souvislosti s přípravou a realizací developerských projektů při instalaci a provozu sledovacích systémů v bytových objektech nebo v jejich bezprostředním okolí. V říjnu 2016 byly na základě kontrolního plánu zahájeny dvě kontroly: kontrola Společenství vlastníků jednotek budovy Rezidenčního centra Zvonařka čp. 2536, kterou vede inspektorka Čajková a která nebyla v roce 2016 ukončena, a kontrola Společenství vlastníků jednotek pro budovu Čistovická 1700/62, kterou vedla inspektorka Rippelová a kterou nebylo zjištěno porušení zákona č. 101/2000 Sb.

6. **Zpracování osobních údajů v oblasti církví a náboženských společností**

Prvním kontrolovaným subjektem bylo Ministerstvo kultury. Kontrola byla zahájena na základě kontrolního plánu. Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb. při zpracování osobních (citlivých) údajů subjektů údajů, tj. členů či občanů hlásících se k církvím nebo náboženským společnostem v souvislosti s návrhem na jejich registraci nebo v souvislosti s vedením seznamů registrovaných církví a náboženských společností. Kontrolu řídil inspektor Petr Krejčí. Kontrola se zaměřila na zpracování osobních údajů osob v souvislosti s provozem informačního systému s velkým objemem dat, zejména citlivých údajů občanů hlásících se k určité církvi nebo náboženské společnosti. Při kontrole nebylo zjištěno porušení zákona o ochraně osobních údajů.

Druhým kontrolovaným subjektem byli členové přípravného výboru náboženské společnosti na základě podnětu Ministerstva kultury v souvislosti s podáním návrhu na registraci náboženské společnosti u tohoto ministerstva, ze kterého vyplynulo podezření, že členové přípravného výboru náboženské společnosti porušují zákon o ochraně osobních údajů. Kontrolu řídil inspektor Petr Krejčí. Podezření uvedené v podnětu se potvrdilo a při kontrole bylo zjištěno porušení ustanovení § 5 odst. 1 písm. g), § 5 odst. 2, § 9 a § 11 odst. 1 zákona č. 101/2000 Sb.

Třetím kontrolovaným subjektem byli další členové přípravného výboru náboženské společnosti na základě podnětu Ministerstva kultury. Kontrolu řídil inspektor Petr Krejčí. V daném případě musela být zajištěna rozsáhlá součinnost dalších subjektů, neboť bylo nutné v rámci protikladných tvrzení kontrolovaných zjistit skutečný stav věci, a to jak pro účely kontrolního zjištění Úřadu, tak následně proto, aby protokol o kontrole mohl být podkladem i pro další správní rozhodování jiného správního orgánu. Takto provedenou kontrolou pak bylo zjištěno porušení ustanovení § 5 odst. 1 písm. g), § 5 odst. 2, § 9 a § 11 odst. 1 zákona č. 101/2000 Sb.

7. **Předávání osobních údajů do třetích zemí**

Kontrolovanou osobou, kterou je subjekt poskytující služby v oblasti cestovního ruchu, jejichž součástí je předávání osobních údajů do třetích zemí, je společnost Čedok a.s. Kontrola byla zahájena v prosinci 2016 a tuto kontrolu vede inspektor Petr Krejčí. Kontrolním záměrem je prověřit dodržování podmínek při zpracování osobních údajů v souladu s § 27 odst. 3 zákona č. 101/2000 Sb. ze strany odpovědného subjektu. Kontrola, která navazuje na rozsudek Soudního dvora Evropské unie ve věci C-362/14 Maximillian Schrems v. Data Protection Commissioner, nebyla dosud ukončena.

8. **Zpracování osobních údajů žadatelů o víza**

Kontrolovaným subjektem byl zastupitelský úřad Generální konzulát New York. Kontrolu řídil inspektor Petr Krejčí. Kontrolním záměrem bylo prověření dodržování povinností odpovědného subjektu při zpracování osobních údajů žadatelů o víza pro krátkodobý a dlouhodobý pobyt v ČR. Kontrola byla zahájena v květnu 2016 a ukončena v září 2016. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb.

9. Oblast archivnictví a spisové služby

   Kontrolovaným subjektem byl Národní archiv. Kontrolu řídila inspektorka Jiřina Rippelová. Předmětem kontroly bylo zpracování osobních údajů, které byly předány Národnímu archivu Českým statistickým úřadem dle § 22 odst. 4 zákona č. 296/2009 Sb., o sčítání lidu, domů a bytů v roce 2011. Kontrolovaný převzal od ČSÚ v březnu 2014 částečně anonymizované sčítací formuláře vyplněné povinnými osobami při sčítání (tj. Sčítací list osoby, Bytový list a Domovní list). Anonymizaci provedl ČSÚ tak, že odstranil (začernil) některé údaje. Ve Sčítacím listě nicméně nebyly anonymizovány údaje, na základě kterých mohou být podle názoru Úřadu některé fyzické osoby určitelné (např. kombinací údajů obec, část obce a údaje o konkrétně specifikovaném zaměstnání, nebo o příslušnosti k národnostní menšině, málo se vyskytujícím mateřském jazyku, příslušnosti k méně početné církvi, nebo údaji o neobvyklém počtu dětí, ve spojení s rokem narození).

   Kontrolující proto konstatovali, že sporné údaje uvedené ve formuláři Sčítací list osoby jsou osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. a v některých případech také citlivými údaji podle § 4 písm. b) tohoto zákona (údaje vypovídající o tom, zda osoba žije v registrovaném partnerství, a údaje o národnosti nebo náboženské víře subjektů údajů). Kontrolou bylo zjištěno, že předmětné osobní a příp. citlivé údaje kontrolovaný zpracovává v souladu s § 5 odst. 2 písm. a), resp. § 9 písm. ch) zákona č. 101/2000 Sb. Kontrolou bylo dále hodnoceno plnění povinnosti vyjádřené v § 13 zákona č. 101/2000 Sb. a bylo konstatováno, že kontrolovaný přijal taková technicko-organizační opatření, která zohledňují účel a prostředky zpracování osobních údajů a která garantují vyžadovanou míru ochrany zpracování osobních údajů.

10. Zpracování osobních údajů pomocí dohledových systémů využívajících biometrické údaje

    Kontrolovaným subjektem byla společnost Skanska a.s. Kontrolu řídila inspektorka Jiřina Rippelová. Kontrolním záměrem k prověření byly dostupné poznatky týkající se nasazování biometrické identifikace osob vstupujících na staveniště kontrolovaného subjektu pomocí tzv. FaceID technologie. Kontrolující prověřovali, jakým způsobem jsou dodržovány povinnosti odpovědných subjektů v oblasti zpracování osobních údajů, včetně údajů biometrických, které patří mezi skupinu citlivých údajů. Podle kontrolního zjištění a dalších dostupných informací používá kontrolovaný subjekt pomocí speciálního softwaru právě tyto skupiny informací pro identifikaci osob vstupujících do prostor, kde probíhají stavební práce nebo jiné související aktivity. Kontrola byla zahájena dne 5. dubna 2016 a ukončena dne 30. září 2016.

    Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb.

11. Zpracování osobních údajů při dodržování povinností České republiky v oblasti mezinárodní policejní spolupráce

    Dle čl. 8 Rozhodnutí Rady o Europolu (2009/371/SVV) je každý členský stát povinen zřídit nebo určit národní jednotku Europolu pověřenou prováděním určených úkolů. Národní jednotka Europolu je styčným bodem mezi Europolem a národními kompetentními orgány členských států. Kontrolovaným subjektem bylo Ministerstvo vnitra ČR. Kontrolu řídil inspektor Daniel Rovan. Kontrolním záměrem k prověření byl postup a způsob, jak jsou

dodržovány povinnosti odpovědného subjektu v oblasti zpracování osobních údajů při jejich přenosu a zpřístupňování v rámci mezinárodní policejní spolupráce.
Kontrola byla zahájena dne 16. května 2016 a ukončena dne 31. srpna 2016. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb.

12. Oblast elektronických komunikací
Kontrola se v oblasti výkonu dozoru zaměřila na prověření a vyhodnocení dodržování povinností odpovědných subjektů při sdílení a zpřístupňování důvěrných informací účastníků nebo uživatelů z hlediska legality jejich postupů v návaznosti na § 89 zákona č. 127/2005 Sb., o elektronických komunikacích, a stanovisko Úřadu č. 6/2013, Poskytování informací o provozních a lokalizačních údajích uchovávaných provozovateli služeb elektronických komunikací. Kontrolovaným subjektem byla společnost O2 Czech Republic a.s., která je jedním ze subjektů poskytujících veřejně dostupnou službu elektronických komunikací. Kontrolu řídil inspektor Daniel Rovan. Kontrolou, která byla zahájena v září 2016 a ukončena v prosinci 2016, nebylo zjištěno porušení zákona č. 101/2000 Sb.

13. Oblast zdravotnictví
Záměrem kontroly bylo prověřit dodržování podmínek při zpracování osobních údajů orgány státní správy v ochraně veřejného zdraví a dalších subjektů, které se na zpracování podílejí. Kontrolovaným subjektem je Krajská hygienická stanice v Brně. Kontrola, kterou řídí inspektorka Jana Rybínová, byla zahájena dne 30. září 2016 a nebyla dosud ukončena.

14. Oblast školství
Jako kontrolní záměr k prověření určila kontrolující inspektorka Jana Rybínová prověřit dodržování podmínek při zpracování osobních údajů Ministerstvem školství, mládeže a tělovýchovy ČR a případně dalších subjektů, které se na zpracování podílejí. Kontrola byla zahájena dne 21. března 2016 a dosud probíhá.

15. Dodržování povinností odpovědných subjektů při využívání služeb „Cloud computing"
Součástí kontrolního plánu pro rok 2016 bylo provést kontrolu, která se zaměří na realizaci podmínek pro ochranu osobních údajů podle zákona č. 101/2000 Sb., týkající se povinností správce či zpracovatele při zpracování osobních údajů při využívání cloudů, zejména s ohledem na podmínky zabezpečení zpracovávaných osobních údajů.
Kontrolovanými subjekty jsou: Česká spořitelna, a.s., MONETA Money Bank, a.s., a Sberbank CZ, a.s. Všechny kontroly, které řídí inspektor Josef Vacula, byly zahájeny v prosinci 2016.

16. Dodržování povinností odpovědných subjektů podle zákona č. 480/2004 Sb.
Součástí kontrolního plánu pro rok 2016 bylo i provedení kontroly podle zákona č. 480/2004 Sb., která se zaměří na podmínky pro dodržování zasílání obchodních sdělení, a dále též kontroly podle zákona č. 101/2000 Sb., týkající se povinností správce či zpracovatele při zpracování osobních údajů v souvislosti s jejich obchodní činností.
Kontrola byla zahájena dne 1. června 2016 a kontrolovaným subjektem je společnost AAA Auto International a.s. Kontrolu, která dosud probíhá, vede inspektor Josef Vacula.

17. **Zpracování osobních údajů při využívání údajů pořizovaných v souvislosti s provozem sledovacích systémů při provozu na pozemních komunikacích Policií ČR**

Při instalaci a provozu sledovacích systémů v dopravě dochází ke zpřístupnění systémů a čerpání informací pro potřeby Policie ČR. Záměrem kontroly bylo prověřit legitimitu následného využívání těchto údajů a dodržování podmínek pro jejich zpracování v podmínkách zákona č. 101/2000 Sb.

Kontrola Krajského ředitelství policie Libereckého kraje byla zahájena 7. září 2016 a ukončena 23. září 2016. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb. Kontrola Ministerstva vnitra – Policie ČR byla zahájena 19. října 2016 a nebyla dosud ukončena. Obě kontroly řídí inspektor František Bartoš.

• POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

V této kapitole jsou uváděny poznatky ze zásadních kontrol. Kompletní přehled výsledků kontrolní činnosti je uveden na webových stránkách Úřadu v rubrice Dozorová činnost/Zveřejňování informací o kontrolách.

Kontrola ve zdravotnickém zařízení Stellart s.r.o. (inspektorka Jana Rybínová)
Stěžovatelka v podnětu Úřadu sdělila, že podstoupila v roce 2012 ve zdravotnickém zařízení Stellart s.r.o. (dále také „Kontrolovaná osoba" nebo „Klinika") umělé oplodnění.

Po narození dcery v roce 2013 v souvislosti s návrhem na určení otcovství ze strany stěžovatelky požádal Okresní soud v Mostě v listopadu 2014 Kontrolovanou osobu o originály listin, které měl za nezbytné k určení otcovství. Kontrolovaná osoba tyto listiny soudu neposkytla, protože došlo k jejich ztrátě. Dle Kontrolované osoby se celá zdravotnická složka týkající se stěžovatelky ztratila a nebyla dohledána, následně bylo odůvodňováno zničením dokumentace. Nový jednatel Kontrolované osoby se v této věci obrátil podáním trestního oznámení ve věci krádeže zdravotnické dokumentace (dále také „ZD") na Policii České republiky, a to dne 20. listopadu 2014. Stěžovatelka ve věci ztráty ZD podala trestní oznámení v březnu 2015. Věc byla šetřena PČR KŘP Ústeckého kraje. V uvedené věci byli v daném řízení vyslechnuti svědci. Z výpovědi zdravotní sestry, kterou učinila na Policii ČR, vyplývalo, že šanony s dokumentací žadatelek o umělé oplodnění se ukládaly na recepci do neuzamčeného šuplíku a do neuzamčených polic v zasedací místnosti kliniky. Z dalších výpovědí vyplývalo, že přístup ke ZD stěžovatelky mělo u Kontrolované osoby více osob.

Na Klinice došlo dle některých svědků podávajících vysvětlení v roce 2013 k vytopení prostor vodou. Dne 14. května 2015 jednatel Kontrolované osoby Okresnímu soudu v Mostě sdělil, že část ZD byla při vytopení v červenci 2014 poškozena, pro její promočení nemohla být řádně identifikována. Určité listiny tedy musely být na skartačním přístroji Kontrolované osoby skartovány. Dokumenty prokazující a související s umělým oplodněním stěžovatelky ke dni podání podnětu, tj. k 6. lednu 2016, Kontrolovaná osoba soudu nepředala.

Ze sdělení Policie ČR Ústeckého kraje vyplývalo, že na základě trestního oznámení stěžovatelky zahájil policejní orgán v roce 2015 úkony trestního řízení dle § 158 odst. 3 trestního řádu ve věci trestného činu neoprávněného nakládání s osobními údaji dle ust. § 180 odst. 2 trestního zákoníku, a to proti neznámému pachateli, který se tohoto jednání mohl dopustit tím, že v blíže nezjištěném období od roku 2012 do současné doby v budově Kliniky dostatečně nezabezpečil ZD stěžovatelky, a z tohoto důvodu mohlo následně dojít k její ztrátě, čímž mohlo dojít ke zpřístupnění ZD třetí osobě. Tímto jednáním mohla být způsobena vážná újma na právech poškozené. Z výpovědi současného jednatele Kliniky vyplynulo, že poté, kdy byla zjištěna ztráta ZD stěžovatelky, nařídil ze své pozice jednatele kontrolu ZD pacientů Kliniky, přičemž byla zjištěna ztráta pouze ZD stěžovatelky. Věc byla následně policejním orgánem ukončena návrhem na uložení, jelikož policejní orgán na základě výsledku svého šetření neshledal podezření ze spáchání trestného činu nebo přestupku.

Krajský úřad Ústeckého kraje v rámci součinnosti Úřadu sdělil, že v uvedené věci neobdržel žádný podnět, tedy u poskytovatele zdravotních služeb Stellart s.r.o. nebylo provedeno žádné šetření.

Kontrola byla zahájena u Kontrolované osoby dne 1. března 2016, předmětem kontroly bylo dodržování povinností Kontrolované osoby (správce nebo zpracovatele) osobních údajů stanovených zákonem č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů, se zaměřením na zpracování osobních údajů pacientky společnosti Stellart s.r.o. ve ZD, a s tím související kontrola zabezpečení ZD dle ustanovení § 13 zákona č. 101/2000 Sb.

V rámci kontroly bylo zjištěno, že v době kontroly probíhala v budově kliniky rozsáhlá rekonstrukce, která byla před dokončením zhruba koncem dubna 2016. Rekonstrukce probíhala za provozu ve všech podlažích budovy. Inspektorka Úřadu zjistila, že Kontrolovaná osoba jako správce osobních údajů pacientů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. v době kontroly neměla dispozici nad ZD stěžovatelky v listinné podobě, nedisponovala ani žádnou její částí (záznam o odběru a uchovávání biologického vzorku podepsaný oběma partnery – embryologická dokumentace), která je jinak uchovávána v laboratoři Kliniky. Kontrolovaná osoba nebyla schopna určit přesnou dobu, odkdy ZD stěžovatelky na Klinice chybí. Po změně osoby jednatele (listopad 2014) v rámci změn uskutečněných v souvislosti se změnou jednatele Kliniky nebylo provedeno protokolární předání společnosti. Ke zjištění, že uvedená ZD na Klinice není, došlo dle sdělení Kontrolované osoby zřejmě po obdržení žádosti soudu o předložení ZD stěžovatelky. Žádost Okresního soudu v Mostě o předložení ZD stěžovatelky obdržela Kontrolovaná osoba dne 20. listopadu 2014. V létě roku 2014 došlo dle Kontrolované osoby v budově Kliniky k havárii vody, přičemž bylo vytopeno 3. a 2. patro a částečně i 1. patro, kde se v konzultační místnosti nacházela v plechových registračních skříních ZD pacientů, tedy i stěžovatelky. Zároveň došlo dle Kontrolované osoby i k poškození dalších pěti ZD, tyto nebyly k dohledání.

Kontrolující inspektorka konstatovala, že kontrolou nebylo posuzováno, kdo je osobně odpovědný za ztrátu ZD stěžovatelky a za ztrátu dalších pěti zdravotnických dokumentací. V závěru kontroly konstatovala, že správce osobních údajů pacientů vedených ve ZD, tj. Kontrolovaná osoba, porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. tím, že ztratila dispozici nad ZD stěžovatelky a dalších celkem pěti pacientek, tedy Kontrolovaná osoba nepřijala taková opatření, aby nedošlo ke ztrátě ZD stěžovatelky i ke ztrátě dalších zdravotnických dokumentací pěti pacientek.

V rámci kontroly byl posuzován i současný stav zabezpečení ZD pacientů, kdy bylo zjištěno, že ZD je vedena v listinné podobě, v elektronické podobě jsou ve zdravotnickém informačním systému Kliniky vedeny záznamy o průběhu léčby, přičemž bylo zjištěno, že Kontrolovaná osoba nejpozději do 26. května 2016 nepořizovala elektronické záznamy, které umožní určit a ověřit kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány v rámci zdravotnického softwaru, a tím Klinika porušila ustanovení § 13 odst. 4 písm. c) zákona č. 101/2000 Sb. Úřad s Klinikou nezahájil řízení o uložení opatření k odstranění zjištěných nedostatků ve smyslu § 40 zákona o ochraně osobních údajů, neboť kontrolou sice bylo prokázáno, že Klinika porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb., tedy nepřijala taková opatření, aby nedošlo ke ztrátě ZD stěžovatelky a ke ztrátě dalších ZD pěti pacientek, kontrolou bylo však zároveň zjištěno, že v současné době při vedení ZD Klinika neporušuje ustanovení § 13 odst. 1 zákona č. 101/2000 Sb., tedy sama přijala opatření k zabezpečení zdravotnické dokumentace pacientek a zároveň v průběhu kontroly zajistila funkčnost logování ve smyslu § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

Úřad jako příslušný správní orgán společnosti Stellart s.r.o. za spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., neboť nepřijala nebo neprovedla opatření pro zajištění bezpečnosti zpracování osobních údajů, uložil pokutu ve výši 250.000 Kč.

Kontrola nakládání s obrazovou zdravotnickou dokumentací ve zdravotnickém zařízení Perfect Clinic s.r.o. (inspektorka Jana Rybínová)

Předmětem kontroly ve zdravotnickém zařízení Perfect Clinic s.r.o. (dále také „Kontrolovaná osoba" nebo „Klinika") bylo dodržování povinností stanovených v hlavě II zákona č. 101/2000 Sb., se zaměřením na dodržování povinností při zpracování osobních údajů při poskytování zdravotních služeb, zejména zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace (dále také „ZD") a jejich zabezpečení dle § 13 zákona č. 101/2000 Sb.

Důvodem pro zahájení kontroly byl podnět, který Úřad obdržel od stěžovatelky s tím, že v průběhu poskytování zdravotních služeb Kontrolovanou osobou zaznamenala řadu skutečností, na základě kterých má podezření, že Kontrolovaná osoba, jako poskytovatel zdravotních služeb dlouhodobě a systematicky neplní povinnosti uložené jí právními předpisy, zejména zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ale také zákonem č. 101/2000 Sb. Stěžovatelka se domnívala, že Kontrolovaná osoba nezavedla žádná systematická opatření pro zajištění bezpečnosti zpracování osobních údajů, jak vyžaduje § 13 zákona č. 101/2000 Sb. Ošetřující lékař pořizoval její fotografie (místa zákroku) svým soukromým mobilním telefonem, a ještě ani po několika měsících od jejich pořízení je neuložil do žádného zabezpečeného úložiště patřícího Klinice.

Kontrolou bylo zjištěno, že Kontrolovaná osoba je zdravotnickým pracovištěm a poskytuje zdravotní péči na základě zákona č. 372/2011 Sb., účel a prostředky zpracování osobních údajů má tedy Kontrolovaná osoba stanoveny ustanovením § 53 odst. 1 uvedeného zákona, dle něhož je zdravotnické zařízení povinno vést ZD pacienta a nakládat s ní podle tohoto zákona a jiných právních předpisů. ZD je souborem informací podle odstavce 2 uvedeného ustanovení zákona vztahujících se k pacientovi, o němž je vedena. Kontrolovaná osoba je ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. správcem osobních a citlivých údajů pacientů.

Stěžovatelka podstoupila u Kontrolované osoby celkem tři operační zákroky, přičemž v rámci všech souvisejících poskytovaných zdravotních služeb jí byla pořizována ošetřujícím lékařem fotodokumentace. V té době však Kontrolovaná osoba neměla přijatu interní směrnici, upravující nakládání s obrazovou dokumentací, tato problematika byla se zaměstnanci řešena ústní formou. V případě poskytované zdravotní péče související s jedním z operačních zákroků ošetřující lékař pořídil v dubnu 2013 více fotografií stěžovatelky svým mobilním telefonem, fotografie z operačního zákroku přehrál do databáze Kontrolované osoby v říjnu 2013. Bylo zjištěno, že Kontrolovaná osoba neměla úplnou dispozici nad pořízenými pěti fotografiemi stěžovatelky minimálně v období od dubna 2013 do října 2013. Uložení snímků v paměti mobilního telefonu neposkytovalo jejich dostatečnou ochranu před zničením, neoprávněným přístupem a přenosem, takový způsob uložení je nutno pokládat za velmi rizikový. Dále bylo zjištěno, že jedna fotografie vztahující se k poskytnuté zdravotní péči související s operačním zákrokem v prosinci 2013 nebyla součástí ZD stěžovatelky ještě v dubnu 2015. Kontrolovaná osoba tedy neměla úplnou dispozici nad pořízenou fotografií stěžovatelky minimálně v období od prosince 2013 do května 2015.

Kontrolující inspektorka v závěru konstatovala, že Kontrolovaná osoba minimálně ve výše uvedených obdobích zpracovávala ZD stěžovatelky, která nebyla úplná, neboť neobsahovala fotodokumentaci pořízenou v rámci poskytování zdravotnických služeb (celkem šest fotografií), a to v důsledku neexistujícího vnitřního předpisu dokumentujícího a upravujícího řízený postup při pořizování fotodokumentace klientů a jejím nakládání, neboť předložená interní směrnice „Fotodokumentace klienta" neexistovala. Tedy Kontrolovaná osoba ve výše uvedeném období nepřijala taková opatření, aby nemohlo dojít k neoprávněnému zpracování osobních, resp. citlivých, údajů stěžovatelky, čímž porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb.

Dále bylo zjištěno, že archiv ZD Kontrolované osoby se nachází v podzemních garážích budovy, vstup do archivu je ze samostatné neuzamčené chodby, dveře do archivu nejsou bezpečnostní, nejsou osazeny bezpečnostním zámkem, v prostoru chodby ani samotného archivu není instalován kamerový systém a dokumenty uložené v archivu nejsou evidovány. Kontrolující inspektorka konstatovala, že Kontrolovaná osoba nepřijala dostatečná technicko-organizační opatření ve smyslu § 13 odst. 1 zákona č. 101/2000 Sb. tak, aby dostatečně zabezpečila zdravotnickou dokumentaci uloženou v archivu, neboť v důsledku nedostatečných technicko-organizačních opatření nemá zajištěnu úplnou dispozici nad zdravotnickou dokumentací uloženou v archivu, čímž porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb.

Kontrolovaná osoba podala námitky proti kontrolním zjištěním s tím, že pořizování fotodokumentace k estetickému zákroku je čistě na uvážení a v dispozici ošetřujícího lékaře. Fotodokumentace je prováděna vždy za vědomí a souhlasu pacienta. Pokud došlo k pořízení fotografií pacientky lékařem prostřednictvím mobilního telefonu, jednalo se o mimořádnou situaci, kdy fotoaparát Kliniky nebyl lékaři výjimečně k dispozici, a bylo nutné při vyšetření fotografie pořídit. Lékař použil služební telefon ve vlastnictví Kliniky a fotografie byly po jejich pořízení převedeny na chráněné úložiště společnosti a z mobilního telefonu vymazány. Ze strany lékaře došlo k opomenutí a prodlevě, tyto fotografie nebyly okamžitě nahrány do zdravotnické dokumentace stěžovatelky. Z tohoto individuálního pochybení lékaře vyvodila Klinika odpovídající důsledky, vůči lékaři uplatnila sankci za porušení jeho povinností a s okamžitou účinností výslovně nařídila všem svým zaměstnancům i spolupracovníkům užívat k pořizování fotografií pacientů výhradně a bez výjimek k tomu určený fotoaparát, kdy případné porušení tohoto nařízení je Klinikou sankcionováno. Klinika v námitkách dále uvedla, že není pravdivé tvrzení, že fotografie byly uchovávány mimo zdravotnickou dokumentaci stěžovatelky v období do 2. října 2013. Klinika v námitkách dále uvedla, že měla vždy plnou dispozici nad všemi fotografiemi všech pacientů, které byly pořízeny při jejich vyšetření pro účely jejich zařazení do ZD pacientů. K zabezpečení archivu ZD Klinika namítala, že v současnosti intenzivně řeší možnost důkladnějšího zabezpečení archivu (zabezpečení dveří, kamerový systém), včetně jeho případného přesunu do jiných prostor. Již nyní též probíhá evidence dokumentů v archivu uložených. Společnost tedy přijala první opatření k nápravě zjištěných nedostatků a na odstranění zbývajících pracuje.

Předsedkyně Úřadu, jako druhoinstanční správní orgán, rozhodnutím ze dne 11. března 2016, námitky Kliniky zamítla a kontrolní zjištění, tedy porušení § 13 odst. 1 zákona č. 101/2000 Sb. Klinikou, potvrdila.

Úřad jako příslušný správní orgán společnosti Perfect Clinic s.r.o. za spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., neboť nepřijala nebo neprovedla opatření pro zajištění bezpečnosti zpracování osobních údajů, uložil pokutu ve výši 15.000 Kč.

Kontrola elektronické výměny a sdílení zdravotnické dokumentace ve zdravotnických zařízeních Kraje Vysočina (inspektorka Jana Rybínová)

Předmětem kontroly bylo dodržování povinnosti správce a zpracovatele osobních údajů stanovených v hlavě II zákona č. 101/2000 Sb., v souvislosti se shromažďováním, zpracováním a sdílením osobních a citlivých údajů při provozu informačního systému zdravotnických zařízení zřizovaných vyšším územně samosprávným celkem, se zaměřením na ochranu osobních údajů, zpracovávaných prostřednictvím projektu eMeDocS (Exchange Medical Documents System), realizovaným ve zdravotnických zařízeních Kraje Vysočina (dále také „Kontrolovaná osoba") za účelem elektronické výměny a sdílení zdravotnické dokumentace (dále také „ZD"). Kontrola byla zahájena na základě Kontrolního plánu Úřadu pro rok 2015.

Kontrolou bylo zjištěno, že Kontrolovaná osoba v rámci systému eMeDocS poskytuje tyto funkcionality výměny ZD mezi zdravotnickými zařízeními: poskytování urgentních informací o pacientech pro účely zdravotnické záchranné služby (dále také „ZZS") v reálném čase; poskytování urgentních informací o pacientech ošetřujícímu lékaři v nemocnici; zasílání „Záznamu o výjezdu" do nemocnice, kam je pacient předán; zasílání elektronické žádanky na RDG vyšetření pacienta na pracoviště magnetické rezonance Nemocnice Jihlava; zaslání elektronického popisu z RDG vyšetření magnetické rezonance pacienta v jihlavské nemocnici na základě obdrženého elektronického požadavku – žádanky; zasílání Propouštěcí zprávy pacienta mezi nemocnicemi (na vyžádání) a zasílání Ambulantní zprávy o pacientovi mezi nemocnicemi (na vyžádání).

V rámci systému eMeDocS dochází k výměně informací ze ZD pacientů vedených u jednotlivých poskytovatelů zdravotních služeb zapojených do systému eMeDocS, tj. osobních a citlivých údajů pacientů zpracovávaných v Nemocničním informačním systému (dále také „NIS") jednotlivých poskytovatelů zdravotních služeb, a to mezi poskytovateli zapojenými do projektu eMeDocS navzájem a u zdravotnické záchranné služby, poskytující zejména přednemocniční neodkladnou péči osobám se závažným postižením zdraví ve smyslu § 2 odst. 1 zákona č. 374/2011 Sb., o zdravotnické záchranné službě. Zdravotnická zařízení i ZZS pro účely vedení ZD shromažďují a zpracovávají osobní údaje v rozsahu nezbytném pro identifikaci pacienta v souladu s ustanovením § 53 odst. 2 písm. a) zákona č. 372/2011 Sb.

Z printscreenu ukázky přístupu do systému eMeDocS v roli pracovníka ZZS vyplývá, že zdravotnická záchranná služba v rámci sytému eMeDocS zpracovává osobní údaje uvedené v tzv. Emergency card, tj.: příjmení a jméno pacienta, rodné číslo, pohlaví, státní příslušnost, datum narození, věk, trvalé bydliště, údaj o zdravotní pojišťovně, na základě těchto údajů je pacient určitelný a lze jej přímo identifikovat. Jednotliví poskytovatelé zdravotních služeb včetně ZZS zapojení do systému eMeDocS, zpracovávají ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. osobní údaje pacientů. Zpracovávány jsou citlivé údaje pacientů vypovídající o jejich diagnóze, rizikových faktorech, alergiích, medikaci, anamnéze a návštěvách zdravotnických zařízení (ambulance, hospitalizace, vyšetření). V rámci systému eMeDocS jsou dále zpracovávány citlivé údaje o pacientovi, jemuž byla poskytnuta ZZS přednemocniční neodkladná péče ve smyslu § 2 odst. 1 zákona č. 374/2011 Sb., a to formou záznamu o výjezdu, jenž obsahuje citlivé údaje: důvod zásahu, informace o nynějším onemocnění (popis zdravotního stavu), podané léky a diagnóza a informace o umístění do zdravotnického zařízení. Kontrolovaná osoba za účelem výměny ZD, resp. za účelem předávání osobních a citlivých údajů pacientů vytvořila a provozuje komunikační infrastrukturu „eMeDocS", výměna ZD se uskutečňuje na principu přenosu zpráv, které mají definovanou strukturu a jsou založeny na standardu Ministerstva zdravotnictví ČR DASTA.

Během vlastní komunikace mezi jednotlivými koncovými body dle zjištění v kontrole nedochází k trvalému uložení přenášených osobních či citlivých údajů v Centru výměny zpráv.

V rámci systému jsou osobní, resp. citlivé údaje pacientů zpracovávány automatizovaně na straně správce osobních, resp. citlivých údajů pacientů, šifrovaně jsou pak přenášeny směrem k oprávněné osobě. Vzhledem k absenci elektronického podpisu v jednotlivých organizacích, zapojených vždy aktuálně do systému na základě smlouvy o využívání systému eMeDocS, probíhá komunikace při *Zasílání „Záznamu o výjezdu" do nemocnice, kam je pacient předán* a při *Zasílání elektronické žádanky na RDG vyšetření na pracoviště magnetické rezonance Nemocnice Jihlava*, vždy zároveň papírovou formou. V rámci výměny ZD dochází mezi poskytovateli zdravotních služeb, tj. mezi jednotlivými správci osobních, resp. citlivých údajů pacientů prostřednictvím Centra výměny zpráv k přenosu informací automatizovaně, v rámci systému eMeDocS tedy dochází ke zpracování osobních, resp. citlivých údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb.

Kontrolovaná osoba v rámci strategie v oblasti eHealth vytvořila komunikační infrastrukturu za účelem sdílení a výměny informací (eMeDocS) mezi zdravotnickými zařízeními, za tímto účelem zřídila komunikační centrum – Centrum výměny zpráv a auditní databáze, jednotlivá zdravotnická zařízení zapojená do systému jsou v rámci tohoto systému vybavena komunikačními uzly. Komunikační uzly přijímají zprávy a požadavky na vyhledání informací od jednotlivých uživatelů zdravotnických zařízení, a to prostřednictvím jejich NIS nebo webového uživatelského rozhraní. Komunikační uzel zajistí dle typu požadavku či zprávy informace z NIS a zajistí bezpečné odeslání informací komunikačnímu uzlu, který je instalován u příjemce zprávy nebo požadavku. Stejně tak komunikační uzel musí zajistit na straně příjemce příjem zprávy a její předání NIS, případně dohledání požadovaných formací v NIS a jejich předání žadateli.

V době kontroly systém eMeDocS využívalo celkem 19 poskytovatelů zdravotních služeb, a to na základě „Smlouvy o přístupu ke komunikační infrastruktuře eMeDocS". Poskytovatelé zdravotních služeb včetně ZZS (zřizovatelem ZZS je ve smyslu § 24 zákona č. 374/2011 Sb. Kontrolovaná osoba) zapojení do systému eMeDocS, poskytují zdravotní péči ve smyslu zákona č. 372/2011 Sb., zpracovávají osobní, resp. citlivé údaje pacientů na základě právního titulu vyplývajícího ze zákona č. 372/2011 Sb., účel a prostředky zpracování osobních údajů mají tato zdravotnická zařízení stanoveny ustanovením § 53 odst. 1 uvedeného zákona, dle něhož je zdravotnické zařízení povinno vést zdravotnickou dokumentaci pacienta a nakládat s ní podle tohoto zákona a jiných právních předpisů. Jednotlivá zdravotnická zařízení jsou ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. správci osobních a citlivých údajů pacientů, jejichž osobní, resp. citlivé údaje jsou vedeny v jejich NIS a které jsou předávány mezi jednotlivými zdravotnickými zařízeními zapojenými do systému eMeDocS. ZZS je správcem osobních, resp. citlivých údajů pacientů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., jimž poskytla přednemocniční bezodkladnou péči, při níž využila informací předávaných z NIS zdravotnických zařízení zapojených do systému eMeDocS.

K předávání informací o pacientech z jejich ZD vedené v NIS zdravotnických zařízení k ZZS, případně mezi jednotlivými zdravotnickými zařízeními dochází v souladu s ustanovením § 65 odst. 2 písm. a) zákona č. 372/2011 Sb., *„Do zdravotnické dokumentace vedené o pacientovi mohou bez jeho souhlasu nahlížet, jestliže je to v zájmu pacienta nebo jestliže je to potřebné pro účely vyplývající z tohoto zákona nebo jiných právních předpisů, a to v nezbytném rozsahu a) osoby se způsobilostí k výkonu zdravotnického povolání a jiní odborní pracovníci v přímé*

souvislosti s poskytováním zdravotních služeb, kteří jsou zaměstnanci poskytovatele, a další zaměstnanci poskytovatele v rozsahu nezbytně nutném pro výkon povolání, a dále z důvodu splnění úkolů podle tohoto zákona nebo jiných právních předpisů a při hodnocení správného postupu při poskytování zdravotních služeb". V daném případě nelze aplikovat zachování mlčenlivosti v souvislosti se zdravotními službami ve smyslu ustanovení § 51 odst. 1 zákona č. 372/2011 Sb., neboť dle odst. 2 písm. a) uvedeného zákona se *„za porušení mlčenlivosti nepovažuje předávání informací nezbytných pro zajištění návaznosti poskytovaných zdravotních služeb"*. Kontrolovaná osoba prostřednictvím systému eMeDocS určila pravidla a technické prostředky pro zajištění bezpečnosti provozu systému, tedy i bezpečnosti přenášených osobních a citlivých údajů, která vyplývají z technické dokumentace systému eMeDocS, předložené v rámci kontroly. Kontrolovaná osoba neporušila ustanovení § 13 odst. 1 zákona o ochraně osobních údajů.

V souladu s ustanovením § 13 odst. 2 zákona č. 101/2000 Sb. Kontrolovaná osoba v rámci kontroly dokumentovala přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů. Kontrolou bylo prověřováno plnění povinnosti ve smyslu ustanovení § 13 odst. 4 písm. c) zákona č. 101/2000 Sb., tj. povinnosti pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. Kontrolou bylo zjištěno, že informace o všech událostech v komunikačním uzlu se zaznamenávají do lokální auditní databáze, která je přístupná bezpečnostnímu manažerovi pro dohled, současně komunikační uzel odesílá anonymizované zprávy o auditních událostech do centrální auditní databáze v Centru eMeDocS prostřednictvím Centra výměny zpráv. Logy Centra výměny zpráv o přenesených zprávách jsou uchovávány trvale (tzv. „auditní databáze"). Kontrolovaná osoba tedy plní výše uvedenou povinnost.

Uvedenou kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb.

Kontrola zpracování osobních údajů cizinců umístěných v zařízení pro zajištění cizinců

(inspektorka Jiřina Rippelová)

Kontrola byla zahájena na základě podnětu předsedkyně Úřadu a byla zacílena na zpracování osobních údajů cizinců umístěných v zařízení pro zajištění cizinců v rámci provozního informačního systému (dále jen „Provozní IS"), který vede Správa uprchlických zařízení Ministerstva vnitra ČR na základě zmocnění v § 150 zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů.

De facto se jednalo o tři kontroly vedené paralelně s Ministerstvem vnitra ČR, se Správou uprchlických zařízení Ministerstva vnitra ČR a se Zařízením pro zajištění cizinců Bělá – Jezová (dále jen „Ministerstvo", „Správa UZ" a „ZZC Bělá – Jezová"). Důvodem tohoto postupu byl záměr posoudit zpracování osobních údajů cizinců umístěných v zařízení pro zajištění cizinců všemi subjekty, které se na zřizování, provozu a vedení těchto zařízení podílejí.

ZZC Bělá – Jezová a ostatní zařízení pro zajištění cizinců (dále jen „Zařízení") provozuje Správa UZ, organizační složka státu zřizovaná Ministerstvem, a to na základě zmocnění vyplývajícího ze zákona č. 326/1999 Sb. Do těchto zařízení jsou podle citovaného zákona umísťováni cizinci, u nichž příslušné orgány (Policie České republiky – Služba cizinecké policie, dále jen „Policie ČR") rozhodly o zajištění za účelem správního vyhoštění, vycestování nebo za účelem předání či průvozu.

Správa UZ zajišťuje cizincům umístěným v Zařízení zejména ubytování, stravu a základní hygienické prostředky. Umožňuje jim přijímat a odesílat písemná sdělení a přijímat návštěvy. Dále zajišťuje, aby cizinci umístění v Zařízení mohli podat žádost nebo jiný podnět státním orgánům České republiky nebo mezinárodním organizacím za účelem uplatnění svých práv. Cizincům umístěným v Zařízení jsou také, v případě potřeby, poskytovány psychologické a sociální služby.

Pro zajištění vnitřního provozu Zařízení a pro zajištění práv a právem chráněných zájmů cizinců zde umístěných vede Správa UZ, v souladu s § 150 zákona č. 326/1999 Sb., Provozní IS, který je informačním systémem ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých zákonů. Kontrolou bylo zjištěno, že Správa UZ je ve vztahu k osobním údajům zpracovávaným v Provozním IS v postavení správce osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb. a Zařízení, včetně konkrétně kontrolovaného ZZC Bělá – Jezová, jsou v pozici zpracovatele osobních údajů ve smyslu § 4 písm. k) tohoto zákona vůči osobním údajům cizinců umístěných v daném Zařízení. Ministerstvo naopak v Provozním IS žádné osobní údaje nezpracovává, tj. ani nevkládá, ani jinak tento systém nevyužívá – z pohledu zákona č. 101/2000 Sb. tedy nemá za zpracování osobních údajů cizinců v Provozním IS žádnou odpovědnost.

Co se týče účelu zpracování osobních údajů, vyplývá z příslušných právních předpisů a z kontrolních zjištění, že v Provozním IS jsou zpracovávány osobní údaje v rozsahu, který je nezbytný pro plnění povinností Správy UZ při ochraně zdraví cizince a jeho základních práv, dále pro plnění povinností a oprávnění, které má Správa UZ vůči cizinci podle zákona č. 326/1999 Sb., a také pro zajištění vnitřního provozu Zařízení, jejich organizaci a financování.

Kontrolou bylo zjištěno, že obsahem Provozního IS jsou jednak identifikační osobní údaje cizinců (zejména jméno, příjmení, datum narození, státní příslušnost), a to včetně fotografie cizince, pokud cizinec ke vložení fotografie poskytl souhlas, a jednak řada dalších informací, které se k danému cizinci přiřazují s ohledem na to, jak probíhá jeho pobyt v Zařízení, jaké zde má rodinné příslušníky, jaká uplatňuje práva apod.

Vzhledem k tomu, že každý cizinec je v Provozním IS jednoznačně identifikován, je z pohledu zákona č. 101/2000 Sb. každá z informací, které jsou k jednotlivým cizincům dále přiřazeny (a uchovávány), osobním, případně i citlivým údajem podle § 4 písm. a), popř. b) tohoto zákona.

Příkladem lze uvést, že zpracovávány jsou údaje vypovídající o tzv. sociální anamnéze cizince, tedy o jeho vazbách na případné rodinné příslušníky umístěné v Zařízení (informace o tom, zda se jedná o samostatnou ženu, muže, rodinu nebo samostatného nezletilého cizince) – tyto informace slouží dále k rozhodnutí o konkrétním typu ubytování, kdy Správa UZ, resp. jednotlivá Zařízení respektují právo rodin na společné ubytování, popř. zájmy nezletilých na oddělené (chráněné) bydlení. Z hlediska zajištění základních potřeb cizinců je dále zpracovávána informace o preferované stravě, tedy zda cizinec zvolil evropskou, muslimskou či vegetariánskou variantu (ovšem bez dalšího ověřování, zda jeho volba skutečně koresponduje s náboženským vyznáním či přesvědčením). K naplnění zákonných požadavků na maximální lhůty zajištění jsou dále evidovány termíny příchodu a ochodu cizince do a ze Zařízení, včetně zákonných důvodů. Cizinci umístění v Zařízení mají dále nárok na dvě návštěvy (rodinného charakteru) v rozsahu jedné hodiny týdně, z tohoto důvodu jsou v Provozním IS zpracovávány také informace o datu a jménu návštěvy.

Současně bylo zjištěno, že v Provozním IS jsou zpracovávány i údaje vypovídající o etnickém či rasovém původu cizince vyplývající v některých případech z pořízené fotografie, informace

o stravovacích preferencích, z nichž lze alespoň v některých případech (popř. v kombinaci s dalšími informacemi) dovodit náboženství či filozofické přesvědčení cizince a informace o zdravotním stavu cizince vyplývající z dietologického omezení nebo z informace o zdravotním postižení cizince. Je tedy zřejmé, že v Provozním IS jsou zpracovávány osobní i citlivé údaje.

Pokud se týká právního titulu ke zpracování osobních údajů v Provozním IS, bylo již výše uvedeno, že Správa UZ disponuje ke zřízení a provozu tohoto informačního systému zákonným zmocněním (v § 150 zákona č. 326/1999 Sb.), v němž je definován i účel, který má zpracování osobních údajů v Provozním IS naplnit. Po srovnání vymezeného účelu zpracování osobních údajů a zjištěného rozsahu těchto osobních údajů byl učiněn závěr, že v Provozním IS jsou zpracovávány osobní údaje na základě právního titulu uvedeného v § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., neboť se jedná o zpracování nezbytné pro dodržení právní povinnosti správce osobních údajů. Ve vztahu k citlivým údajům zachyceným na fotografiích cizinců pak Správa UZ, resp. Zařízení získávají výslovný souhlas dle § 9 písm. a) citovaného zákona, i bez takového souhlasu by ale toto zpracování bylo možné na základě § 9 písm. h) zákona č. 101/2000 Sb., a to s ohledem na účel zpracování těchto údajů, tj. zajištění provozu Zařízení, v němž jsou cizinci z povahy věci umístěni proti své vůli a zároveň je třeba je navzájem důsledně odlišit, aby bylo možno uplatnit veškerá oprávnění Správy UZ vůči těmto osobám, a garantovat všechna práva, která těmto osobám svědčí. Obdobně v případě zpracování citlivých údajů vyplývajících z informací o stravovacích preferencích a citlivých údajů o zdravotním stavu cizince lze přiznat právní titul v § 9 písm. h) zákona č. 101/2000 Sb., tedy dochází ke zpracování nezbytnému pro zajištění a uplatnění právních nároků Správy UZ.

Kontrolou bylo dále zjišťováno, zda a jak Zařízení plní své povinnosti v oblasti informování subjektů údajů a povinnosti odpovídající jejich dalším právům (např. právo na vysvětlení, opravu či výmaz chybných údajů). V tomto směru bylo zjištěno, že informace o režimu v Zařízení, včetně důvodu zpracování určitých osobních údajů, jsou cizincům poskytovány v rámci pohovoru bezodkladně po přijetí do Zařízení, kdy jsou doplňovány informace do Provozního IS. Pro tyto účely jsou zaměstnancům Zařízení k dispozici překladatelé a tam, kde je to nezbytné, využívají se pro vysvětlení piktogramy i jiné formy nonverbální komunikace.

V neposlední řadě bylo hodnoceno, jakým způsobem je zajištěna bezpečnost osobních údajů zpracovávaných v Provozním IS. Správa UZ upravila požadavky na zabezpečení osobních údajů zpracovávaných v Provozním IS v několika interních předpisech. Na základě těchto interních norem je přístup k osobním a citlivým údajům zpracovávaným v Provozním IS omezen pouze na oprávněné osoby v rámci daného Zařízení a na osoby s administrátorským oprávněním ze Správy UZ. Jiné subjekty, popř. orgány, nemají do tohoto Provozního IS přístup. Tyto osoby disponují individuálními přístupovými jmény a hesly a jsou proškoleny o jejich využívání. Přijatá opatření zohledňují také požadavky na fyzickou bezpečnost zpracovávaných dat (tj. fyzické zabezpečení prostor, kde jsou osobní údaje uchovávány, a to jak na úrovni Zařízení, tak na úrovni Správy UZ). Současně jsou realizovány pravidelné kontroly dodržování stanovených pravidel při zpracování osobních údajů.

Osoby oprávněné zpracovávat osobní údaje cizinců jsou dále vázány povinností mlčenlivosti, která je jim uložena jak interními předpisy, tak v pracovní smlouvě. Zjištěná opatření směřující k zajištění bezpečnosti zpracovávaných osobních údajů byla proto kontrolou shledána jako vyhovující požadavkům stanoveným v § 13 zákona č. 101/2000 Sb.

Závěrem lze shrnout, že úroveň ochrany osobních údajů zpracovávaných v Provozním IS v ZZC Bělá – Jezová, resp. Správou UZ zjištěná při kontrole zcela odpovídala požadavkům zákona č. 101/2000 Sb., a to včetně garancí práv subjektů údajů.

Bytové družstvo – provozování kamerového systému v domech a evidence držitelů přístupových čipů (inspektorka Jiřina Rippelová)

Kontrolu Úřad zahájil na základě obdrženého podnětu, který upozorňoval na nedostatky při zpracování osobních údajů obyvatel bytového domu v souvislosti s vydáváním a vedením evidence přístupových čipů a dále při provozování kamerového systému v domě. Úřad tedy provedl kontrolu bytového družstva, která byla zaměřena na dodržování povinností správce osobních údajů stanovených v hlavě II zákona č. 101/2000 Sb., zejména pak ustanovení § 5, § 11, § 13 a § 16 citovaného zákona.

Kontrolou bylo zjištěno, že v předmětném bytovém domě (tvořeném 280 bytovými jednotkami) je nainstalováno celkem 31 kamer, které však prozatím nejsou uvedeny do provozu, tj. zatím nepořizují a doposud nikdy nepořizovaly záznam a ani nefungují v režimu on-line. Co se týče kamerového systému, bylo tedy shledáno, že ke zpracování osobních údajů nedochází a působnost zákona č. 101/2000 Sb., ani Úřadu tak není dána.

Provozování čipového systému a s tím související vedení evidence přidělených čipů, které majitelům čipů umožňují vstup do domu, bylo naopak kontrolou potvrzeno, a tedy i hodnoceno z hlediska souladu s požadavky zákona č. 101/2000 Sb. Bylo zejména zjištěno, že předmětný systém je nastaven pouze v základní softwarové úrovni, tzn. že čip funguje obdobně jako klíč, ale již nedochází k záznamu čísla použitého čipu ve vztahu k datu a času vstupu do domu. V souvislosti s provozem čipového systému tedy nedochází ke zpracování osobních údajů fyzických osob, kterým byl čip přidělen, a není důvodné hodnotit plnění povinností plynoucích pro správce či zpracovatele osobních údajů ze zákona č. 101/2000 Sb.

V souvislosti s provozem čipového systému nicméně bytové družstvo vede evidenci všech osob, kterým byl konkrétní přístupový čip do domu vydán. Dle kontrolních zjištění byly čipy vydávány jak členům družstva a členům jejich domácnosti, tak i jiným osobám, které v předmětném domě bydlely, a dále také osobám, kterým nájemce bytu zamýšlel umožnit vstup do domu (příbuzní, známí, podnájemníci apod.). V době kontroly bylo vydáno již cca 1200 čipů a bytové družstvo shromažďovalo a vedlo evidenci osobních údajů těchto osob za účelem blokování konkrétního přístupového čipu v případě jeho ztráty a odcizení tak, aby do domu neměly přístup nepovolané osoby.

Bytové družstvo zvolilo takový přístup, kdy vydávalo jednotlivé čipy žadatelům pouze v případě, že každý žadatel o čip vyplnil formulář o předání čipů pro vstup do domu, v němž uvedl své osobní údaje v rozsahu jméno, příjmení, číslo občanského průkazu či jiného dokladu totožnosti, adresa trvalého pobytu, adresa pro doručování, telefon a podpis. K těmto osobním údajům dále bytové družstvo připojilo údaj o čísle přiděleného čipu a datu předání čipu. Součástí vyplňovaného formuláře byl i text, na jehož základě žadatel o čip bytovému družstvu poskytoval souhlas se zpracováním osobních údajů v uvedeném rozsahu.

Pokud by žadatel o čip odmítl poskytnout výše uvedené osobní údaje anebo odmítl podepsat souhlas se zpracováním osobních údajů, bytové družstvo vydání čipu pro vstup do domu odepřelo a tyto osoby odkázalo na možnost vstupu do domu dveřmi, u nichž byl ponechán

klíčový systém. Ačkoli byly v každé ze tří sekcí bytového domu ponechány jedny takové dveře, je zjevné, že přístup osob, které odmítly poskytnout bytovému družstvu požadované osobní údaje, k jejich bytu byl tímto opatřením ztížen.

Tento postup bytového družstva byl posouzen jako odporující požadavkům vyjádřeným v § 5 odst. 1 písm. d) zákona č. 101/2000 Sb., tedy bytové družstvo shromažďovalo osobní údaje, které nebyly nezbytné k naplnění stanoveného účelu. Dle Úřadu je pro naplnění účelu (zjištění konkrétního přiděleného kódu při ztrátě nebo odcizení vstupního čipu, vymazání konkrétního kódu ze systému tak, aby do domu nemohla vstupovat cizí osoba a možnost vydání, nahrání, jiného přístupového kódu konkrétní osobě) plně dostačující zpracování osobních údajů nájemce bytové jednotky v rozsahu číslo bytové jednotky, jméno, příjmení nájemce, počet předaných čipů včetně evidenčních čísel čipů, data předání čipů a podpis nájemce bytové jednotky. Ostatní osobní údaje nájemců bytů a všechny osobní údaje osob bydlících v bytovém domě, resp. docházejících do tohoto domu, zpracovávalo bytové družstvo v rozporu se zákonem.

Konkrétní zpracování osobních údajů je dle názoru Úřadu vždy nutno vztáhnout ke konkrétnímu správci osobních údajů, jím stanovenému účelu a specifickým okolnostem daného zpracování. Jestliže bytové družstvo stanovilo jako účel zpracování osobních údajů správu vstupních čipů (včetně zajištění blokování konkrétních čipů v případě jejich ztráty či odcizení a včetně přidělení náhradního čipu), není možné, aby k tomuto účelu zpracovávalo tak rozsáhlé množství osobních údajů, jak bylo kontrolou zjištěno. Správu čipů ke vstupním dveřím bylo v daném případě možné zajistit jinými prostředky, resp. za použití výrazně menšího rozsahu zpracovávaných údajů, a tedy s menším zásahem do práv fyzických osob na ochranu jejich soukromí.

V případě dalších povinností, které správci osobních údajů ze zákona č. 101/2000 Sb. vyplývají (např. dle § 13 a 16 tohoto zákona), došla kontrola k závěru, že k žádnému pochybení nedošlo.

Bytové družstvo ještě v průběhu kontroly přistoupilo k částečné nápravě zjištěného stavu, proti kontrolním zjištění uvedeným v protokole o kontrole nicméně podalo námitky. Předsedkyně Úřadu podaným námitkám však nevyhověla, a tím byla kontrola ukončena.

Na základě skutečností zjištěných v průběhu kontroly byl následně vydán příkaz, kterým Úřad bytovému družstvu uložil opatření k odstranění zjištěných nedostatků. Bytovému družstvu bylo uloženo zlikvidovat osobní údaje, které na základě kontrolních zjištění zpracovávalo nadbytečně (resp. v rozporu se zákonem č. 101/2000 Sb.) konkrétně osobní údaje všech osob vyjma nájemce bytu a k němu se vztahujícím informacím o počtu vydaných čipů a jejich kódu. Bytové družstvo uložené opatření ve stanovené 30denní lhůtě splnilo, o čemž následně Úřad písemně informovalo.

Za spáchání správního deliktu dle § 45 odst. 1 písm. c) zákona č. 101/2000 Sb. Úřad bytovému družstvu uložil pokutu ve výši 80.000 Kč.

Generální ředitelství cel – neoprávněná lustrace registračních značek vozidel v registru silničních vozidel (inspektorka Jiřina Rippelová)

Kontrolu Generálního ředitelství cel (dále také „GŘC“ nebo „Kontrolovaná osoba“) provedl Úřad na základě doručeného podnětu, jehož obsahem bylo upozornění na hromadnou lustraci 113 registračních značek (dále jen „RZ“) majitelů vozidel v registru silničních vozidel parkujících v areálu GŘC.

Předmětem kontroly bylo dodržování povinností kontrolovaného stanovených v hlavě II zákona č. 101/2000 Sb., zejména pak ustanovení § 5 a 13 citovaného zákona, kde jsou jednak

upraveny základní podmínky pro zákonnost zpracování a jednak požadavky na zajištění bezpečnosti zpracovávaných osobních údajů.

Kontrolou bylo zjištěno, že vedení GŘC si vyžádalo prostřednictvím svého Operačního centra lustraci RZ vozidel za účelem zjištění majitelů vozidel parkujících v areálu GŘC. Důvodem identifikace vlastníků vozidel byla dle kontrolovaného zhoršená bezpečnostní situace v ČR a podezření na protiprávní umístění vozidel v areálu bezpečnostního sboru.

Hromadnou lustrací RZ vozidel GŘC shromáždilo osobní údaje o 43 fyzických osobách (vlastnících vozidel), a to v rozsahu jméno, příjmení a RZ vozidla. K těmto údajům GŘC přiřadilo údaj o tom, zda je vlastník vozidla zaměstnancem Celní správy a kód útvaru GŘC, do kterého je zaměstnanec zařazen.

Kontrolující posuzovali, zda Kontrolovaná osoba v pozici správního úřadu disponovala k provedení této hromadné lustrace legálním a legitimním právním titulem a zda postupovala pouze v mezích a způsoby, které ve vztahu ke zpracování osobních údajů stanoví zákon. Oprávnění Kontrolované osoby přistupovat k registru silničních vozidel (jehož správcem je Ministerstvo dopravy ČR) vyplývá ze zákona č. 17/2012 Sb., o Celní správě České republiky. Orgány celní správy mohou o informace z uvedeného registru nicméně žádat pouze v rozsahu potřebném pro plnění konkrétního úkolu při výkonu své působnosti, přičemž rozsah úkolů, při jejichž plnění je kontrolovaný oprávněn o informace žádat a věcná působnost Kontrolované osoby jsou stanoveny v § 4 zákona č. 17/2012 Sb. Podle § 4 odst. 2 písm. b) zákona č. 17/2012 Sb., se GŘC mimo jiné podílí na „zabezpečování analytických a koncepčních úkolů".

Jak bylo uvedeno výše, stanovila Kontrolovaná osoba jako účel lustrace předmětných RZ ověření oprávněnosti majitelů vozidel parkovat na parkovišti v areálu GŘC. V rámci dotazu vzneseného do registru silničních vozidel však odkázal na svoji pravomoc vyplývající z citovaného zákona č. 17/2012 Sb., tedy oprávnění požadovat informace z registru silničních vozidel v rámci zabezpečování analytických a koncepčních úkolů.

Kontrolou tak bylo zjištěno, že Kontrolovaná osoba v případě této lustrace RZ postrádala zákonné zmocnění pro zpracování osobních údajů, neboť ve skutečnosti neprováděla činnost, kterou by bylo možno podřadit pod citovaný § 4 odst. 2 zákona č. 17/2012 Sb., a tedy nebylo možné na její postup aplikovat zákonné zmocnění uvedené v § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., podle kterého je zpracování osobních údajů možno považovat za zákonný postup za předpokladu, že se jedná o plnění zákonných povinností správce či zpracovatele osobních údajů.

V souladu s ustáleným výkladem Úřadu je pro aplikaci právního titulu podle § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. nezbytné, aby zákonné zmocnění, na které se správce či zpracovatel odvolává, bylo dostatečně určité, tedy buď zpracování osobních údajů výslovně ukládalo, anebo stanovilo takovou povinnost, jejíž naplnění není bez zpracování osobních údajů možné. Zabezpečení analytických a koncepčních úkolů je naopak z povahy věci možné s využitím anonymních či anonymizovaných dat. Výše uvedené jednání GŘC bylo proto kontrolujícími posouzeno jako porušení ustanovení § 5 odst. 2 zákona č. 101/2000 Sb.

V této souvislosti je vhodné uvést, že s ohledem na to, že Kontrolovaná osoba je v pozici správního úřadu, který v souladu s čl. 2 odst. 3 zákona č. 1/1993 Sb., Ústava České republiky, smí postupovat pouze v mezích a způsoby, které stanoví zákon, a to i ve vztahu ke zpracování osobních údajů, připadá v úvahu pouze zpracování osobních údajů na základě § 5 odst. 2 písm. a) zákona č. 101/2000 Sb.

Kontrola se rovněž zaměřila na posouzení, zda Kontrolovaná osoba jako správce osobních údajů získaných lustrací RZ v registru vozidel přijala taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Kontrolující shledali, že Kontrolovaná osoba přijala vnitřní pokyny a stanovila pravidla pro postup při poskytování informační podpory (tj. při dotazování do registru silničních vozidel) orgánům CS a dalším oprávněným subjektům. Vnitřní pokyn upravuje i obsah žádosti o informační podporu, přičemž je v něm výslovně zakázáno do žádosti uvádět smyšlené a nepravdivé údaje a požadovat poskytnutí informační podpory pro účely nesouvisející s plněním služebních nebo pracovních povinností. V posuzovaném případě nicméně jednaly odpovědné osoby v rozporu s těmito interními předpisy, když nejdříve vedení GŘC vydalo pokyn k provedení lustrace RZ vozidel a následně byla tato lustrace provedena s odkazem na plnění úkolů GŘC, což neodpovídalo skutečnosti.

Kontrolovaná osoba tedy sice přijala organizační a technická opatření k zabezpečení zpracování osobních údajů zpracovávaných v Registru silničních vozidel, a to včetně mechanismu kontrol plnění těchto opatření, nicméně tato opatření v praxi důsledně neprovedla, v důsledku čehož došlo k neoprávněnému přístupu k osobním údajům, a tím i k porušení § 13 odst. 1 zákona č. 101/2000 Sb.

Kontrolovaná osoba podala proti kontrolnímu zjištění konstatujícímu porušení § 13 odst. 1 zákona č. 101/2000 Sb. obsaženému v protokolu o kontrole námitku, které předsedkyně Úřadu nevyhověla. V návaznosti na kontrolní zjištění vedl Úřad správní řízení, ve kterém byla za výše popsané jednání uložena sankce ve výši 40.000 Kč.

Závěrem lze uvést, že v případě využívání veřejnoprávních registrů a rejstříků státními orgány je z pohledu Úřadu nutno vždy striktně vyžadovat naplnění právního titulu dle § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., neboť v mnoha případech se jedná o registry obsahující značné množství informací, jejichž zneužití by mohlo vést k závažnému zásahu do práv subjektů údajů. Obdobně zásadní je požadavek na jasná interní pravidla pro zpracování osobních údajů, jejichž dodržování je současně pravidelně kontrolováno a vymáháno.

Ministerstvo práce a sociálních věcí (dále jen „MPSV" nebo „ministerstvo") – plnění povinností správce při zabezpečení osobních údajů žadatelů o dávky a zaměstnanců MPSV a Úřadu práce ČR (inspektorka Božena Čajková)

Kontrola MPSV a společností Fujitsu a VITSOL byla zahájena na základě pokynu předsedkyně Úřadu reagujícího na podnět Národního bezpečnostního úřadu. Z obsahu podnětu vznikala obava ze zneužití zálohovaných dat ministerstva a úřadů práce v externích datových centrech, z jejich řádného vrácení a nevratné likvidace společnostmi (zpracovateli podle zákona č. 101/2000 Sb.).

MPSV přistoupilo k Prováděcí smlouvě (smlouva uzavřená Ministerstvem vnitra ČR se společností Fujitsu), na jejímž základě došlo k modifikaci smluvního vztahu postupným uzavíráním dodatků. Předmětem dodatků byl závazek společnosti poskytovat ministerstvu a úřadům práce služby, spočívající v poskytování pronájmu výpočetní kapacity v externích datových centrech, na nichž byly provozovány nejen informační systémy zajišťující výplaty nepojistných sociálních dávek a dávek státní politiky zaměstnanosti, ale i informační systémy pro Identity management a elektronickou spisovou službu ministerstva a úřadů práce. Uvedené služby pak pro Fujitsu zajišťovala společnost VITSOL.

Z obsahu podnětu vznikla obava, že při ukončení smluvního vztahu ministerstva se společnostmi by mohlo dojít ke zneužití zálohovaných dat v externích datových centrech, z jejich řádného vrácení a nevratné likvidace dat. Aby kontrolující eliminovali reálné riziko, vydali Rozhodnutí o nařízení předběžného opatření. Společnostem tak bylo nařízeno zdržet se a zabránit jakékoliv činnosti, která by vedla ke změně či výmazu dat (osobních údajů žadatelů sociálních dávek, zaměstnanců a souvisejících provozních dat MPSV a úřadů práce).

V souvislosti s výše uvedeným byla kontrola zaměřena na plnění povinností ministerstva při zabezpečení osobních údajů žadatelů o dávky a zaměstnanců, zejména pak na přijetí technicko-organizačních opatření při ukončení smluvního vztahu se společnostmi při procesu řádného vrácení veškerých zálohovaných dat MPSV, úřadů práce, nevratné likvidace osobních údajů a dále přijetí opatření při kontrole přístupů k záznamům o činnostech se zálohovanými daty v externích datových centrech (k tzv. logům).

Společnosti v datových centrech zálohovaly (zpracovávaly) velký rozsah osobních údajů nejen žadatele o sociální dávky, který je nezbytný shromažďovat a dále zpracovávat za účelem přiznání jednotlivých dávek (např. jméno, příjmení, rodné příjmení, datum a místo narození, rodné číslo, adresa bydliště, telefon, e-mail, datová schránka, číslo občanského průkazu, číslo cestovního dokladu, číslo karty sociálního systému, číslo bankovního účtu), ale i některých osobních údajů společně posuzovaných osob žadatele o příspěvek či dávku. Dále v souladu se zákonem č. 329/2011 Sb., o poskytování dávek osobám se zdravotním postižením a o změně souvisejících zákonů, byly zálohovány i citlivé údaje vypovídající o zdravotním stavu žadatele (zdravotní postižení). V souvislosti se správou informačních systémů pro Identity management a elektronickou spisovou službu byly v externích datových centrech zálohovány i další osobní údaje (zaměstnanců MPSV a úřadů práce).

Podle Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, se řadí informační systémy ministerstva mezi kritické systémy, a proto je nezbytné, aby správci takovýchto systémů důsledně plnili povinnosti při zabezpečení osobních údajů. V případě, kdy ministerstvo jako správce dle zákona č. 101/2000 Sb. pověří zpracováním osobních údajů zpracovatele (společnost), musí postupovat v souladu s § 6 zákona č. 101/2000 Sb. Toto ustanovení zákona deklaruje, že: „*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*“.

Kontrolující vyhodnotili obsah smluvních ujednání ministerstva se společností Fujitsu, zejména Prováděcí smlouvu a její postupně uzavírané dodatky. Tyto nejenže neobsahovaly záruky společnosti (zpracovatele) o technickém a organizačním zabezpečení ochrany osobních údajů, ale neupravovaly ani konkrétní postupy a opatření smluvních stran při ukončení smluvního vztahu v souvislosti se zpracováním osobních údajů. Ministerstvo tak porušilo citované ustanovení § 6 zákona č. 101/2000 Sb.

Dále se kontrolující zaměřili na plnění povinnosti ministerstva při zabezpečení osobních údajů žadatelů o dávky a dalších posuzovaných osob zálohovaných v datových centrech. Podle § 13 odst. 1 zákona č. 101/2000 Sb. je „*správce a zpracovatel povinen přijmout taková opatření, 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". Podle odst. 2 téhož ustanovení zákona je „*správce nebo zpracovatel povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.*" Odst. 4 písm. c) § 13 citovaného zákona ukládá správci nebo zpracovateli povinnost „*pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány*".

Kontrolující vyhodnotili zjištěný stav a konstatovali, že v průběhu ukončování služeb se společnostmi ministerstvo v souvislosti s vrácením záloh a likvidací dat přijalo dostatečná technicko-organizační opatření ve smyslu ustanovení § 13 odst. 1 a odst. 2 zákona č. 101/2000 Sb.

Podle smluvních ujednání se společnostmi nemělo ministerstvo přístup k záznamům o činnosti se zpracovávanými daty v datových centrech (k tzv. logům). Ze strany MPSV jako správce tak bylo nezbytné přijmout podle § 13 odst. 1 zákona č. 101/2000 Sb. opatření související s pravidelnou kontrolou oprávněnosti přístupů k datům uloženým v datových centrech. Kontrolou bylo zjištěno, že během trvání smluvního vztahu, tj. od přistoupení k Prováděcí smlouvě, ministerstvo neplnilo kontrolní činnost směrem k ustanovení § 13 odst. 4 písm. c), a tím porušilo povinnost vyplývající z § 13 odst. 1) zákona č. 101/2000 Sb., a v důsledku tak ztratilo průběžnou kontrolu nad nakládáním s produkčními daty zálohovanými v externích datových centrech.

Kontrolující se v rámci provedené kontroly zaměřili i na přijetí opatření při likvidaci osobních údajů v datových centrech v souvislosti s ukončením smluvního vztahu se společnostmi. MPSV spolu se společnostmi stanovilo jednoznačný postup pro likvidaci dat a kontrolující konstatovali, že provedená opatření, na nichž se MPSV aktivně podílelo, znemožnilo zneužití dat před jejich smazáním a vybraný způsob smazání dat zaručoval vysoký stupeň účinné likvidace dat.

Za spáchání správního deliktu dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. Úřad ministerstvu uložil pokutu ve výši 150.000 Kč.

Obvodní soud v Praze – zpracování osobních údajů žadatelů o osvobození od soudních poplatků (inspektorka Božena Čajková)

Kontrola byla provedena na základě podnětu doručeného Úřadu, který se týkal zpracování osobních údajů žadatelů o osvobození od soudních poplatků, konkrétně skutečnosti, že příslušný soud vede veškerou dokumentaci k této žádosti přímo v soudním spise, a informace zde uváděné jsou tak dostupné všem, kterým svědčí právo na nahlížení do spisu.

Jelikož účastníky soudních řízení je z povahy věci nezbytné vždy přesně identifikovat, je zřejmé, že veškerá podání, která vůči soudu učiní, resp. veškeré informace, které sdělí na podporu svých tvrzení, obsahují osobní údaje a v některých případech i údaje citlivé ve smyslu § 4 písm. a) anebo b) zákona č. 101/2000 Sb.

Účel a prostředky zpracování osobních údajů soudy jsou stanoveny zvláštními právními předpisy (tedy nikoli soudem samotným), v obdobných případech se má nicméně dle Úřadu za to, že správce osobních údajů byl určen zvláštním zákonem, kterým je mu předmětné zpracování uloženo, v tomto případě i včetně prostředků zpracování. Příslušný soud je tedy správcem osobních údajů dle § 4 písm. j) zákona č. 101/2000 Sb. a je odpovědný za plnění povinností tímto zákonem stanovených.

Z příslušných právních předpisů je zřejmé, že veškeré písemnosti, které účastník řízení soudu předloží, musí být zařazeny do spisu, přičemž není právem ani povinností soudu, aby odmítal jakékoliv informace a podklady do soudního spisu zařadit. Veškerá podání, tj. veškeré osobní,

případně citlivé údaje v nich uvedené, doručená soudu v rámci řízení vedeného před soudem, jsou tedy v souladu s platnými právními předpisy založena do příslušného soudního spisu. Tento postup má oporu ve vyhlášce č. 37/1992 Sb., o jednacím řádu pro okresní a krajské soudy. Nakládání se spisy podléhá také úpravě uvedené v interní instrukci Ministerstva spravedlnosti ČR č. 505/2001, kterou se vydává vnitřní a kancelářský řád pro okresní, krajské a vrchní soudy (dále jen „Instrukce ministerstva").

Z podkladů shromážděných v rámci kontroly a z příslušných právních předpisů je tedy zjevné, že soud je jednak povinen řádně identifikovat všechny účastníky řízení, příp. i další na řízení zúčastněné osoby, a současně je povinen od těchto osob přijímat veškeré listiny (podklady, dokumenty) a zakládat je do příslušných soudních spisů, a to aniž by měl vliv na obsah těchto listin. Rozsah osobních nebo i citlivých údajů, které soud v rámci soudních spisů zpracovává, je tak do značné míry dán předmětem sporu, který určuje žalobce, a obsahem listin, které jednotliví účastníci soudu předkládají.

Co se týče právního titulu (zákonem předvídaného důvodu) pro zpracování osobních údajů, byl v tomto případě učiněn závěr, že právním titulem pro zpracování osobních údajů účastníků řízení, příp. i dalších na řízení zúčastněných osob, je § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., tedy že soud svým postupem plní povinnosti uložené zvláštními zákony. V případě citlivých údajů lze právní titul pro zpracování nalézt v § 9 g) a h) citovaného zákona, tedy že se jedná o zpracování nezbytné pro uplatnění právních nároků subjektu údajů, případně údajů zveřejněných subjekty údajů. Zvláštními právními předpisy, které stanoví podmínky vedení soudních spisů jednotlivými soudy, jsou pak vyhláška č. 37/1992 Sb. a Instrukce ministerstva.

Někteří účastníci soudních řízení mohou (na základě §138 zákona č. 99/1963 Sb., Občanský soudní řád) také podat žádost o osvobození od soudních poplatků. Kontrolou bylo zjištěno, že k této žádosti se připojuje vyplněný formulář, který obsahuje identifikační údaje žadatele (jméno, datum narození, rodné číslo, adresa trvalého bydliště) a další informace, např. rodinný stav, výše příjmu, údaj o zaměstnavateli, informace, zda žadatel pobírá sociální dávky a v jaké výši, případně zda má příjmy z podnikání, osobní majetek, nějaké závazky či vyživovací povinnost (a to vč. jména vyživovaných, příbuzenského poměru a výše jejich příjmu), dále informace o manželovi/manželce a jeho/její majetkové poměry.

V případě, kdy je dle žadatele o osvobození od soudních poplatků důvodem žádosti jeho zdravotní stav, mohou být v žádosti a formuláři uvedeny informace o zdravotním stavu, popř. bývají také přiloženy lékařské zprávy apod.

Na základě žádosti o nahlédnutí do spisu je soud povinen zpřístupnit spis, a to účastníkům soudních řízení, jejich zástupcům a těm, kteří prokáží svůj právní zájem. Za situace, kdy součástí hlavního spisu je i spisový materiál k řízení o osvobození od soudních poplatků, který obsahuje osobní údaje žadatele, případně i citlivé údaje (typicky informace vypovídající o zdravotním stavu), zahrnuje právo na seznámení se s obsahem spisu, případně i právo na pořízení výpisů, opisů či kopií, také tyto dokumenty, resp. údaje.

S ohledem na fakt, že dle zákona č. 99/1963 Sb. řízení ohledně osvobození od soudních poplatků se týká jen toho účastníka, který návrh na osvobození od soudních poplatků uplatnil, a také pouze jemu se doručuje usnesení soudu, dospěl Úřad v dané kontrole k závěru, že soud v rámci zpracování osobních, případně i citlivých údajů, postupoval na základě zákonného zmocnění, současně však nedbal práva subjektů údajů na ochranu soukromého a osobního života subjektu údajů, a jednal tedy v rozporu s povinností vyjádřenou v § 5 odst. 3 zákona č. 101/2000 Sb.

Městská policie Hlavního města Prahy (inspektorka Božena Čajková)

Kontrola zpracování osobních údajů v souvislosti s pořizováním videozáznamů z průběhu úkonů strážníků Městské policie Hlavního města Prahy (dále jen „MP HMP") byla provedena na základě stížnosti, směřující proti zveřejnění konkrétního videozáznamu zákroku strážníků MP HMP prostřednictvím serveru pro sdílení videí YouTube, na vysílacím kanálu DS MP HMP a na vlastní webové stránce MP HMP (dále společně jen „internet"). Předmětem záznamu, kterého se stížnost týkala, bylo provádění identifikace a dechové zkoušky na přítomnost alkoholu v krvi u stěžovatelky.

Kontrolou bylo zjištěno, že strážníci MP HMP pořizují o průběhu některých svých zákroků – v případě, kdy to vyhodnotí jako potřebné pro plnění jejich úkolů – videozáznamy, které následně zálohují v datovém úložišti MP HMP. V okamžiku pořízení záznamu a při dalším zpracování těchto záznamů jsou osoby na nich zachycené z pohledu MP HMP jednoznačně identifikovány, popř. identifikovatelné za pomoci dalších informací, které mají strážníci k dispozici. Jedná se tedy nepochybně o osobní údaje dle § 4 písm. a) zákona č. 101/2000 Sb. vypovídající jak o identitě, tak o chování konkrétních osob. MP HMP je potom ve vztahu k těmto záznamům v pozici správce osobních údajů dle § 4 písm. j) zákona č. 101/2000 Sb.

Oprávnění k pořizování obdobných záznamů vyplývá MP HMP z § 24b odst. 1 zákona č. 553/1991 Sb., o obecní policii, podle kterého jsou strážníci městské policie oprávněni pořizovat zvukové, obrazové nebo jiné záznamy o průběhu zákroků nebo úkonů z míst veřejně přístupných, je-li to potřebné pro plnění jejich úkolů podle tohoto nebo jiného zákona.

Strážníci MP HMP pořizují videozáznam v situaci, kdy tento postup vyhodnotí jako účelný pro ochranu své osoby (pro následné posuzování legálnosti provádění zákroku či úkonu nebo v případě zákroku proti agresivní osobě), pro řešení jakékoli mimořádné situace, pro medializaci práce městské policie nebo pro výcvikové a výukové účely v rámci interního vzdělávání a školení zaměstnanců.

Předmětem popisované kontroly bylo nicméně nikoli samotné pořizování videozáznamů, ale jejich následné zveřejňování na internetu, ke kterému dle kontrolních zjištění dochází za účelem prevence kriminality a informování veřejnosti o možnostech ochrany před trestnou činností, kterou MP HMP poskytuje, resp. informování o činnosti MP HMP obecně.

Před zveřejněním vybraných záznamů dochází k jejich sestřihu, rozostření obličejů a registračních značek vozidel a remodulaci hlasu zaznamenaných osob. Dochází tedy k anonymizaci těchto záznamů a zveřejněny mají být již jen takové záznamy, z nichž nejsou konkrétní osoby (subjekty údajů) identifikovatelné. V takovém případě, tedy pokud MP HMP důsledně před zveřejněním videozáznamy anonymizuje, nejedná se nadále o zpracovávání osobních údajů, a tudíž jejich další zveřejnění nepodléhá režimu zákona č. 101/2000 Sb.

Ve vztahu ke konkrétnímu záznamu, který byl předmětem stížnosti, bylo nicméně zjištěno, že v tomto případě k důsledné anonymizaci záznamu nedošlo, v důsledku čehož byla stěžovatelka na zveřejněném záznamu rozpoznána okruhem známých a rodinou. V daném případě tak byly osobní údaje stěžovatelky zpracovávány nejen při pořízení a následné úpravě předmětného záznamu pověřenými pracovníky MP HMP, ale také zveřejněním na internetu, čímž došlo k zásahu do práva na ochranu soukromého a osobního života stěžovatelky, a tedy k porušení povinnosti MP HMP stanovené v § 5 odst. 3 zákona č. 101/2000 Sb.

V této souvislosti je třeba zdůraznit, že respektování práva na soukromí a na ochranu osobních údajů při pořizování záznamů zákroků a úkonů strážníků MP HMP je zásadní s ohledem

na to, že se z povahy věci vždy jedná o záznam jednání, který je způsobilý (v důsledku zveřejnění) způsobit dotčené osobě vážnou újmu na zmíněných právech. Tím spíše, je-li záznam anonymizován pouze částečně, případně zveřejněn i včetně neodborných až dehonestujících komentářů zasahujících strážníků, jako se stalo v tomto konkrétním případě.

Zvolí-li správce osobních údajů způsob či prostředky zpracování osobních údajů, se kterými je spojeno velké potenciální riziko zásahu do práv subjektů údajů – což je nepochybně případ zveřejňování informací na internetu – musí si být vědom toho, že v případě pochybení bude jeho odpovědnost posuzována právě s ohledem na toto jeho rozhodnutí. Svým rozhodnutím použít určité prostředky správce osobních údajů totiž zvýšil riziko zásahu do práv subjektu údajů, případně zvýšil i intenzitu tohoto zásahu, za což nese odpovědnost.

V rámci této kontroly bylo dále hodnoceno, zda a do jaké míry MP HMP plní své povinnosti v oblasti zabezpečení zpracovávaných osobních údajů, jak je uloženo v § 13 zákona č. 101/2000 Sb. Bylo zjištěno, že MP HMP přijala interní normy upravující postup strážníků při nakládání se záznamy pořízenými z průběhu úkonů strážníků. Tyto záznamy jsou pravidelně přehrávány na centrální úložiště, kde jsou uchovávány, a následně (po uplynutí stanovené lhůty) jsou nevratným způsobem odstraněny. Výjimkou jsou záznamy, které jsou vyhodnoceny jako potřebné k dokumentaci trestného činu, přestupku nebo jiného správního deliktu. Současně bylo zjištěno, že MP HMP pořizuje elektronické záznamy vypovídající o tom, kdo a jakým způsobem s jednotlivými záznamy nakládal, resp. k nim přistupoval.

Záznamy, které jsou posouzeny jako vhodné pro účely mediální prezentace a jsou určeny ke zveřejnění, jsou upraveny výše popsaným způsobem (sestřih, anonymizace) a následně zveřejněny na internetu. MP HMP tedy v souvislosti se zpracováním osobních údajů formou videozáznamů úkonů strážníků přijala technicko-organizační opatření k zajištění ochrany osobních údajů v prostředí MP HMP, a to včetně postupu, který je zapotřebí dodržet před zveřejněním záznamu pořízeného strážníky z průběhu konkrétního úkonu. Tím MP HMP, v obecné rovině, plní své povinnosti podle § 13 odst. 3 a 4 zákona č. 101/2000 Sb.

V případě záznamu stěžovatelky však MP HMP přijaté postupy dostatečně neaplikovala, neboť identita stěžovatelky byla ze zveřejněného záznamu rozpoznatelná a její osobní údaje tak byly v rozporu s požadavky § 13 odst. 1 zákona č. 101/2000 Sb. vystaveny riziku neoprávněného nebo nahodilého přístupu ze strany všech, kdo předmětný záznam zhlédli.

K otázce zveřejňování osobních údajů na internetu je nutno v této souvislosti dále uvést, že po zveřejnění videozáznamů MP HMP ztrácí nad těmito záznamy kontrolu, resp. nemůže již ovlivnit, kdo se s těmito záznamy seznámí a jakým způsobem je dále využije, případně i zneužije. Jsou-li součástí těchto záznamů také informace, které lze vyhodnotit jako osobní údaje dle § 4 písm. a) zákona č. 101/2000 Sb., pak nelze než dojít k závěru, že tyto údaje byly v rozporu s požadavkem § 13 odst. 1 citovaného zákona vystaveny riziku zneužití.

Jak bylo uvedeno již výše, toto riziko je tím větší, že se jedná o zveřejnění na internetu, u něhož je dosah a dopad zveřejněných informací značný. V návaznosti na uvedená kontrolní zjištění vedl Úřad správní řízení, které nebylo v roce 2016 pravomocně ukončeno.

Kontrola Administrativního registru ekonomických subjektů (ARES) vedeného Ministerstvem financí ČR (inspektor Petr Krejčí)

Inspektor provedl kontrolu na základě podnětu odboru pro styk s veřejností Úřadu, kdy bylo v rámci vyřizování podnětů a stížností v několika případech zjištěno, že v Administrativním registru ekonomických subjektů (ARES) vedeném Ministerstvem financí (dále také „Kontrolovaná osoba") jsou zveřejňovány osobní údaje fyzických osob podnikajících dle zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), které již po dobu čtyř a více let neprovozují podnikání dle živnostenského zákona, a to i přesto, že v souladu s ustanovením § 60 odst. 3 písm. b) zákona č. 455/1991 Sb. ve veřejné části živnostenského rejstříku jejich osobní údaje vedeny nejsou, a tedy nejsou zveřejňovány, a jsou převedeny do neveřejné části živnostenského rejstříku, v tomto smyslu byl stanoven i předmět kontroly.

ARES umožňuje vyhledávání ekonomických subjektů registrovaných v ČR k zajištění efektivního výkonu veřejné správy s cílem zajistit komunikaci ekonomických subjektů navzájem a s veřejnou správou, včetně snížení provozních nákladů na vlastní výkon státní správy a zprostředkovává zobrazení údajů vedených v jednotlivých registrech, ze kterých čerpá data (tzv. zdrojové registry) v souvislosti se zpřístupněním informací z veřejných rejstříků, které vedou jednotlivé orgány státní správy s napojením na ARES.

Účelem ARES provozovaného Kontrolovanou osobou je poskytnout rychlé a obecně dostupné informace o jednotlivých ekonomických subjektech souhrnným zpřístupněním údajů z informačních systémů registrů a evidencí veřejné správy. ARES přehledně zpřístupňuje údaje, přebírané ze zdrojových registrů do databáze ARES a současně umožňuje přímo odkazem přejít do www aplikací (webové stránky) orgánů veřejné správy, které příslušné informační systémy provozují. Opravu údajů v ARES Kontrolovaná osoba neprovádí. V případě žádosti veřejnosti o změnu údajů v ARES zjistí Kontrolovaná osoba zdrojový registr, kde se chyba nachází, a informace o správci registru sdělí tazateli, ke kterému správci má svůj dotaz adresovat, resp. u kterého uplatní požadavek na změnu. V případě provedené opravy u správce zdrojového rejstříku se tato změna automaticky promítne do systému ARES.

S ohledem na charakter provozu ARES a jeho zabezpečení si Kontrolovaná osoba vyhradila právo omezit nebo znemožnit přístup k www aplikaci ARES uživatelům, kteří denně odešlou k vyřízení více než 1.000 dotazů v době od 8:00 hod. do 18:00 hod. nebo více než 5.000 dotazů v době od 18:00 hod. do 8:00 hod. rána následujícího dne, nebo se snaží o porušení bezpečnostní ochrany www serveru Kontrolované osoby. Obnovení přístupu k údajům aplikace ARES po jeho případném zákazu bude řešeno zásadně na základě dostatečných písemných záruk, které uživatel dohodne s Kontrolovanou osobou.

Vzhledem k charakteru aplikace ARES Kontrolovaná osoba prohlásila, že nenese odpovědnost za aktuálnost a úplnost údajů z databáze ARES ani za nepřetržitý provoz www aplikací pro zpřístupnění údajů z informačních systémů zdrojových registrů ani za korektnost a aktuálnost jimi zpřístupňovaných informací. Kontrolovaná osoba není schopna garantovat správnost dat, která nevznikají z činnosti Kontrolované osoby a vznikají z činností jiných orgánů státní správy. Kontrolovaná osoba nemůže pozměňovat data uložená těmito orgány státní správy. Kontrolním zdrojem je Územně identifikační registr adres (UIR-ADR), vedený Ministerstvem práce a sociálních věcí ČR.

ARES jako informační systém veřejné správy je pod identifikátorem č. 48 registrován v Informačním systému o informačních systémech veřejné správy, zřízeném v souladu s ustanovením

zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve spojení s § 3 odst. 6 písm. a) prováděcí vyhlášky č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy (vyhláška o informačním systému o informačních systémech veřejné správy).

Po zaslání Oznámení o zahájení kontroly provedla Kontrolovaná osoba z vlastní iniciativy změnu, resp. úpravu v systému ARES, aby napříště nedocházelo ke zveřejňování údajů, které jsou v současné době převedené do neveřejné části živnostenského rejstříku ve smyslu ustanovení § 60 odst. 3 písm. b) živnostenského zákona. Toto iniciativní opatření Kontrolovaná osoba předložila na ústním jednání, jednalo se o otisky obrazovky ze systému ARES – veřejně přístupných stránek, s doložením přijatých opatření o nezveřejňování údajů subjektů údajů pod záložkou „zaniklé", kdy při zadání identifikační číslo fyzické osoby systém zobrazí informaci, že „požadavek nelze realizovat".

Bylo-li podnikateli živnostenským úřadem přiděleno IČ osoby poskytnuté správcem základního registru osob, nemůže být přeneseno na jinou osobu a je jím tato osoba identifikovatelná i v případě, že by obnovila svoji dříve ukončenou podnikatelskou činnost na základě nově vydaného živnostenského oprávnění. Po zařazení údajů do veřejné části živnostenského rejstříku dochází ke zveřejnění i úplného rozsahu zveřejňovaných údajů v ARES v odkazu „RŽP".

Kontrolovaná osoba neodpovídá za to, pokud by se v ARES nacházely osobní údaje osob podnikajících podle živnostenského zákona, kterým před čtyřmi a více lety zaniklo poslední živnostenské oprávnění, a jejichž údaje by tedy podle ustanovení § 60 odst. 3 písm. b) živnostenského zákona měly být převedeny z veřejné části živnostenského rejstříku do části neveřejné a být tak dostupné jen ve specifických případech uvedených v ustanovení § 60 odst. 4 písm. b) živnostenského zákona, tj. osobě, která prokáže právní zájem. Za správnost zveřejňovaných údajů uvedených v ARES s odkazem na „RES" odpovídá jeho správce Český statistický úřad. Veřejné údaje, které se podle ustanovení § 20 odst. 1 zákona č. 89/1995 Sb., o státní statistické službě, zapisují do registru ekonomických subjektů, mají pouze evidenční význam. Podle ustanovení § 20 odst. 2 zákona č. 89/1995 Sb. ve spojení zejména s ustanovením § 20 odst. 8, 4 a 5 jsou veřejnými údaji u fyzických osob: jméno, příjmení, identifikační číslo, místo podnikání (sídlo), datum vydání povolení nebo dokladu o registraci nebo zápisu opravňujícího ji k podnikání, datum a příčina zániku oprávnění podnikat. Kontrolovanou osobou ani žádnou jinou osobou, včetně kontrolních orgánů, nebyl zjištěn žádný rozpor týkající se činnosti Kontrolované osoby s předpisy či vnitřními dokumenty týkajícími se ochrany osobních údajů.

Na podporu svých tvrzení odkázala Kontrolovaná osoba dále na její postup podle vnitřních předpisů, které jsou v souvislosti s plněním informační povinnosti veřejně přístupné na jejích webových stránkách.

Ustanovení § 3 odst. 1 zákona č. 101/2000 Sb. charakterizuje okruh adresátů právní normy z hlediska tzv. osobní působnosti. Podle tohoto ustanovení zákona se tento zákon vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby. Kontrolovanou osobu lze považovat za státní orgán podle ustanovení § 3 odst. 1 zákona č. 101/2000 Sb.

Podle ustanovení § 4 písm. a) zákona č. 101/2000 Sb. je osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě

čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. To vše ARES splňuje.

Podle ustanovení § 4 písm. e) zákona č. 101/2000 Sb. se zpracováním osobních údajů rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zejména shromažďování, používání, uchovávání a zpřístupňování osobních údajů v registru ARES Kontrolovanou osobou lze považovat ve smyslu ustanovení § 4 písm. e) zákona č. 101/2000 Sb. za zpracování osobních údajů.

Podle ustanovení § 4 písm. j) zákona č. 101/2000 Sb. je správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.

Účel a prostředky zpracování osobních údajů určuje v daném případě pro veřejnou a neveřejnou část registru ARES zejména podle zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a evidenci svěřenských fondů, Kontrolovaná osoba.

Podle ustanovení § 5 odst. 1 písm. a) zákona č. 101/2000 Sb. je správce povinen stanovit účel, k němuž mají být osobní údaje zpracovány. Účelem informačního systému ARES provozovaného Kontrolovanou osobou je poskytnout rychlé a obecně dostupné informace o jednotlivých ekonomických subjektech souhrnným zpřístupněním údajů z informačních systémů registrů a evidencí veřejné správy. ARES přehledně zpřístupňuje údaje, přebírané ze zdrojových registrů do databáze ARES a současně umožňuje přímo odkazem přejít do www aplikací (webové stránky) orgánů veřejné správy, které příslušné informační systémy provozují. Všechny informace zpřístupněné systémem ARES mají pouze informativní charakter, nemají charakter úřední listiny a dle vyjádření Kontrolované osoby nemohou být jako průkazné využity jinými osobami, resp. použity, např. jako dostatečný důkaz či podklad zejména pro soudní řízení nebo jiné úřední jednání, ani nemůže být požadována náhrada škody, která by vznikla jejich využitím. Vzhledem k tomu, že Kontrolovaná osoba stanovila účel zpracování osobních údajů, splnila svoji povinnost uvedenou v ustanovení § 5 odst. 1 písm. a) zákona č. 101/2000 Sb. V souladu s ustanovením § 5 odst. 2 zákona č. 101/2000 Sb. může správce zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat pouze ve výjimečných případech uvedených pod písm. a) až g) tohoto ustanovení zákona. Podle ustanovení § 5 odst. 2 písm. d) zákona č. 101/2000 Sb. může správce osobní údaje zpracovávat bez souhlasu subjektu údajů, jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů. Kontrolovaná osoba neporušila ustanovení § 5 odst. 2 zákona č. 101/2000 Sb., pokud zpracovává osobní údaje k danému účelu v rozsahu plnění svých povinností v souvislosti s provozováním ARES.

Podle ustanovení § 11 odst. 3 písm. c) zákona č. 101/2000 Sb. není správce osobních údajů informace a poučení podle odstavce 1 povinen poskytovat v případech, kdy osobní údaje nezískal od subjektu údajů, pokud zpracovává výlučně oprávněně zveřejněné osobní údaje. Kontrolovaná osoba neporušila ustanovení § 11 zákona č. 101/2000 Sb.

V souladu s ustanovením § 13 zákona č. 101/2000 Sb. jsou správce a zpracovatel povinni přijmout taková opatření, 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. Tato povinnost platí i po ukončení zpracování osobních údajů. Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy. V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel povinen také pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. Přijatá opatření na ochranu dat v neveřejné části ARES proti neoprávněnému nebo nahodilému přístupu k osobním údajům a jejich řádnému zabezpečení proti jejich zneužití třetími osobami bez souhlasu subjektů údajů ve smyslu ustanovení § 13 zákona č. 101/2000 Sb. jsou dokumentována ve vnitřních předpisech.

Kontrolovaná osoba zpracovává osobní údaje subjektů údajů ve veřejné a neveřejné části ARES. Do neveřejné části ARES mohou vstupovat pouze podle zvláštních zákonů oprávněné orgány státní správy, např. Finanční správa, orgány Policie ČR, Celní správy apod., na základě přístupových oprávnění. Informační systém ARES umožňoval do 7. června 2016 vyhledávání ekonomických subjektů pod záložkou „aktivní" nebo „zaniklé". Pod záložkou „zaniklé" bylo možné dohledat u označených ekonomických subjektů, u nichž uplynuly čtyři roky ode dne zániku posledního živnostenského oprávnění podnikatele, a jejichž osobní údaje byly i v živnostenském rejstříku v ARES (RŽP) převedeny z veřejné části do části neveřejné, pouze odkazem na registr ekonomických subjektů (RES) v rozsahu: IČ, jméno, příjmení, adresa, datum vzniku a datum zániku živnostenského oprávnění, způsob zániku (nezjištěno, ukončení na základě oznámení), sídlo, resp. místo podnikání, počet zaměstnanců.

Aby napříště nedocházelo ke zveřejňování údajů, které jsou v současné době převedeny do neveřejné části živnostenského rejstříku ve smyslu ustanovení § 60 odst. 3 písm. b) živnostenského zákona, i odkazem na záložku RES v ARES, jenž se týká registru ekonomických subjektů, jehož správcem je Český statistický úřad s odpovědností za zpracovávané osobní údaje, byla nad rámec doporučení kontrolujících z ARES odstraněna jakákoliv možnost vyhledávání ekonomických subjektů pod záložkou „zaniklé". V současné době jsou proto v ARES veřejnosti zpřístupněna data pouze u aktivních ekonomických subjektů, resp. osob vedených ve veřejné části živnostenského rejstříku, a tím tak bylo zcela znemožněno veřejnosti v ARES zjistit např. účastníky správního, soudního či trestního řízení, zda daná osoba byla v minulosti (minimálně před čtyřmi lety ode dne zániku živnostenského oprávnění) osobou podnikající podle zvláštního zákona.

Přístup do neveřejné části ARES mají pouze oprávněné orgány státní správy, např. Finanční správa, orgány Policie ČR, Celní správy apod., na základě přístupových oprávnění, ze kterých je možné i zpětně (5 let) dohledat, kdo a kdy na základě svého pracovního zařazení do systému vstoupil za účelem zjištění požadované informace, resp. jsou v tomto případě pořizovány logy. Za účelem kontroly systému mají do neveřejné části tohoto systému přístup i zaměstnanci příslušného útvaru Kontrolované osoby. Všechny vstupy jsou logovány a zpětně dohledatelné. Kontrolovaná osoba doložila výpis vzorku logů přístupů odpovědných subjektů do neveřejné části systému ARES. Kontrolovaná osoba neporušila ustanovení § 13 zákona č. 101/2000 Sb.

Podle ustanovení § 18 odst. 1 písm. a) zákona č. 101/2000 Sb. se oznamovací povinnost podle § 16 nevztahuje na zpracování osobních údajů, které jsou součástí datových souborů veřejně přístupných na základě zvláštního zákona. V daném případě Kontrolovaná osoba zpracovává osobní údaje subjektů údajů získaných ze zdrojových registrů, včetně rejstříku živnostenského oprávnění (RŽP) a registru ekonomických subjektů (RES), přičemž zpřístupňuje

v ARES pouze údaje aktivních ekonomických subjektů z veřejných částí zdrojových registrů. Kontrolovaná osoba neporušila ustanovení § 16 zákona č. 101/2000 Sb.

Požádá-li subjekt údajů podle ustanovení § 12 zákona č. 101/2000 Sb. o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat. Za poskytnutí informace ve smyslu ustanovení § 12 odst. 3 zákona č. 101/2000 Sb. má správce právo požadovat přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace.

Podle ustanovení § 21 odst. 1 zákona č. 101/2000 Sb. každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může požádat správce nebo zpracovatele o vysvětlení nebo požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů. Kontrolovaná osoba eviduje množství žádostí, ve smyslu ustanovení § 12 a § 21 zákona č. 101/2000 Sb., což doložila přehledovou tabulkou realizovaných dotazů a podnětů, včetně způsobu jejich vyřízení (odpovědí) rozdělených do skupin podle druhu dotazu, přičemž z obsahu odpovědí Kontrolované osoby vyplývá informace, že za vedení živnostenského rejstříku (RŽP) a správnost z něho zveřejněných údajů v ARES odpovídá Ministerstvo průmyslu a obchodu ČR a za vedení registru ekonomických subjektů (RES) a správnost z něho zveřejněných údajů v ARES odpovídá Český statistický úřad. Opravu údajů v ARES Kontrolovaná osoba neprovádí. V případě žádosti veřejnosti o změnu údajů v ARES zjistí Kontrolovaná osoba zdrojový registr, kde se chyba nachází, a informace o správci registru sdělí tazateli, ke kterému správci má svůj dotaz adresovat, resp. u kterého uplatní požadavek na změnu. V případě provedené opravy u správce zdrojového rejstříku se tato změna automaticky promítne do systému. V daném případě, za dané právní úpravy nebylo zjištěno, že by Kontrolovaná osoba porušovala práva subjektů údajů podle ustanovení § 12 a § 21 zákona č. 101/2000 Sb.

Závěr

Aby nedocházelo k chybným záznamům v ARES tak jako např. u stěžovatelky, kdy byla v minulosti v ARES a odkazem v RES jmenovaná uvedená pod různými jmény (původním neaktualizovaným), bylo kontrolujícími doporučeno na ústním jednání a místním šetření dne 9. června 2016 vhodným způsobem analyzovat případný přínos úpravy postavení a fungování ARES a provést legislativní úpravu přímo příslušným zvláštním právním předpisem, včetně na to navazujících vnitřních regulačních nástrojů jeho správce, tak, aby ARES neobsahoval rovněž údaje, které neodpovídají skutečnosti a za něž nenese Kontrolovaná osoba jako jeho správce jakoukoliv odpovědnost tak, jak je tomu u ostatních správců, kteří odpovídají za zpracování přesných osobních údajů ve svých zveřejňovaných rejstřících podle zvláštních zákonů. Legislativní úpravou o ARES by tak mohla být odstraněna případná kompetenční nedorozumění a vymezena zákonná odpovědnost za aktuálnost, úplnost a správnost údajů převzatých do veřejné i neveřejné části ARES, což by současně mělo i vliv na posílení důvěry veřejnosti v ARES, resp. Kontrolovanou osobu. I když chybí speciální právní úprava ARES, není důvodné pochybovat o legálnosti oprávněně sdružovaných údajů v ARES z ostatních rejstříků, registrů, evidencí a seznamů k účelu užití dat z něho, s využitím úpravy obecné, a to zákona č. 304/2013 Sb.

Úřad pro ochranu osobních údajů doporučil, aby byly přijaty speciální právní úpravy pro zpracovávání osobních údajů v ARES tak, aby byly použity obdobné postupy při zpracovávání osobních údajů subjektů údajů jako v jiných rejstřících (např. živnostenský rejstřík).

Nelze považovat pro veřejnost za udržitelné tak, jak vyplývá i z velkého množství probíhající korespondence s veřejností, aby správce veřejné a neveřejné části v ARES nenesl žádnou odpovědnost za aktuálnost a úplnost údajů z databáze ARES ani za nepřetržitý provoz www aplikací pro zpřístupnění údajů z informačních systémů zdrojových registrů využívaných k danému účelu veřejností, tj. ke komunikaci s veřejnou správou a mezi ekonomickými subjekty navzájem, ani za korektnost a aktuálnost jimi zpřístupňovaných informací tak, jak je to v současnosti a vyplývá to z veřejně přístupných informací prezentovaných Kontrolovanou osobou.

Absencí speciální právní úpravy pro registr ARES tak dochází i ke zřejmým a zbytečným nedorozuměním, rovněž i ke dni 18. srpna 2016 na webových stránkách Kontrolované osoby http://www.info.mfcr.cz/ares/ares.html zveřejněného nedůvodného upozornění pro uživatele: „Na základě podnětu ÚOOÚ jsme byli nuceni dočasně pozastavit vyhledávání zaniklých ekonomických subjektů. Za případné způsobené potíže se omlouváme. V případě nutnosti využijte vyhledávání ve zdrojových rejstřících: veřejný rejstřík…, registr živnostenského podnikání..., registr ekonomických subjektů…".

Kontrola členů přípravného výboru pro registraci náboženské společnosti Pauperes commitiones Christi templique Salomonici – SKT (inspektor Petr Krejčí)

Předmětem kontroly bylo dodržování povinností správce a zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb., při zpracování osobních údajů subjektů údajů, včetně shromažďování dat občanů na podpisových arších pro účely registrace výše uvedené náboženské společnosti u Ministerstva kultury (dále také „MK"). Podnět ke kontrole podalo na Úřad samo MK , a to z důvodu nesrovnalostí, které byly zjištěny při přezkumu petičních archů, které na MK dodal přípravný výbor náboženské společnosti. Jednalo se zejména o:

- Vyplněné a Ministerstvu kultury zpět doručené dotazníky osob, které nepodepsaly podpisový arch k registraci náboženské společnosti Pauperes commitiones Christi templique Salomonici – SKT.
- Vyplněné a Ministerstvu kultury zpět zaslané dotazníky osob, které sice podepsaly podpisový arch, ale k jinému účelu, než byly jejich osobní údaje užity, a necítí se být osobou hlásící se k náboženské společnosti Pauperes commitiones Christi temlique Salomonici – SKT.

Inspektor Úřadu provedl kontrolu a v provedeném šetření v podstatě potvrdil skutečnosti avizované MK. Po posouzení všech skutečností považoval za zřejmé, že existují důvodné pochybnosti, že nejméně v 48 případech došlo k neoprávněnému užití osobních údajů a zfalšování podpisů, a to za účelem získání registrace náboženské společnosti SKT. Kontrolované osoby v doplnění protokolu z ústního jednání uvedly, že podpisové archy respondenti podepisovali až po vysvětlení účelu, historie, poslání a poučení, přičemž současně vyjádřily domněnku, že při získávání (prezentaci) budoucí náboženské společnosti si ne všichni respondenti mohli být vědomi toho, že se historicky jedná o skotský templářský řád (z názvu společnosti to vyplývá pouze pro „latiníky"), a když si tuto skutečnost následně uvědomili, začali zpochybňovat svoje podpisy na podpisových arších. I když Kontrolované osoby na ústním jednání uvedly, že jim není nic

známo o tom, že by byly údaje uvedené na podpisových arších použity z nějaké určité databáze vytvořené k jinému účelu, je zřejmé, že u podpisových archů č. 1 a č. 50 byly osobní údaje u 75 respondentů v rozsahu pořadové číslo, jméno, příjmení, adresa trvalého pobytu a datum narození vyplněny strojově, což nemohlo být učiněno samotnými náhodně na veřejném místě se nacházejícími respondenty.

Podle ustanovení § 5 písm. g) zákona č. 101/2000 Sb. je správce povinen shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti. Toto ustanovení zákona předpokládá jednat při shromažďování osobních údajů subjektů údajů čestně a otevřeně, tedy nesnažit se „vymámit" osobní údaje ze subjektu údajů pro účely zcela odlišné od účelu stanoveného členy přípravného výboru SKT.

Účelem shromažďování osobních údajů kontrolovanými osobami bylo získání zákonem stanoveného množství osobních údajů a podpisů osob hlásících se k náboženské společnosti SKT, tj. osob, které k této náboženské společnosti přináleží podle svého přesvědčení i podle jejích vnitřních předpisů, potřebných k podání návrhu na registraci náboženské společnosti SKT u MK.

Kontrolované osoby tedy jako správci osobních údajů nejméně u 23 osob shromažďovaly osobní údaje pod záminkou jiného účelu, než byl uveden ve vnitřních předpisech, tj. základním dokumentu, jak byl také prezentován i na MK pro účely návrhu na registraci náboženské společnosti, jehož součástí měly být i podpisové archy s osobními údaji členů náboženské společnosti SKT, kteří tak podpisem měli stvrdit, že se stali součástí řádu templářů – náboženské společnosti a že jako řadoví členové budou mít povinnosti členů náboženské společnosti stanovenými českými zákony. Je tedy zřejmé, že osobní údaje těchto osob byly shromážděny pod záminkou jiného účelu, čímž Kontrolované osoby porušily ustanovení § 5 odst. 1 písm. g) zákona č. 101/2000 Sb., které přímo vylučuje shromažďovat údaje pod záminkou jiného účelu.

Zákon č. 101/2000 Sb. v ustanovení § 4 písm. n) stanoví, že pro účely tohoto zákona se rozumí souhlasem subjektu údajů svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.

Tak jak uvedly Kontrolované osoby ve svém doplněném vyjádření, ani samy neuměly kontrolujícím odpovědět na dotaz, jakým způsobem byli do „seznamu" zařazeni občané, kteří souhlas se zpracováním jejich osobních údajů pro účely registrace náboženské společnosti nedali, a kdo tedy za ně podpisový arch vyplnil nebo mohl vyplnit s tím, že namítaly, že kontrolující nemají dostatek relevantních podkladů, že by uvedené občany na podpisových arších prokazatelně podepsala jiná (odlišná) osoba, přičemž se mělo jednat o respondenty (subjekty údajů), kteří dle tvrzení Kontrolovaných osob měli být osloveni zejména na veřejně přístupných místech.

Přitom bylo v souvislosti s touto skutečností prokazatelně zjištěno, že např. podpisové archy č. 1 a č. 50 byly již předem strojově vyplněné údaji v rozsahu: jména, příjmení, adresy trvalého pobytu i data narození, což svědčí o tom, že nemohly být vyplňovány na veřejných místech přímo samotnými respondenty, a že tyto údaje musely být předem zjištěny a opatřeny z jiné databáze či jiného zdroje údajů. U strojově předem vyplněných údajů osob, které nejsou členy, resp. sympatizanty náboženské společnosti SKT, nebylo prokázáno, že by tyto osoby daly souhlas se zpracováním jejich osobních údajů pro daný účel, ale naopak bylo prokázáno vyjádřením těchto osob, že takový souhlas ke zpracování osobních údajů vůbec nedaly, a to z důvodu, že osobní údaje neposkytly a na podpisový arch se nepodepsaly nebo že sice podpisový arch podepsaly, ale k jinému účelu. Přitom nelze opomenout, že řada osob uvedených na

podpisových arších č. 1 a 50 nemohla být vůbec MK ztotožněna pro uvedení chybných osobních údajů nebo se jednalo i o zemřelou osobu.

Jestliže tedy 48 občanů ve své odpovědi MK uvedlo, že podpisový arch nepodepsalo, svědčí tato skutečnost o tom, jak se někteří z nich vyjádřili, že jejich osobní údaje byly zneužity za účelem registrovat náboženskou společnost SKT.

Citace např.: „*Nikdy jsem se k žádné církvi nehlásila a nic nepodepsala. Doufáme, že to neprojde jen tak.*" „*Žádný arch jsem nepodepsal, je to na trestní oznámení, je to zneužití mých osobních údajů. Nehlásím se k žádné církvi.*" „*Nikdy jsem o existenci této církve neslyšela. Nechápu, kdo mohl mého jména zneužít.*" „*Nemám s touto organizací nic společného, jsem římskokatolického vyznání.*" „*Od uvedené náboženské skupiny se distancuji. Výše uvedenou náboženskou skupinu neznám. Nikdy jsem vědomě podpisový arch nepodepsala a nejsem si vědoma, za jaké situace by mohl být získán můj podpis.*" „*Neznám tuto společnost, nikdy jsem nic nepodepsal. Děkuji za Vaši práci tento podvod odhalit.*" „*Dotčený arch jsem neviděl.*" „*Vůči mé osobě byly zneužity osobní údaje.*" „*Nikde jsem se nevedla. Nemám s tím nic společného! Jedná se o omyl!*" „*Tuto církev neznám. Žádný podpis jsem nedával. Pravděpodobně došlo ke zfalšování podpisu.*" „*Někdo si moje data evidentně koupil, opravdu žádnou církev nepodporuji!*" „*O této církvi či sektě slyším poprvé.*" jasně vypovídají o postojích dotčených osob, které nedaly souhlas se zpracováním svých osobních údajů k danému účelu, tj. k členství, resp. registraci náboženské společnosti SKT, o této společnosti řada z nich nikdy neslyšela, natož aby byla přinejmenším osobou hlásící se k náboženské společnosti SKT, tj. osobou, která k této náboženské společnosti přináleží podle svého přesvědčení i podle vnitřních předpisů této náboženské společnosti, jak striktně vyžaduje zákon č. 3/2002 Sb., o svobodě náboženského vyznání a postavení církví a náboženských společností a o změně některých zákonů (zákon o církvích a náboženských společnostech), pro splnění podmínek registrace náboženské společnosti u MK.

Navíc existují pochybnosti o tom, zda i další osoby uvedené na podpisových arších se skutečně hlásily k náboženské společnosti SKT. Z počtu 306 osob pak MK nezaslalo žádnou odpověď celkem 189 osob a 28 dotazníků bylo poštou vráceno jako nedoručitelné. Šetřením bylo rovněž zjištěno, že na podpisových arších č. 44–49 byly u 21 předložených podpisů uvedeny buď chybné adresy trvalého pobytu, nebo se jedná o již zemřelé osoby, případně se tyto osoby nepodařilo ztotožnit s údaji v registru obyvatel. I tyto skutečnosti tedy svědčí o tom, že přinejmenším u uvedených zemřelých osob nebyly a ani nemohly být osobní údaje na podpisové archy získávány přímo od těchto osob.

Jako nepravděpodobné se jeví tvrzení Kontrolovaných osob, že byl každý z respondentů, pokud docházelo ke shromažďování osobních údajů na veřejně přístupných místech, informován nejen o účelu, ale i o historii, poslání a poučení a svým podpisem tak měl stvrdit členství v náboženské společnosti SKT. Jelikož Kontrolované osoby zpracovávaly osobní údaje 48 domnělých členů náboženské společnosti SKT bez jejich souhlasu, přičemž na toto zpracování nelze uplatnit ani některý z právních titulů uvedených v ustanovení § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb., porušily ustanovení § 5 odst. 2 zákona č. 101/2000 Sb.

Pokud fyzické osoby uvedené na podpisových arších nebyly přítomné při shromažďování jejich osobních údajů, resp. podpisový arch nepodepsaly, a přesto byly shromažďovány bez jejich vědomí jejich osobní údaje, včetně rodných čísel, je zřejmé, že Kontrolované osoby nedisponují souhlasem těchto osob jako nositelů rodného čísla s jejich nakládáním. Jelikož bylo z vyjádření

respondentů zjištěno, že Kontrolované osoby prokazatelně zpracovávaly rodná čísla 16 osob z podpisových archů bez jejich souhlasu, porušily Kontrolované osoby ustanovení § 13c odst.1 písm. c) zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). Kontrolované osoby v případě zpracovávání rodných čísel, aniž by disponovaly prokazatelným a informovaným souhlasem subjektů údajů či splnily podmínku zpracování rodného čísla bez souhlasu subjektu údajů na základě zákonem stanovených výjimek, porušily tak i ustanovení § 5 odst. 2 zákona č. 101/2000 Sb. Citlivé údaje je možné podle ustanovení § 9 písm. a) zákona č. 101/2000 Sb. zpracovávat, jen jestliže subjekt údajů dal ke zpracování výslovný souhlas. Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Správce je povinen předem subjekt údajů poučit o jeho právech podle ustanovení § 12 a ustanovení § 21.

V průběhu kontroly bylo prokazatelně zjištěno, že uvedený souhlas se zpracováváním osobních údajů k účelu podání návrhu na registraci náboženské společnosti SKT nedalo nejméně 48 osob, které uvedly, že podpisový arch vůbec nepodepsaly, a nejméně 23 osob, které uvedly, že sice podpisový arch podepsaly, ale nejsou osobami hlásícími se k náboženské společnosti SKT, resp. jejími členy.

Vzhledem k tomu, že Kontrolované osoby neprokázaly souhlas se zpracováním osobních citlivých údajů u všech subjektů údajů (respondentů), jejichž osobní údaje, včetně citlivých údajů, obsahovaly podpisové archy, porušily Kontrolované osoby ustanovení § 9 zákona č. 101/2000 Sb.

Dle ustanovení § 11 odst. 1 zákona č. 101/2000 Sb. je správce povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v ustanovení § 21 zákona č. 101/2000 Sb. Informace a poučení by nebyl správce v daném případě povinen poskytnout, pokud by zpracovával osobní údaje, které sice nezískal od subjektů údajů k účelu podání návrhu na registraci náboženské společnosti SKT tak, jak se stalo v případě nejméně 48 osob, u kterých bylo zjištěno, že se shromažďování jejich osobních údajů neúčastnilo a podpisové archy nepodepsalo, ale musel by mít od těchto osob jejich prokazatelný souhlas ke zpracovávání jejich osobních údajů k účelu návrhu na registraci náboženské společnosti SKT, resp. souhlas se členstvím v této náboženské společnosti.

Uvedené informační povinnosti vůči subjektům údajů, i když měla být ze strany Kontrolovaných osob plněna prostřednictvím osob, které byly ke shromažďování osobních údajů, včetně podpisů na podpisové archy zmocněny, se nemůže správce osobních údajů zprostit. Pokud těchto 23 osob prokazatelně uvedlo, že podpisový arch podepsalo, ale současně uvedlo např. *„nebylo mi dostatečně vysvětleno, co přesně podepisuji"*, *„podepsal jsem arch jen o spolupráci"*, *„svůj podpis jsem připojila na podporu vzniku a registrace"*, *„ je možné, že jsem něco podepsala, ale nejsem si vědoma, že by to bylo něco k nějakému náboženství. Je možné, že jsem byla uvedena v omyl. Nejsem člověk hlásící se k tomuto náboženství"*, *„byla jsem požádána a byla jsem pro její vznik"*, *„arch jsem podepsala, podporuji registraci náboženské společnosti"*, *„k této církvi se jako člen nehlásím, ale jejich registraci podporuji"* . Tyto odpovědi prokazují, že osoby, které podpisový arch podepsaly, ale nebyly kontrolovanými ani jinými osobami dosta-

tečně informovány ve smyslu ustanovení § 11 zákona č. 101/2000 Sb., a nebyly tak informovány zejména o účelu zpracování osobních údajů, tj. že podpisem na podpisový arch se stávají členy náboženské společnosti SKT, resp. že by tak měly být osobou hlásící se k náboženské společnosti SKT, která podle svého přesvědčení a vnitřních předpisů náboženské společnosti SKT s ní přináleží tak, jak předpokládá jedna z podmínek registrace náboženské společnosti SKT, a tak, jak byly tyto osoby prezentovány Kontrolovanými osobami u MK.

Kdyby Kontrolované osoby řádně splnily jako správce osobních údajů subjektů údajů svoji informační povinnost, zejména o účelu zpracování osobních údajů subjektů údajů, nedošlo by k uvedeným rozporům, kdy prokazatelně u 23 osob uvedených na podpisových arších a shodně vedených i u MK bylo shledáno, že byly o skutečném účelu mylně informovány. Za této situace nemůže obstát tvrzení Kontrolovaných osob, že shromažďovaly osobní údaje, které samy subjekty údajů na podpisové archy vyplňovaly, a Kontrolované osoby neprokázaly a ani prokázat nemohly, že by subjekty údajů řádně informovaly, zejména o účelu zpracování jejich osobních údajů. Kontrolované osoby tedy nejméně v 71 případech subjekty údajů neinformovaly řádně o tom, jaký je účel zpracování osobních údajů, kdo a jakým způsobem bude jejich osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny ani o jejich právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v ustanovení § 21 zákona č. 101/2000 Sb. a nejméně v 48 případech tak nebyly subjekty údajů informovány ani o tom, v jakém rozsahu budou jejich osobní údaje zpracovávány. Kontrolované osoby tak porušily i ustanovení § 11 odst. 1 zákona č. 101/2000 Sb.

Ministerstvo kultury žádosti přípravného výboru nevyhovělo a náboženskou společnost SKT nezaregistrovalo.

Dvěma členům přípravného výboru byla za spáchání přestupků dle § 44 odst. 2 písm. b), c), e) a f) zákona č. 101/2000 Sb. Úřadem uložena pokuta ve výši 10.000 Kč každému.

Kontrola statutárního města Plzeň (inspektor Petr Krejčí)

Předmětem opakované kontroly bylo dodržování povinností správce-zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů získaných od žadatelů o městský byt, kteří vyplnili přihlášky do výběrového řízení, vyhlášeného nájemcem bytu v době před uzavřením smluvního vztahu anebo v průběhu trvání nájemních/podnájemních smluv k bytům ve vlastnictví kontrolovaného města, kde byly vyžadovány i citlivé osobní údaje, zejména týkající se (ne)odsouzení za trestný čin. Inspektor kontrolu provedl na základě podnětu zástupce veřejné ochránkyně práv doručeného Úřadu pro ochranu osobních údajů v září 2015.

Statutární město Plzeň (dále také „Kontrolovaná osoba“) ve smyslu ustanovení § 2 zákona č. 128/2000 Sb., o obcích (obecní zřízení), je veřejnoprávní korporací, která má vlastní majetek, vystupuje v právních vztazích svým jménem a nese odpovědnost z těchto vztahů vyplývající a dále pečuje o všestranný rozvoj svého území a o potřeby svých občanů; při plnění svých úkolů chrání též veřejný zájem. Jedním z účelů zpracování osobních údajů je i jednání o smluvním vztahu týkajícího se nájemců v jednotlivých domech ve správě Kontrolované osoby. K předmětu kontroly se váže zejména oznámení o zpracování osobních údajů ze dne 9. října 2009, doručené dne 12. října 2009 a doplněné 27. listopadu 2009, ve kterém Kontrolovaná osoba oznamovala zpracování citlivých údajů vypovídajících o odsouzení za trestný čin. Zdůvodnění obce bylo, že podle ustanovení § 38 zákona č. 128/2000 Sb. majetek obce musí být využíván účelně

a hospodárně v souladu s jejími zájmy a úkoly vyplývajícími ze zákonem vymezené působnosti. Obec je povinna pečovat o zachování a rozvoj svého majetku. Majetek obce musí být chráněn před zničením, poškozením, odcizením nebo zneužitím. Povinností obce je tedy chránit svůj majetek před neoprávněnými zásahy a včas uplatňovat právo na náhradu škody a právo na vydání bezdůvodného obohacení. Obec je povinna trvale sledovat, zda dlužníci včas a řádně plní své závazky, a zabezpečit, aby nedošlo k promlčení nebo zániku práva.

Přihláška k výběru nájemce musí být řádně vyplněna ve všech předepsaných bodech. Přihlášku doručí účastník v termínu uvedeném v záměru. Nedílnou součástí přihlášky je Souhlas se zpracováním a zveřejněním osobních (citlivých) údajů podle zákona č. 101/2000 Sb. Bez vyplnění přihlášky a podepsání tohoto souhlasu nelze se zájemcem o nájem bytu uzavřít nájemní smlouvu.

Právě tento nedobrovolný souhlas se zpracováním a zveřejněním citlivých údajů se stal předmětem nesouhlasu veřejného ochránce práv občanů, neboť zejména skutečnost, že zájemce o obecní byt, který se přihlásil do výběrového řízení o nájem a byl soudně trestán, neměl při takové soutěži rovné podmínky.

Jelikož Kontrolovaná osoba zpracovává údaje o fyzických osobách (žadatelích o byt): jméno, příjmení, titul, rodné číslo, adresa trvalého bydliště, doručovací adresa, telefon, rodinný stav, zdroj příjmu a jeho výše, údaj o počtu osob, které spolu s žadatelem budou byt užívat, informaci, zda osoba byla či nebyla odsouzena za úmyslný trestný čin a případně informaci o tom, jak spolupracuje či nespolupracuje se sociálním nebo probačním pracovníkem nebo sociálním kurátorem – je subjekt údajů na základě těchto údajů určitě identifikován, a proto lze považovat údaje zpracovávané Kontrolovanou osobou za osobní údaje ve smyslu ustanovení § 4 písm. a) zákona č. 101/2000 Sb.

Podle ustanovení § 4 písm. a) zákona č. 101/2000 Sb. se citlivým osobním údajem rozumí osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

Kontrolovaná osoba požadovala od žadatelů o byt čestné prohlášení, zda jejich výpis z rejstříku trestů obsahuje či neobsahuje údaj o odsouzení za úmyslný trestný čin, přičemž žadatel dokládal k čestnému prohlášení také výpis z rejstříku trestů, a to pouze k nahlédnutí a ověření skutečností uvedených v čestném prohlášení. V případě, že výpis z rejstříku trestů obsahuje údaj o odsouzení za úmyslný trestný čin, požaduje Kontrolovaná osoba písemné potvrzení od sociálního pracovníka, probačního pracovníka, či sociálního kurátora o dlouhodobé spolupráci (která trvala minimálně po dobu šesti měsíců) v jejímž rámci účastník aktivně spolupracoval na řešení své životní situace vedoucí ke změně svého dosavadního způsobu života. V případech, kdy čestné prohlášení bude obsahovat informaci o tom, že žadatel byl odsouzen za trestný čin, lze informaci obsaženou v takovémto čestném prohlášení považovat za citlivý údaj. Za citlivý údaj lze taktéž považovat písemné potvrzení od probačního pracovníka či sociálního kurátora. Probačního pracovníka musí navštěvovat ten, komu byl k podmíněnému propuštění nařízen probační dohled, tzn. že potvrzení od probačního pracovníka vypovídá o tom, že žadatel o byt byl odsouzen za trestný čin, a potvrzení od probačního úředníka je tedy citlivým údajem. Sociální kurátor pracuje s klientem ve všech fázích trestního řízení a po jeho skončení, to je ve výkonu trestu odnětí svobody, případně ve výkonu vazby, i na svobodě. Potvrzení od sociálního

kurátora tedy opět může vypovídat o tom, že žadatel o byt byl odsouzen za trestný čin, a toto potvrzení je tedy citlivým osobním údajem.

Na základě ustanovení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. je každý správce osobních údajů povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu. Při zpracování osobních údajů musí správce shromažďovat vždy takový rozsah osobních údajů, aby nedošlo k nadbytečnému zpracování osobních údajů. Kontrolovanou osobou je povinně od fyzických osob – žadatelů o byt požadováno čestné prohlášení, že výpis z rejstříku trestů žadatele o byt neobsahuje údaj o odsouzení za úmyslný trestný čin spolu s předloženým výpisem z rejstříku trestů, a to pouze k nahlédnutí a ověření skutečností uvedených v čestném prohlášení. V případě, že výpis z rejstříku trestů obsahuje údaj o odsouzení za úmyslný trestný čin, požaduje Kontrolovaná osoba potvrzení od sociálního nebo probačního pracovníka nebo sociálního kurátora. Zpracovávaní tohoto citlivého údaje o odsouzení za jakýkoliv úmyslný trestný čin Kontrolovanou osobou lze považovat jako nadbytečný údaj, jelikož není zřejmé, jak citlivý údaj o odsouzení za úmyslný trestný čin v obecné rovině vypovídá o tom, zda žadatel aktuálně plní či v budoucnosti bude plnit své povinnosti nájemce vůči Kontrolované osobě, resp. povinnosti vůči státu, a zda porušuje či v budoucnosti v případě uzavření nájemní smlouvy bude porušovat „dobré mravy v domě“, přičemž právě tyto skutečnosti Kontrolovaná osoba považuje za účel zpracování těchto citlivých údajů. Fakt, že žadatel má záznam v trestním rejstříku pro úmyslný trestný čin, nijak nevypovídá o jeho aktuálním chování a snaze dostát povinnostem nájemce bytu ve vlastnictví Kontrolované osoby či jeho budoucím chování vůči jiným nájemcům městských bytů nebo Kontrolované osobě či státu. I když se Kontrolovaná osoba vyjádřila tak, že na základě praxe a dlouhodobých zkušeností v oblasti pronajímání a správy bytů považuje za velmi rizikové z hlediska plnění povinností nájemce bytu, aby umožnila bydlení v bytě žadateli, který již byl odsouzen za úmyslný trestný čin, ničím nedoložila, že by žadatelé o byt, jejichž trestní rejstřík obsahuje záznam o odsouzení za úmyslný trestný čin, byli pro Kontrolovanou osobou skutečným rizikem z hlediska řádného placení nájemného a nákladů na služby. Z pohledu Kontrolované osoby by byl žadatel odsouzený např. za přijetí úplatku, podplácení nebo poškození a ohrožení životního prostředí či porušení předpisů o pravidlech hospodářské soutěže, což jsou úmyslné trestné činy, rizikem z hlediska řádného plnění povinností nájemce bytu. Takovou premisu Kontrolované osoby lze jednoznačně odmítnout jako neopodstatněnou. Lze samozřejmě Kontrolované osobě přisvědčit, že některé druhy úmyslných trestných činů mohou znamenat zvýšené riziko z hlediska plnění povinností nájemce bytu, nelze však s Kontrolovanou osobou souhlasit, že každý žadatel o byt, který neprokáže, že nebyl odsouzen za úmyslný trestný čin, je pro Kontrolovanou osobou potenciálním neplatičem a nájemcem porušujícím „dobré mravy a pořádek v domě i jeho okolí“. I Kontrolovanou osobou uváděné ustanovení § 2288 odst. 1 písm. b) zákona č. 89/2012 Sb., občanský zákoník, jež dává pronajimateli možnost vypovědět nájem v případě, je-li nájemce odsouzen pro úmyslný trestný čin spáchaný na pronajímateli nebo členu jeho domácnosti nebo na osobě, která bydlí v domě, kde je nájemcův byt, nebo proti cizímu majetku, který se v tomto domě nachází, podmínku výpovědi nájmu vztahuje pouze na úzce specifické druhy úmyslných trestných činů, a ne na všechny úmyslné trestné činy jako celek. Kontrolovanou osobou uvedený účel zpracování citlivých osobních údajů o odsouzení za úmyslný trestný čin, takto v obecné rovině mající podstatný vliv na bodové ohodnocení, resp. zařazení žadatele o byt na určité místo do pořadníku žadatelů o nájemní byt, proto nelze

považovat za zpracování osobních údajů v nezbytném rozsahu pro naplnění stanoveného účelu. Pokud existují rizikové skupiny žadatelů o byt, je možné tuto skutečnost řešit i jiným vhodným způsobem, např. i ve smlouvě.

Zpracováním nadbytečných citlivých osobních údajů žadatelů o byt, které nejsou z hlediska účelu nutné, porušila Kontrolovaná osoba povinnosti vyplývající z ustanovení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb.

Ztráta evidenčních listů (inspektor František Bartoš)

Úřad obdržel prostřednictvím poštovního přepravce v zalepené poštovní obálce celkem 15 kusů originálu Evidenčních listů, včetně průvodního anonymního dopisu, ve kterém bylo uvedeno, že tyto dokumenty byly nalezeny na veřejném prostranství.

Bylo zjištěno, že Evidenční listy byly vypracovány společností Forcorp Group spol. s.r.o. (dále také „Kontrolovaná osoba" nebo „Společnost") za rok 2014 a obsahovaly osobní údaje v rozsahu: jméno, příjmení, datum narození, rodné číslo pojištěnce, rodné příjmení, místo narození, adresu (ulice, číslo popisné, obec, pošta, PSČ), státní příslušnost, průběh pojištění v daném roce (od–do, kód, počet dnů pojištění, vyloučené doby, vyměřovací základ, doba od kdy je společnost registrována). Evidenční listy byly označeny názvem zaměstnavatele, včetně podpisu a razítka osoby, která za jejich vyhotovení zodpovídá.

Evidenční listy jsou každoročně vypracovávány pro všechny zaměstnance a jsou vypracovávány ve dvojím listinném vyhotovení. Jedno vyhotovení je určeno pro evidenci Společnosti, přičemž jsou ukládány za příslušný rok v samostatné evidenci Evidenčních listů. Druhé vyhotovení je určeno pro potřeby zaměstnance. Evidenční listy důchodového zabezpečení jsou po svém vyhotovení předávány k podpisu zaměstnancům, a to buď osobně, nebo prostřednictvím oblastního vedoucího nebo jsou zasílány prostřednictvím České pošty. K podpisu jsou předkládány vždy oba stejnopisy. Kontrolou bylo zjištěno, že vypracované Evidenční listy jsou předávány k podpisu zaměstnancům buď přímo v kanceláři mzdové účtárny, nebo jsou zasílány vedoucím detašovaných pracovišť. Dále bylo zjištěno, že Společnost nevedla žádnou evidenci zpracovaných Evidenčních listů. Přístup do kancelářských prostor, ve kterých byly zpracovávány pracovně-právní dokumenty, se neřídil žádným vnitřním předpisem, a proto nebylo možné žádným způsobem zjistit, kdy a jakým způsobem ke ztrátě došlo.

Kontrolou bylo dále zjištěno, že Kontrolovaná osoba neměla v rámci přijaté technicko-organizační dokumentace k zabezpečení ochrany osobních údajů zpracována přesná pravidla, vztahující se k ostraze jednotlivých kanceláří, pohybu osob v budově, včetně přesných pravidel evidence dokumentů obsahujících osobní údaje zaměstnanců. Kontrolou bylo konstatováno, že Společnost nesplnila povinnost správce osobních údajů přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich ztrátě, přičemž nezjistila, kdo, kdy a jakým způsobem odeslal Úřadu Evidenční listy obsahující osobní údaje jejich zaměstnanců. Tím došlo k porušení povinností dle § 13 odst. 1 zákona č. 101/2000 Sb., a to jako důsledek skutečnosti, že kontrolovaná společnost nepřijala dostatečná technicko-organizační opatření k ochraně osobních údajů, čímž porušila povinnost správce dle § 13 odst. 2 zákona č. 101/2000 Sb.

V rámci oprávnění Úřadu bylo se Společností zahájeno správní řízení, kterým bylo uloženo opatření k nápravě zjištěných nedostatků ve smyslu § 40 zákona č. 101/2000 Sb., a to zpracovat a přijmout prostřednictvím interních pracovních předpisů konkrétní opatření k zajištění

ochrany osobních údajů se stanovením přesné specifikace účelu a rozsahu zpracovávaných osobních údajů se stanovením konkrétní odpovědnosti za toto zpracování konkrétním zaměstnancům v návaznosti na účel a rozsah zpracovávaných osobních údajů zaměstnanců.

V návaznosti na kontrolní zjištění byla společnosti Forcorp Group spol. s.r.o., v rámci správního řízení, za porušení povinnosti stanovené v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnosti přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů za spáchání správního deliktu podle § 45 odst. 1 písm. h) téhož zákona, uložena pokuta ve výši 15.000 Kč, neboť jako správce nepřijala nebo neprovedla opatření k zajištění bezpečnosti zpracování osobních údajů.

Národní park Šumava – povolení ke vjezdu (inspektor František Bartoš)
Na základě obdrženého podnětu uskutečnil Úřad kontrolu ve Správě Národního parku Šumava, a to ve věci kontroly dodržování povinností správce osobních údajů, v souvislosti se zpracováním osobních údajů subjektů údajů při udělování výjimek podle § 43 odst. 3 a 4 ze zákazu dle § 16 odst. 1 písm. d) zákona č. 114/1992 Sb., o ochraně přírody a krajiny, zejména pak okolnosti vydávání a užívání „Potvrzení o výjimce" ze zákazu vjíždět a setrvávat s motorovými vozidly mimo silnice, místní komunikace a místa vyhrazená se souhlasem orgánu ochrany přírody v Národním parku Šumava.

Kontrolou bylo zjištěno, že Správa NP Šumava za účelem vedení povolovacího řízení dle zákona č. 114/1992 Sb. v rámci správního řízení shromažďuje a zpracovává osobní údaje žadatelů o vydání povolení v rozsahu: jméno, příjmení, adresa, registrační značka vozidla, resp. osobní údaje vztahující se ke třetím osobám, které zajišťují pro žadatele různé práce, služby, opravy apod., identifikace komunikace, prostoru a doby pro parkování, včetně informace o adrese nemovitosti, která se vztahuje ke konkrétnímu vozidlu, tedy oprávnění vjíždět a setrvávat v NP Šumava, účel vjezdu a setrvání osob a vozidel, informací vztahujících se k účelu žádosti, tedy vlastnictví nemovitosti, sloužící k bydlení, rekreačním účelům nebo podnikání, vlastnictví pozemků, trvalému užívání, rekreaci, včetně uvedení parcelního čísla dle katastrální mapy, dále číslo jednací a datum rozhodnutí správního řízení, informaci o konkrétním rozsahu platnosti výjimky. Současně jsou v souladu s § 70 až 74 zákona č. 114/1992 Sb. s osobními údaji žadatele a dalších osob seznamována i dotčená občanská sdružení a obce.

Kontrolou bylo dále zjištěno, že Správa NP Šumava za účelem vydání „Potvrzení o výjimce" ze zákazu vjíždět a setrvávat s motorovými vozidly mimo silnice, místní komunikace a místa vyhrazená se souhlasem orgánu ochrany přírody v Národním parku Šumava zpracovává osobní údaje přímo na Potvrzení, a to ke vjezdu motorových vozidel, v rozsahu jméno, příjmení, adresa bydliště, registrační značka vozidla, adresa nemovitosti, ke které se výjimka vztahuje, parcelní číslo dle katastrální mapy, identifikace přístupové či příjezdové komunikace, identifikace místa pro setrvání (parkování) vozidla, účel a doba platnosti výjimky, datum a podpis zástupce Správy NP Šumava. Držitele výjimky zavazuje, aby Potvrzení (oboustranně potištěný papírový karton) bylo umístěno za přední sklo vozidla tak, aby přední strana Potvrzení byla čitelná. Účelem bylo, aby kontroly prováděné v terénu, a to profesionální i laické, měly umožněny jednoduchou kontrolu oprávnění vjezdu či setrvání v NP Šumava.

Kontrolou bylo konstatováno, že k naplnění stanového účelu je dostačující zpřístupnit kontrolním pracovníkům, profesionálním i laickým, osobní údaje v rozsahu RZ (dříve SPZ) vozidla,

časová a územní platnost a číslo výjimky, dále účel vjezdu a označení orgánu, který Potvrzení o výjimce vydal a schválil, případně jednací číslo správního řízení. Takovýto rozsah informací neomezuje žádným způsobem výkon kontroly.

Kontrolou bylo tedy konstatováno, že Správa NP Šumava tím, že stanovila povinnost umístit „Potvrzení o výjimce" ke vstupu do I. zóny za přední sklo vozidla tak, aby byly informace uvedené na přední straně čitelné vně vozidla, porušila povinnost správce osobních údajů přijmout taková opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům.

S ohledem na skutečnost, že Správa Národního parku Šumava neprodleně po zahájení kontroly připravila změnu interních směrnic, které upravují postupy při udělování výjimek ze zákazu vjíždět a setrvávat v NP Šumava, a to včetně změny přístupu zpracování osobních údajů uváděných přímo na povolení, bylo rozhodnuto o přístupu dle § 40a zákona č. 101/2000 Sb., tj. neukládat pokutu za spáchání správního deliktu.

Využívání osobních údajů za účelem zřízení marketingových karet (inspektor František Bartoš)

Na základě obdrženého podnětu uskutečnil Úřad kontrolu ve Stavebním bytovém družstvu Zahradní město (dále také „SBD", „Družstvo" nebo „Kontrolovaná osoba"). Podnět upozorňoval na jednání Družstva, které jako člen Družstevního marketingového sdružení Česká republika zajišťoval pro své členy a pro své klienty možnost využívání věrnostního programu Sphere Card, prostřednictvím slevové karty Sphere, umožňující slevy na různé produkty a služby vybraných obchodních společností. Poskytování těchto služeb bylo členům nabízeno za účelem zlepšení péče o členy a klienty SBD, a to bez jejich souhlasu.

Bylo zjištěno, že SBD zpracovává osobní údaje v rámci vlastní činnosti v oblasti správy bytového fondu a správy nemovitostí elektronicky i písemně pro své vlastní členy. Na základě smluv s jinými stavebními družstvy a Společenstvími vlastníků bytových jednotek zajišťuje dodavatelské služby správy bytového fondu a správy nemovitostí, a to včetně elektronického zpracování osobních údajů jejich členů a rodinných příslušníků, včetně osob bydlících v bytových nástavbách. SBD zpracovává osobní údaje v databázi členů a klientů (a v rámci pasportu bytů) elektronicky i v listinné podobě.

Kontrolou bylo zjištěno, že na základě příkazních smluv o zpracování ekonomických agend a smluv o zajišťování správy vykonává Družstvo pro dalších 117 samostatných právních subjektů správu společných částí domů, pozemků a některých služeb spojených s užíváním jednotek (účetnictví atd.).

Přístup k listinné podobě (pasportu bytů) i k elektronické databázi je umožněn pouze na základě pracovní náplně zaměstnanců. Představenstvo Družstva rozhodlo o vypracování databáze, obsahující přehled osobních údajů v rozsahu jméno, příjmení, číslo bytu, a tento přehled předalo v elektronické podobě Družstevnímu marketingovému sdružení Česká republika za účelem nabídky slevového programu Sphere Card, přičemž číslo bytu je zakódováno v číselné řadě, uvedené na slevové kartě Sphere. Toto číslo je jedinečný informační údaj, který se vztahuje ke konkrétnímu bytu, a to bez ohledu, zda se jedná o byt, který je užíván členem Družstva, nebo bytu v osobním vlastnictví, který je součástí samostatného SVJ, pro který Družstvo zabezpečuje služby správy bytů za úplatu, resp. pro jiná stavební družstva a bytové nástavby. Informace o programu slevových karet byla předána zástupcům jednotlivých samospráv, SBD a Společenství vlastníků jednotek, kteří měli informovat své členy. O vyhotovení slevových karet

pro členy a klienty Družstva a jiných subjektů, pro které provádí Družstvo správu, rozhodlo představenstvo Družstva na svém zasedání.

Slevové karty Sphere vyhotovila společnost EFIN spol. s r.o. na základě kupní smlouvy uzavřené s Družstevním marketingovým sdružením Česká republika za úplatu. V předmětu smlouvy bylo uvedeno: Karty věrnostního programu Sphere Card umožňují jejich oprávněným držitelům využívat výhod poskytovaných partnerskými firmami společnosti EFIN spol. s r.o. po celou dobu platnosti karty. Společnost EFIN spol. s r.o. jako prodávající převádí na kupujícího Družstevní marketingové sdružení Česká republika vlastnické právo k těmto kartám věrnostního programu Sphere Card, jejichž dodání je upraveno uvedenou smlouvou, a to včetně práva pro jejich oprávněné držitele, využívat všech výhod poskytovanými partnerskými firmami společnosti EFIN spol. s r.o. Platnost karet je sjednána na pět let od data vydání karet, nejdéle však do 31. prosince 2020.

Po vyhotovení slevových karet, byly tyto následně prostřednictvím SBD distribuovány jednotlivým členům a klientům prostřednictvím zástupců konkrétních samospráv, SBD a Společenstvím vlastníků jednotek, pro které Družstvo zajišťuje na základě smlouvy správcovské služby.

V období roku 2011 až 2015 bylo SBD dodáno od Družstevního marketingového sdružení Česká republika 6.742 slevových karet. Členům a klientům Družstva bylo rozdáno 6.172 slevových karet. Pro období roku 2016 až 2020 bylo SBD od Družstevního marketingového sdružení Česká republika dodáno 7.648 slevových karet. Členům Družstva a klientům bylo předáno celkem 5.967 slevových karet. Slevové karty Sphere byly SBD v minulosti objednány v roce 2004 na tři roky, tj. do roku 2006, od roku 2007 na tři roky, tj. do roku 2009, a v roce 2011 na pět let, tj. do roku 2015.

Kontrolou bylo konstatováno, že SBD jako správce osobních údajů svých členů a klientů a jako zpracovatel osobních údajů členů a klientů jiných subjektů na základě příkazních smluv předalo bez souhlasu subjektů údajů jejich osobní údaje v rozsahu jméno, příjmení a číslo bytu Družstevnímu marketingovému sdružení Česká republika, které je následně předalo dalšímu správci osobních údajů společnosti EFIN spol. s r.o., a to za účelem realizace slevového programu Sphere Card, který držitelům umožňuje využívat výhody poskytované partnerskými firmami společnosti EFIN spol. s r.o. pro svoje klienty, a to prostřednictvím výroby slevových karet.

Na základě výše uvedených skutečností a po posouzení celé záležitosti bylo kontrolujícími konstatováno, že Družstvo porušilo ustanovení § 5 odst. 2 zákona č. 101/2000 Sb., jelikož osobní údaje členů Družstva, nájemníků, družstevníků jiných SBD, vlastníků bytů jiných SVJ v rozsahu jméno, příjmení a číslo bytu předalo jinému správci osobních údajů, Družstevnímu marketingovému sdružení Česká republika, bez souhlasu subjektů údajů, přičemž výjimky uvedené v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. se na uvedené zpracování osobních údajů nevztahují.

V návazném správním řízení byla Družstvu za spáchání správního deliktu podle § 45 odst.1 písm. e) zákona č. 101/2000 Sb. uložena pokuta ve výši 40.000 Kč.

S ohledem na rozhodnutí Představenstva SBD ukončit činnost v rámci programu Sphere Card nebylo s Kontrolovanou osobou zahájeno řízení o uložení opatření k nápravě ve smyslu § 40 zákona č. 101/2000 Sb.

Kontrola spolku Mamma HELP (inspektor Daniel Rovan)

Na základě stížností inspektor Úřadu počátkem roku 2016 provedl kontrolu zájmového spolku Mamma HELP (dále také „Kontrolovaný"), jejímž předmětem bylo upozornění na obesílání

přispěvatelů a osob oslovovaných se žádostí o finanční příspěvek a s tím spojené zpracovávání, zejména aktualizace, osobních údajů oslovených subjektů, včetně zemřelých.

Stížnosti podávali příbuzní oslovených nežijících osob, kteří vnímali tuto korespondenci za necitlivou a cítili se tímto způsobem získávání finanční podpory dotčeni.

Kontrolou bylo zjištěno, že Kontrolovaný má zpracovaný vnitřní předpis pro ochranu osobních údajů a jeho zaměstnanci byli s předpisem prokazatelně seznámeni. Dále bylo zjištěno, že Kontrolovaný sám výběr adresátů – potenciálních dárců neprovádí. Za tímto účelem má uzavřenu rámcovou smlouvu se společností prodialog, s.r.o., která pro Kontrolovaného zajišťuje službu *direkt mailing*, a která v této souvislosti obstarává adresy potenciálních dárců, jež obesílá se žádostí o finanční podporu pro Mamma HELP, z.s. Toto činí na základě smlouvy o zpracování osobních údajů, jejímž předmětem je zpracovávání zveřejněných osobních údajů za účelem fundraisingu pro Kontrolovaného, a to na základě rámcové smlouvy.

Spolek Mamma HELP s těmito adresami nepřichází do styku. Pouze v případě, že oslovení na žádost o podporu reagují kladně a stanou se jeho dárci, jsou jejich osobní údaje zpracovávány v databázi dárců.

Kontrolou byly prověřovány povinnosti správce ve smyslu § 5 odst. 1 písm. c), § 5 odst. 2 a § 11 odst. 1 zákona č. 101/2000 Sb. Bylo zjištěno porušení § 11 odst. 1, tedy informační povinnosti, neboť subjektům údajů byla poskytována mylná informace spočívající v tom, kdo je zpracovatelem (změna jména obchodní firmy, neuvedené IČO) jejich osobních údajů, neboť dopisy se žádostmi byly opatřeny názvem a logem partnerské společnosti, které již nebyly aktuální a neodpovídaly skutečnosti. Mohly tedy být pro oslovené matoucí, neboť je oslovovala de iure neexistující společnost. Vzhledem k tomu, že Kontrolovaný přijal opatření k nápravě již v průběhu kontroly a že porušení nepředstavovalo významný zásah do soukromí, nebyla uložena pokuta.

Kontrolní závěry vedly k provedení následné kontroly u dalšího subjektu, a to společnosti prodialog s.r.o., která byla v době konání kontroly smluvním partnerem Mamma HELP, z.s. Kontrolou bylo zjištěno porušení § 5 odst. 1 písm. c), neboť společnost prodialog s.r.o. neaktualizovala osobní údaje konkrétní osoby, jejíž osobní údaje v době kontroly nebyly již několik let veřejně dostupné, a která v důsledku neprovedené aktualizace byla obeslána jako potenciální dárce, přestože v době zaslání žádosti již nežila. Vzhledem k tomu, že Kontrolovaný přijal opatření k nápravě již v průběhu kontroly a vzhledem k nízké společenské nebezpečnosti nebyla pokuta uložena.

Kreditech Česká republika s.r.o. (inspektor Daniel Rovan)

V lednu 2016 obdržel Úřad stížnost od *Hamburské kanceláře zmocněnce pro ochranu osobních údajů a svobodný pohyb informací*, ve které byl požádán o prošetření postupů při nakládání s osobními údaji společností Kreditech Česká republika s.r.o. (dále také „Kontrolovaný"), součásti německého holdingu Kreditech Holding SSL GmbH. V podnětu bylo poukazováno na „*extensive data collection, automated individual decision, no freely given consent, endless retention*".

Předmětem činnosti společnosti Kreditech Česká republika je mimo jiné poskytování nebo zprostředkování spotřebitelského úvěru, a to formou online půjčky, která díky automatizovanému úvěrovému systému funguje 24 hodin denně. Společnost je registrována u Úřadu a jako první účel zpracování je uvedeno posouzení úvěruschopnosti žadatele o úvěr, identifikace klienta. Druhým účelem je vytvoření souboru informací v rámci nebankovního registru klientských

informací sdružení (CNCB), zajištění vzájemného informování s dalšími finančními institucemi, které jsou členy CNCB a členy CBCB (bankovní registr klientských informací). Zdrojem osobních údajů jsou zákazníci (klienti) a jako jiné zdroje jsou uvedeny registry dlužníků.

Kontrolou bylo zjištěno, že Kreditech má přijata opatření k ochraně osobních údajů v dokumentu *Všeobecné zásady ochrany osobních údajů a soukromí*. V něm se mj. uvádí, že společnost používá šifrovací zabezpečení k ochraně osobních údajů. Osobní údaje jsou uloženy na serverech zabezpečených firewallem a společnost má zavedeny postupy pro neoprávněný přístup, zničení, používání, měnění a sdělování osobních údajů. Všichni zaměstnanci a zástupci třetích stran, kteří mají přístup k osobním údajům, jsou vázáni zvláštní povinností mlčenlivosti.

Dalším prověřovaným dokumentem byla *Rámcová úvěrová smlouva*, která upravuje podmínky jednotlivých smluv o úvěru uzavíraných mezi Kontrolovaným a klientem na základě jednotlivých žádostí klienta o poskytnutí úvěru a související právní vztahy. V dokumentu je uvedeno, že jednotlivé smlouvy o úvěru se uzavírají za užití prostředku komunikace na dálku, a to prostřednictvím textových zpráv SMS, nebo prostřednictvím formuláře pro uzavření jednotlivé smlouvy o úvěru umístěného v rámci uživatelského účtu. Pokud by bylo vyžadováno uzavření této rámcové smlouvy o úvěru v tištěné formě, je Kreditech oprávněn vyžadovat rovněž uzavření jednotlivé smlouvy o úvěru v tištěné podobě. V části týkající se ochrany osobních údajů je uvedeno, že ke zpracování osobních údajů klienta, který je fyzickou osobou, dochází v souladu se zákonem č. 101/2000 Sb. Poskytnutí osobních údajů klienta je dobrovolné. V rozsahu, v jakém je věřitel dle zákona povinen osobní údaje klientů zpracovávat, je jejich poskytnutí podmínkou pro uzavření smlouvy a poskytování služeb ze strany věřitele.

Rámcová úvěrová smlouva je komplexním dokumentem, ve kterém se Kreditech vypořádává s povinnostmi správce osobních údajů, včetně souhlasů se zpracováním, kopírováním občanského průkazu nebo informační povinností. Dále je zde řešen souhlas klienta s formou komunikace mezi ním a společností prostřednictvím elektronické pošty.

Kontrolou bylo zjištěno, že Kreditech Česká republika, s.r.o. využívá know-how mateřské společnosti Kreditech Holding SSL GmbH, Hamburg, a to na základě Smlouvy o poskytování externích služeb, ve které je uvedeno, že Kreditech Česká republika s.r.o. je stoprocentně vlastněná pobočka společnosti Kreditech Holding SSL GmbH a při poskytování služeb mikrofinancování výhradně pro solventní úvěrované s vysokou pravděpodobností, že úvěr splatí, využívá společnost Kreditech Česká republika s.r.o. při hodnocení potenciálních úvěrovaných software, který jí poskytne Kreditech Holding SSL GmbH.

Vzhledem k typu poskytované služby se kontrola zaměřila také na zpracovávání osobních údajů ze sociálních sítí. Ze zjištění vyplynulo, že Kreditech tyto údaje využívá k částečnému ověření totožnosti žadatele o úvěr a pro zabránění podvodným žádostem. Data získaná z připojení prostřednictvím sociálních sítí nepoužívá k hodnocení. Zákazníci se, pokud se tak sami rozhodnou, připojí k webové stránce společnosti prostřednictvím svých sociálních sítí k dalšímu doložení toho, že daný zákazník existuje. K hodnocení úvěrového rizika používá Kreditech pouze skutečnost, zda se zákazník připojil prostřednictvím sociální sítě či nikoli. Tento krok je dobrovolný a potenciální klient je motivován lepšími úvěrovými podmínkami, např. možností získat slevu až 15 %.

Přestože Kreditech Česká republika s.r.o. nabízí dva různé úvěrové produkty (K24 1.000 až 15.000 Kč a Zaimo 15.000 až 75.000 Kč), ve svých dokumentech deklaruje, že cílem společnosti je vystupovat jako spolehlivý věřitel zaručující že jeho produkty jsou vhodné pro jeho zákazníky

a že všem dlužníkům je zaručena úplná ochrana, kterou jim poskytují české právní předpisy. Společnost Kreditech Česká republika s.r.o. se zaměřuje nejen na dostupnost svých produktů, ale také na to, aby s jejími zákazníky bylo zacházeno stejně, bez ohledu na výši úvěru, o kterou zažádali. Na zákazníky, kterým byl udělen úvěr ve výši více než 25.000 Kč, se vztahují dodatečná opatření v rámci boje proti praní špinavých peněz.

Kontrolou byly prověřovány povinnosti správce ve smyslu § 5 odst. 1 písm. a) a b), tedy povinnost stanovit účel, prostředky a způsob zpracování osobních údajů, § 5 odst. 1 písm. d), tedy shromažďování osobních údajů v rozsahu nezbytném pro naplnění stanoveného účelu a § 5 odst. 1 písm. e), tedy uchovávání osobních údajů pouze po dobu, která je nezbytná k účelu jejich zpracování. Kontrolou nebylo zjištěno porušení těchto povinností.

Dalšími prověřovanými ustanoveními byly § 5 odst. 2 a § 4 písm. n), které ukládají správci zpracovávat osobní údaje pouze se souhlasem subjektu údajů s tím, že souhlasem se rozumí svobodný a vědomý projev vůle subjektu údajů. Ani zde nebylo porušení povinností správce zjištěno.

Kontrolou byla prověřena povinnost správce informovat subjekt údajů o tom, v jakém rozsahu a pro jaký účel budou jeho osobní údaje zpracovávány (§ 11 odst. 1 a odst. 2). Z kontrolních zjištění vyplývá, že klient souhlasí se získáváním, shromažďováním, zpracováním a uchováváním osobních údajů věřitelem, a to pro účely uzavření jednotlivé smlouvy o úvěru, poskytnutí úvěru a následné správy úvěru (včetně případných kroků souvisejících s vymáháním či postoupením pohledávek z úvěru), ověření identity klienta, posouzení jeho platební morálky.

S odkazem na stanovisko Úřadu č. 3/2014 k nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a k výše uvedeným kontrolním zjištěním kontrolující konstatovali porušení § 11 odst. 2 zákona č. 101/2000 Sb.

Nakonec bylo prověřováno ustanovení § 27 týkající se předávání osobních údajů do členských států EU, resp. do třetích zemí (tj. mimo území členských států EU). Z kontrolních zjištění vyplývá, že Kontrolovaný předává osobní údaje do USA a Singapuru, tj. do zemí, které jsou z hlediska úrovně ochrany osobních údajů považovány za tzv. třetí země, a dále také, že na tzv. „Safe Harbor List" byly uvedeny společnosti Zendesk, Inc., Twilio, Inc. a Google Inc. (smluvní partneři Kreditech Česká republika, s.r.o.). Z kontrolních zjištění dále vyplynulo, že spolupráce s těmito partnery probíhala v určitém období pouze na základě Všeobecných obchodních podmínek.

S ohledem na kontrolní zjištění a stanovisko Úřadu č. 2/2010 – Předání osobních údajů do jiných států, ve kterém se mimo jiné uvádí: *Institut souhlasu je pouze jednou z alternativ předání osobních údajů do třetích zemí, nicméně v současné době nejčastěji využívanou. V tomto případě je nutné, aby správce Úřadu předložil vzorové znění souhlasu, ze kterého musí být jasně zřetelné, do jakých zemí správce hodlá osobní údaje subjektu údajů předávat a kdo je jejich příjemcem. Subjekt údajů by měl být rovněž srozuměn s tím, že země, do kterých budou jeho osobní údaje předány, neposkytují přiměřenou úroveň ochrany osobních údajů*, nebylo možné výjimku uvedenou v ustanovení § 27 odst. 3 písm. a) zákona č. 101/2000 Sb. vztáhnout a kontrolou bylo konstatováno porušení § 27 zákona č. 101/2000 Sb.

Společnost Kreditech Česká republika, s.r.o. podala v řádném termínu námitku proti kontrolnímu zjištění týkajícímu se porušení § 27 zákona č. 101/2000 Sb. Tato námitka byla předsedkyní Úřadu zamítnuta. V návaznosti na kontrolní zjištění byla společnosti uložena sankce ve výši 50.000 Kč.

Eiscafe Delikana – provozování kamerového systému se záznamem (inspektor Josef Vacula)

Úřad zahájil kontrolu na základě podnětu, který byl doručen dne 24. září 2015. Předmětem kontroly bylo dodržování povinností správce a zpracovatele osobních údajů stanovených v hlavě II zákona č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů v provozovně Eiscafe Delikana (dále také „Kontrolovaná osoba"), provozováním kamerového systému se záznamovým zařízením v provozovně Kontrolované osoby.

V rámci kontroly bylo zjištěno, že v provozovně Kontrolované osoby je kamerový systém, který je tvořen šesti kamerami a řídící jednotkou se záznamem, který je po 48 hodinách automaticky přepisován záznamem novým. Tyto kamery snímají prostory, ve kterých se pohybují zákazníci i zaměstnanci Kontrolované osoby s výjimkou jedné kamery, která snímá pouze zaměstnance Kontrolované osoby v zázemí provozovny, konkrétně v kuchyni. V provozovně Kontrolované osoby se pak dále nachází jedna kamera, která je v současnosti mimo provoz, a pokud v provozu je, tak je provozována v režimu on-line, a tedy záznamy nepořizuje.

Kontrolující inspektor vyhodnotil zjištěný stav věci a konstatoval, že Kontrolovaná osoba provádí zpracování osobních údajů, neboť prostřednictvím kamerového systému shromažďuje a ukládá na záznamové zařízení obrazový záznam. Z dlouhodobé výkladové praxe Úřadu vyplývá, že délka uchování záznamu musí být stanovena tak, aby nepřesáhla dobu potřebnou k tomu, aby incident zaznamenaný kamerou bylo možno dále prošetřit a zajistit další nezbytné informace potřebné například k předání věci příslušným orgánům. Za takovou nezbytnou dobu je považována doba zpravidla 7 dnů, v případě příležitostně navštěvovaných prostor pak až 14 dnů. Kontrolovaná osoba ve vnitřním předpise o provozování kamerového systému deklarovala, že záznam se uchovává 48 hodin s ohledem na uchování záznamu a případné dohledání zaznamenaných událostí, z toho důvodu kontrolující inspektor konstatoval, že nebylo zjištěno porušení povinností stanovených § 5 odst. 1 písm. e) zákona č. 101/2000 Sb.

Kontrolou bylo dále zjištěno, že Kontrolovaná osoba provádí zpracování osobních údajů prostřednictvím kamerového systému se záznamovým zařízením bez souhlasu subjektu údajů (zaměstnanců a návštěvníků jeho provozovny). Kontrolující se proto zabýval otázkou, zda je na toto zpracování osobních údajů aplikovatelné ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., které umožňuje zpracovávat osobní údaje bez souhlasu subjektu údajů, „pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života". Kontrolující provedl test proporcionality, tj. ověřil skutečnost, do jaké míry Kontrolovaná osoba zpracováním osobních údajů zasáhla do soukromého a osobního života snímaných osob. Kontrolou bylo zjištěno, že provozovna Kontrolované osoby je v provozních hodinách volně přístupná veřejnosti a sestává ze dvou podlaží. Tato provozovna je umístěna v centrální části města, kde je možno předpokládat zvýšený pohyb osob. Při provádění testu proporcionality, tj. ověřování skutečností, do jaké míry Kontrolovaná osoba zpracováním osobních údajů zasáhla do soukromého a osobního života snímaných osob, zejména svých zaměstnanců, kontrolující bral v úvahu i příslušná ustanovení zákona č. 262/2006 Sb., zákoník práce.

Ustanovení § 316 odst. 2 zákona č. 262/2006 Sb. předpokládá naplnění dvou základních podmínek pro užití sledovacích a kontrolních mechanismů, a sice závažný důvod spočívající ve zvláštní povaze činnosti a informování zaměstnance o této činnosti. Správce je proto povinen

vyhodnotit vyváženost použitých technických prostředků a míru zásahu do soukromí subjektu údajů. Vzhledem k tomu, že zákoník práce umožňuje zaměstnavateli provádění přiměřené kontroly za splnění uvedených podmínek, není v těchto případech nutný souhlas zaměstnance s prováděnou či zamýšlenou kontrolou. Dále bylo zjištěno, že Oblastní inspektorát práce pro Jihomoravský a Zlínský kraj v rámci svého kontrolního šetření dospěl k závěru, že Kontrolovaná osoba bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušuje soukromí zaměstnanců na pracovišti a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému sledování. Dle kontrolního zjištění Oblastního inspektorátu práce pro Jihomoravský a Zlínský kraj tímto Kontrolovaná osoba nedodržela povinnosti dle ustanovení § 316 odst. 2 zákona č. 262/2006 Sb.

Kontrolující inspektor dále přihlédl k nastavení zorného úhlu kamer, i přesto, že nastavení kamer je provedeno tak, aby snímaly především vchody do provozovny, dále její veřejně přístupné průchozí části, oblast pokladny a také oblast kuchyně, která je přístupná pouze jejím zaměstnancům, jsou ve většině případů v jejich zorném poli také prostory určené ke konzumaci zákazníků. Dle vyjádření Kontrolované osoby je záznam prováděn pouze za účelem zadokumentování případné trestné činnosti, respektive má také funkci prevence proti trestné činnosti. Pro tyto potřeby se záznam ukládá na záznamové zařízení, které je chráněno heslem a nachází se v místnosti, jejíž zámek je zabezpečen číselným kódem, který znají jen dva jednatelé společnosti. Kamerový systém pracuje izolovaně a autonomně a není propojen s dalším zařízením evidujícím jakákoliv data o zaměstnancích.

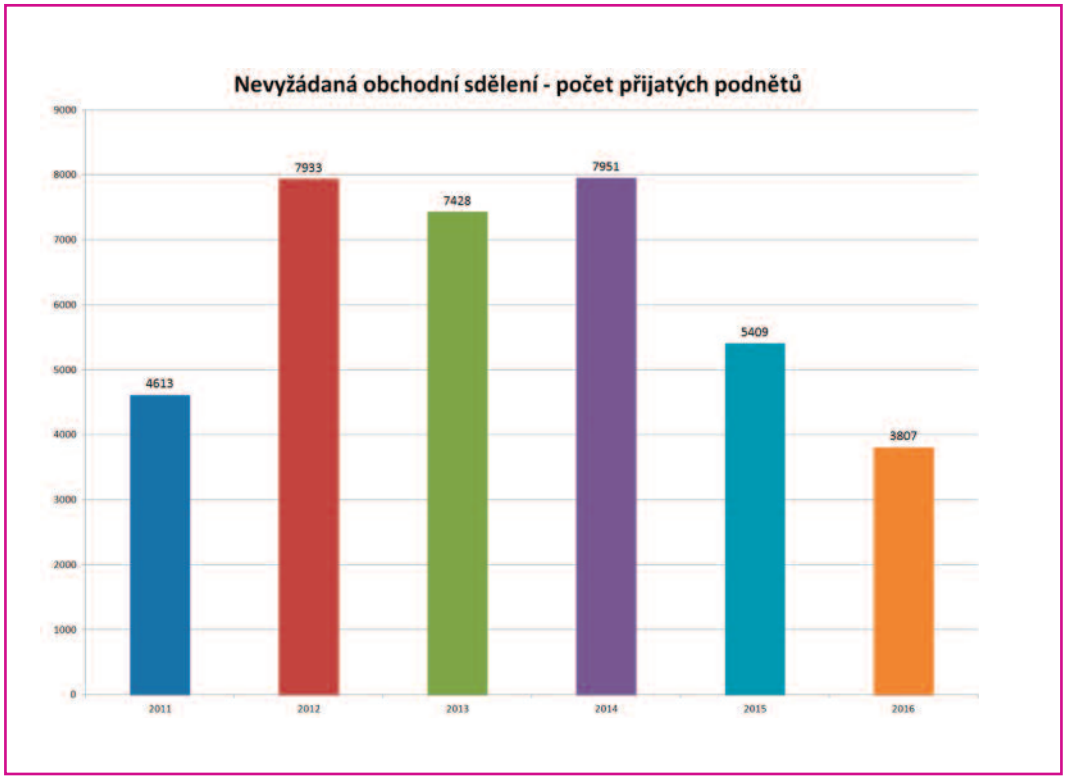
Kontrolující inspektor vyhodnotil zjištěný stav věci a dospěl k závěru, že provozováním předmětného kamerového systému dochází k zásahu do soukromí osob, které se pohybují ve snímaném prostoru, tedy do soukromí zaměstnanců Kontrolované osoby a návštěvníků a zákazníků její provozovny. Současně je kontrolující názoru, že provozovna Kontrolované osoby čítá dvě podlaží a v takto rozsáhlém prostoru není možno zajistit ochranu majetku lidskými silami a ochranu majetku užívaného v souvislosti s podnikatelskou činností Kontrolované osoby v její provozovně by se dalo považovat za ochranu práv a právem chráněných zájmů správce osobních údajů s tím, že za zásah do soukromí lze za přiměřený považovat pouze záznam z jedné kamery, která zaznamenává prostor celého baru společně s prostorem pokladny a hlavního vstupu do provozovny. Nepřiměřený zásah do soukromí kontrolující konstatoval v případě záznamů pořízených pěti kamerami, a tak konstatoval porušení § 5 odst. 2 zákona č. 101/2000 Sb., neboť vzhledem k záběrům snímaných těmito pěti kamerami nelze na předmětné zpracování osobních údajů aplikovat výjimku dle § 5 odst. 2 písm. e) téhož zákona.

Kontrolující inspektor dále zjišťoval, zda Kontrolovaná osoba postupovala při zpracování osobních údajů v souladu s § 11 zákona č. 101/2000 Sb., podle kterého je „správce při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace známy". Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených § 21 zákona č. 101/2000 Sb., tj. právu subjektu údajů v případě zjištění či domněnky, že správce nebo zpracovatel provádí zpracování jeho osobních údajů v rozporu s ochranou soukromého a osobního života, na podání vysvětlení a na žádost o odstranění protiprávního stavu. Kontrolou bylo zjištěno, že Kontrolovaná osoba splnila svou informační povinnost vůči subjektům údajů, tedy postupovala

v souladu s § 11 zákona č. 101/2000 Sb. Kontrolující dále posuzoval, zda Kontrolovaná osoba postupovala při zpracování osobních údajů v souladu s § 13 zákona č. 101/2000 Sb., tj. zda přijala taková opatření, aby zabezpečila zpracovávané osobní údaje. Po posouzení zabezpečení ze strany Kontrolované osoby kontrolující inspektor konstatoval, že Kontrolovaná osoba postupovala v souladu s § 13 zákona č. 101/2000 Sb. Vzhledem k tomu, že Kontrolovaná osoba v rámci kontroly uvedla, že o oznamovací povinnosti dle § 16 odst. 1 zákona č. 101/2000 Sb. nevěděla, a tudíž tuto povinnost nesplnila, kontrolující inspektor zároveň konstatoval, že Kontrolovaná osoba porušila § 16 odst. 1 zákona č. 101/2000 Sb., zároveň však uvedl, že v kontextu aktuálních přístupů evropské legislativy k dané problematice kontrolující považuje v tomto případě porušení oznamovací povinnosti samo o sobě za méně závažné.

Na základě kontrolního zjištění, ze kterého vyplývá porušení § 5 odst. 2 zákona č. 101/2000 Sb., byla v navazujícím správním řízení Kontrolované osobě uložena povinnost provést přenastavení kamer, a to tak, aby nezaznamenávaly prostor, kde hosté konzumují, tedy zejména prostor, kde jsou umístěny stoly a židle, a to např. nastavením jiného zorného úhlu kamery nebo zajištěním rastrem, dále pak zcela demontovat a odstranit kameru, která snímá prostor kuchyně a především zaměstnance, kteří se v tomto prostoru pohybují, a dodatečně splnit oznamovací povinnost podle § 16 odst. 1 zákona č. 101/2000 Sb. Vzhledem k tomu, že Kontrolovaná osoba provozováním kamerového systému se záznamem umístěného v prostorách své provozovny ve Zlíně bez potřebného předchozího souhlasu všech subjektů údajů (zákazníků či zaměstnanců) porušila ustanovení § 5 odst. 2 zákona č. 101/2000 Sb., byla jí uložena pokuta ve výši 30.000 Kč.

NEVYŽÁDANÁ OBCHODNÍ SDĚLENÍ



Šíření nevyžádaných obchodních sdělení (SPAM) je delikt, který zejména v poslední době nabývá nových forem a metod. V České republice upravuje šíření obchodních sdělení zákon č. 480/2004 Sb., o některých službách informační společnosti. Jedná se v principu o transpozici evropských směrnic 2000/31/EU, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu a 2002/58/EU o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. To znamená, že v celé Evropě jsou postupy proti šíření nevyžádaných obchodních sdělení v principu, až na drobné výjimky, stejné. Z kontrolní praxe lze vypozorovat nové formy šíření nevyžádaných obchodních sdělení. Český zákon č. 480/2004 Sb. zakazuje šířit nevyžádaná obchodní sdělení bez souhlasu příjemce. Některé společnosti se rozhodly obcházet zákon tak, že si najmou firmu, která za úplatu šíří obchodní sdělení místo nich, „Systém bílý kůň". Pro ilustraci lze uvést průběh a výsledek kontroly níže u společnosti:

EC PROFIT s.r.o. (inspektor Josef Vacula)
Text sdělení, který byl zasílán a který je součástí jednotlivých stížností, obsahoval obchodní nabídky různých společností s odkazy na internetové stránky. Jednalo se například o nabídku bytových doplňků, nabídku rozesílky obchodních sdělení pro čtenáře crazymag, nabídku on-line hry od bohemia casino, nabídku doplňků stravy, nabídku jazykových kurzů apod. V předmětu každého sdělení byl uveden krátký text obsahující určitý souhrn v těle zprávy obsažené nabídky. Společnost EC PROFIT s.r.o. (dále také „Kontrolovaná osoba) si na šíření spamu najala dvě společnosti. V patičkách či na závěr zasílaných zpráv bylo uvedeno: „Distribuci obchodního sdělení zajišťuje společnost Beckinsale, s.r.o., se sídlem: Bubenská 1, Praha 7 – Holešovice 170 00, IČ: 247 95 691. Nepřejete-li si dostávat naše novinky a zvýhodněné nabídky pouze pro Vás: klikněte na tento odkaz." Nebo „Distribuci obchodního sdělení zajišťuje společnost JDI International, s.r.o., se sídlem: Újezd 40, 118 00 Praha 1, IČ: 292 35 111. Nepřejete-li si dostávat naše novinky a zvýhodněné nabídky pouze pro Vás: klikněte na tento odkaz." Nebo „Distribuci obchodního sdělení zajišťuje crazymag.cz. Nepřejete-li si dostávat naše novinky a zvýhodněné nabídky pouze pro Vás, klikněte na odkaz zde." Nebo v případě nabídky rozesílky obchodních sdělení pro čtenáře kouzelnavarecka.cz byl kromě samotné nabídky v patičce odesílaných zpráv uveden jen kontakt ve tvaru jméno, příjmení, telefonní číslo, e-mail a webová stránka.

Obchodním sdělením se rozumí 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 (§ 2 písm. f) zákona č. 480/2004 Sb.).

Na základě analýzy textů přijatých zpráv bylo zjištěno, že předmětná sdělení, která byla zasílána prostřednictvím elektronické pošty, odpovídají definici obchodního sdělení ve smyslu § 2 písm. f) zákona č. 480/2004 Sb., neboť obsahovala obchodní nabídky a sloužila k podpoře podnikatelské činnosti různých subjektů.

Majiteli odesílajících IP adres jsou společnosti Amazon Technologies Inc, OVH Hosting, Inc., OVH IE Technical Contact a WEDOS Internet, a.s. Všechna obchodní sdělení byla zaslána prostřednictvím služby sendik.cz (www.sendik.cz). Poskytovatelem této služby je společnost EC PROFIT, s.r.o.

V rámci kontrolních šetření byla provedena analýza odesílajících e-mailových adres, pokud jde o doménová jména. Dále byli požádáni o součinnost poskytovatelé hostingových služeb.

Téměř všechny domény, z nichž byla nevyžádaná obchodní sdělení zasílána, jsou registrovány na EC PROFIT s.r.o., případně Beckinsale, s.r.o.

Společnost EC PROFIT s.r.o. byla požádána nejprve o vysvětlení, a to dopisem a dále pak v Oznámení o zahájení kontroly. V těchto dokumentech byla společnost EC PROFIT s.r.o. požádána o vyjádření, zda odeslala obchodní sdělení obsahově odpovídající dokumentům v příloze. Kontrolovaná osoba ve svých vyjádřeních uvedla, že rozesílku obchodních sdělení pro ni zajišťují externí společnosti, se kterými má řádně uzavřené smlouvy. Společnost EC PROFIT s.r.o. zasílá pouze vyžádané obchodní sdělení pro své klienty, např. potvrzení objednávky či oznámení o expedici zboží z e-shopu. Žádné sdělení uvedené v přílohách zaslaných oznámení o zahájení či rozšíření kontroly, tedy dle tvrzení Kontrolované osoby, nebylo touto osobou zasláno, vše pro ně zajišťují externí agentury. Dále uvedla, že ve smlouvách tyto externí společnosti garantovaly, že k veškerým adresám disponují souhlasem s oslovením obchodních sdělení. K jednotlivým e-mailovým adresám, na které byla obchodní sdělení zaslána a na něž se kontrolující Kontrolované osoby taktéž dotazoval, Kontrolovaná osoba sdělila, že se nejedná o zákazníky či klienty společnosti EC PROFIT s.r.o. Na otázku, která externí společnost pro ně zajišťuje rozesílání obchodních sdělení, Kontrolovaná osoba uvedla dvě společnosti, a to: společnost Beckinsale, s.r.o., se sídlem Bubenská 1477/1 – Holešovice, 170 00 Praha 7, IČO: 247 95 691, jednající panem Nikolayem Todorovem Temelkovem, jednatelem společnosti, a společnost JDI International, s.r.o., se sídlem Újezd 450/40, 118 00 Praha 1, IČO: 292 35 111, jednající panem Nikolayem Vasilevem Todorovem, jednatelem společnosti. Kontrolovaná osoba ve svých odpovědích doložila též kopie příkazní smlouvy uzavřené s těmito společnostmi, dále doložila kopie objednávek služeb direct marketingu dle smlouvy u společnosti Beckinsale, s.r.o., a to na období od 1. července 2015 do 31. července 2015, od 1. srpna 2015 do 1. září 2015. Dále kopie objednávek služeb direct marketingu dle smlouvy u společnosti JDI International, s.r.o., a to na období od 2. září 2015 do 30. září 2015, od 1. října 2015 do 31. října 2015, od 1. listopadu 2015 do 30. listopadu 2015, od 1. prosince 2015 do 31. prosince 2015, od 1. ledna 2016 do 31. ledna 2016, od 1. února 2016 do 29. února 2016. V následujících rozšířeních předmětu kontroly byla Kontrolovaná osoba vždy dotazována ohledně dalších e-mailových adres, na které byla obchodní sdělení zasílána. Odpověď Kontrolované osoby byla vždy totožná, tedy že rozesílku provádějí externí společnosti, a bylo odkazováno na předchozí vyjádření a na přiložené smlouvy. K dotazu, kdo v současné době (březen 2016) provozuje webové stránky www.aaahome.cz a www.iklenot.cz, Kontrolovaná osoba uvedla, že tyto webové stránky provozuje společnost Mayden Corporation, s.r.o., IČO: 04264771, se sídlem Husitská 3, Praha 3 – Žižkov. Tato společnost si pronajímá prostor na webových stránkách od společnosti EC PROFIT s.r.o., která je vlastníkem webových stránek a též domén www.aaahome.cz a www.iklenot.cz.

Z § 7 odst. 1 zákona č. 480/2004 Sb. vyplývá, že obchodní sdělení lze šířit, jen když to zákon povoluje. Z odst. 2 téhož zákona vyplývá, že tímto zákonným povolením je předchozí souhlas uživatele. Je nutno rozhodnout, kdo právně odpovídá za šíření obchodního sdělení. Vzhledem k tomu, že správní delikt podle § 11 odst. 1 je konstruován na základě objektivní odpovědnosti, tedy odpovědnosti za právní stav, lze mít za to, že odesílatelem obchodního sdělení je ten, kdo jeho šíření zadá. V případě této kontroly je to Kontrolovaná osoba, protože uzavřela příkazní smlouvu ze dne 25. srpna 2014 se společností Beckinsale, s.r.o., se sídlem Bubenská 1477/1, Praha 7 – Holešovice, 170 00, IČO: 247 95 691 a příkazní smlouvu ze srpna 2015 se společností JDI International, s.r.o., se sídlem Újezd 450/40, Praha 1 – Malá Strana, 118 00,

IČO: 292 35 111. V těchto smlouvách Kontrolovaná osoba, jakožto příkazce, zadala výše uvedeným společnostem, aby zařídily obchodní záležitost spočívající v realizaci direct marketingové kampaně, zejména zajištění rozesílky obchodních sdělení. Přestože v čl. 2 příkazní smlouvy příkazce uložil příkazníkovi mít souhlas se zasíláním obchodních sdělení, tyto společnosti tento článek porušily, jelikož tento souhlas nezajistily. Kontrolovaná osoba jakožto zadavatel zasílání předmětných obchodních sdělení si měla dostatečně prověřit, jakými souhlasy uvedené společnosti disponují. Nelze spoléhat pouze na ujištění třetí strany, že patřičnými souhlasy disponuje. Z povahy souhlasu se zasíláním obchodních sdělení, jak je výše uvedeno, je patrné, že osoba udělující souhlas musí vědět, k čemu souhlas dává (pro jaký účel, k jakému zasílání obchodních sdělení), jakému subjektu nebo ve prospěch jakého subjektu jí budou obchodní sdělení zasílána, tento souhlas musí být také prokazatelný. Kontrolovaná osoba však uvedené souhlasy neprokázala. Toto porušení smlouvy má toliko soukromoprávní důsledky a z hlediska veřejného práva za toto porušení odpovídá Kontrolovaná osoba, jakožto příkazce. Na okraj lze dodat, že náhradu škody za tento veřejnoprávní delikt lze regresem požadovat po příkazníkovi. Z této právní kvalifikace lze tedy učinit závěr, že společnosti Beckinsale, s.r.o. a JDI International, s.r.o. jednaly jménem Kontrolované osoby a na její účet, a proto se jejich jednání přičítá Kontrolované osobě.

Na základě kontrolních zjištění a této právní kvalifikace měl tak kontrolující za prokázané, že v případě těchto rozesílek je odpovědným subjektem za rozesílání obchodních sdělení Kontrolovaná osoba, jelikož šířila obchodní sdělení prostřednictvím výše uvedených subjektů.

Kontrolující posuzoval též dodržování povinností stanovených zákonem č. 101/2000 Sb. při zpracování osobních údajů zákazníků a dalších osob v souvislosti s obchodní a marketingovou činností společnosti EC PROFIT s.r.o. Z důvodu podezření z možného porušení ustanovení § 5 odst. 2 zákona č. 101/2000 Sb. byla Kontrolovaná osoba v rámci Oznámení o rozšíření předmětu kontroly požádána o doložení souhlasů se zpracováním osobních údajů adresátů obchodních sdělení dle ustanovení § 5 odst. 4 zákona č. 101/2000 Sb. Kontrolovaná osoba však na toto Oznámení o rozšíření předmětu kontroly nijak nereagovala a nebylo tak doloženo, zda v souvislosti se svou marketingovou činností zpracovávala osobní údaje v rozporu ustanovení § 5 odst. 2 zákona č. 101/2000 Sb. a zda disponuje či nedisponuje souhlasy se zpracováním osobních údajů dle § 5 odst. 4 téhož zákona.

Námitky vůči kontrolnímu protokolu kontrolovaným podány nebyly.

Na základě výše uvedených zjištění byla společnosti EC PROFIT s.r.o., uložena sankce ve výši 500.000 Kč.

SCM Financial Insurce Corporation s.r.o. (inspektor Josef Vacula)

V uvedeném případě byla nevyžádaná obchodní sdělení zasílána v období od 25. listopadu 2014 do 20. května 2016. Obchodní sdělení byla odesílána z e-mailových adres info@optimal-mailing.cz, obchod@bestmailing.cz a info@marketingmailing.cz. Podle výpisu z whois databáze k těmto doménovým jménům byly tyto domény v době odesílání obchodních sdělení v držení společnosti SCM Financial Insurce Corporation s.r.o. Ze záznamu na jmenném serveru (DNS) je patrné, že těmto doménám odpovídají konkrétní IP adresy. Tyto IP adresy jsou v adresném rozsahu patřícím společnosti WEDOS Internet, a.s. Společnost WEDOS Internet, a.s. uvedla, že majitelem zákaznického účtu je společnost SCM Financial Insurce Corporation, s.r.o. (dále také „Kontrolovaná osoba" nebo „Kontrolovaný"), IČ: 28301064. Na základě zhodnocení

všech skutečností obsažených ve spisovém materiálu je zřejmé, že odesílatelem předmětných obchodních sdělení byla výše uvedená společnost.

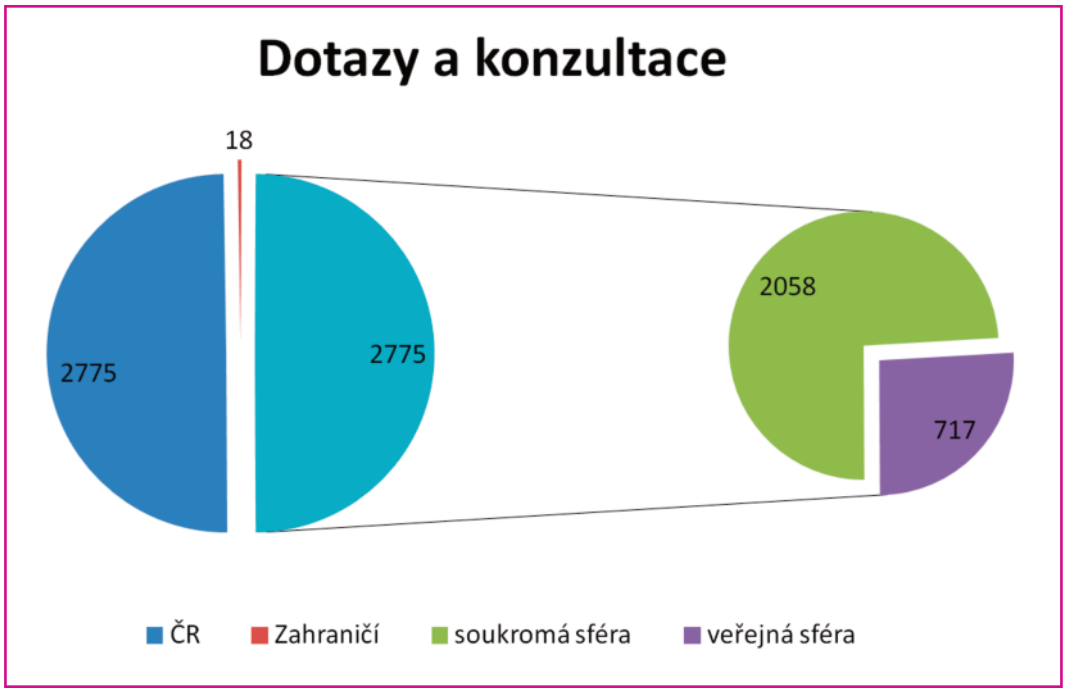
Kontrolující posuzoval, zda jsou splněny podmínky pro zasílání obchodních sdělení uvedené v § 7 zákona č. 480/2004 Sb., především zda je splněna podmínka zasílat obchodní sdělení pouze po předchozím souhlasu adresátů. V Oznámení o zahájení kontroly, Oznámení o rozšíření kontroly a Oznámení o rozšíření kontroly II byla Kontrolovaná osoba vyzvána, aby doložila, zda adresáti e-mailových adres, na které byla obchodní sdělení zasílána, jsou jejími zákazníky nebo aby doložila souhlasy jednotlivých adresátů se zasíláním předmětných obchodních sdělení. Souhlasem se rozumí svobodný, zřejmý a vědomý projev vůle, který učiní adresát vůči odesílateli, aby mu umožnil využívat podrobnosti svého elektronického kontaktu k rozesílání obchodních sdělení. Ze souhlasu musí být patrné, kdo jej poskytuje, komu a pro jaký účel je dáván. Souhlas musí být dán předem (před odesláním obchodního sdělení) a musí být prokazatelný. V případě obchodních sdělení není třeba dokládat, na jakou dobu je souhlas udělen, neboť musí být dána možnost tento souhlas odmítnout v každém zaslaném sdělení. Zákon č. 480/2004 Sb. pro souhlas se zasíláním obchodních sdělení nestanoví povinnou formu, například písemnou. V případě konfliktní situace, kdy adresát obchodního sdělení tvrdí, že mu bylo odesílatelem zasláno obchodní sdělení bez jeho souhlasu, je však důkazní břemeno na straně odesílatele. V tomto případě je odesílatel povinen prokázat, že adresát souhlasil se zasláním obchodního sdělení a že souhlas splňoval všechny výše uvedené náležitosti. Z tohoto vyplývá, že souhlas adresáta musí prokázat odesílatel obchodního sdělení. Souhlas se zasíláním obchodních sdělení je třeba získat předem (pokud nejde o stávajícího zákazníka) a musí být vztažen ke konkrétnímu odesílateli. Kontrolovaná osoba se však k Oznámení o zahájení kontroly nevyjádřila, nevyjádřila se ani ke dvěma rozšířením kontroly, ani k výzvám, které jí byly zaslány. Na základě kontrolních zjištění týkajících se především domén, ze kterých byla obchodní sdělení odesílána a ze shodných tvrzení stěžovatelů (kteří uváděli, že souhlas se zasíláním obchodních sdělení odesílateli neposkytli, nejsou jeho zákazníky ani registrovanými uživateli) a na základě toho, že Kontrolovaná osoba nedoložila a neprokázala, že na předmětné e-mailové adresy byla obchodní sdělení zaslána po předchozím souhlasu adresátů, nebo že by byli adresáti jeho zákazníky, měl kontrolující za prokázané, že Kontrolovaná osoba tím, že z adres info@optimalmailing.cz, obchod@bestmailing.cz a info@marketingmailing.cz zaslala obchodní sdělení týkající se nabídky databáze, ve které se nachází 400.000 ks e-mailových adres na fyzické osoby z celé České republiky, porušila povinnosti stanovené v § 7 odst. 1 a 2 zákona č. 480/2004 Sb., tedy šířit obchodní sdělení elektronickými prostředky jen za podmínek stanovených tímto zákonem, tedy pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.

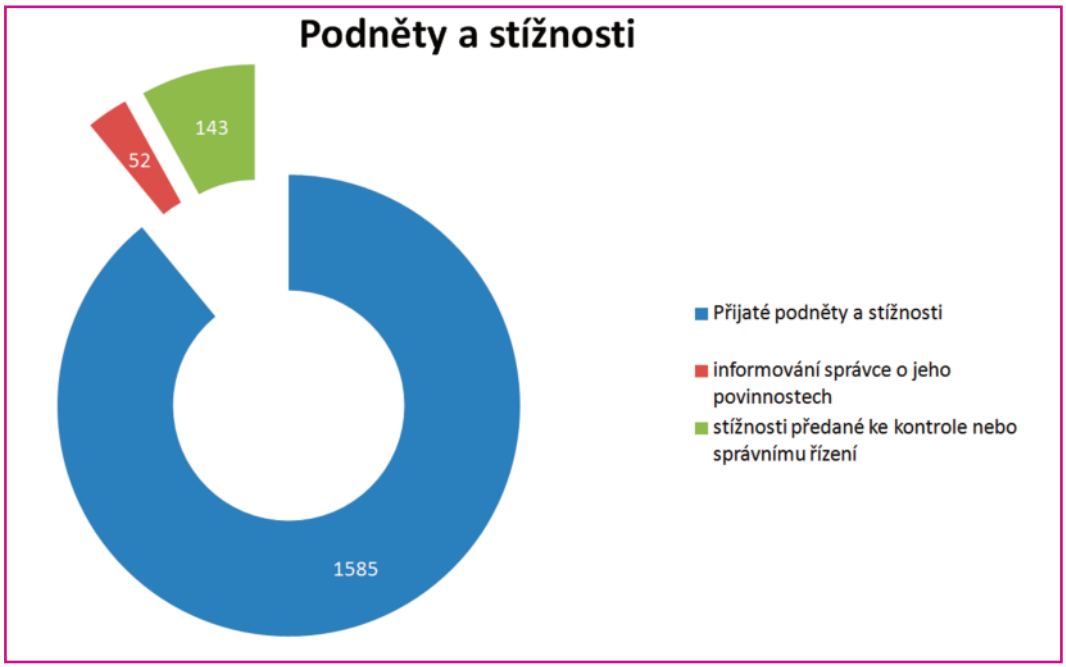
Námitky vůči kontrolnímu protokolu Kontrolovaným podány nebyly. K této věci je třeba uvést, že za neposkytování součinnosti (nereagování na Oznámení o zahájení kontroly, rozšíření kontroly ani výzvy) byla této společnosti uložena též pokuta podle § 16 odst. 1 kontrolního řádu, a to ve výši 100.000 Kč.

Na toto kontrolní řízení navazovalo příslušné řízení správní, které bylo s účastníkem řízení zahájeno Oznámením, ve kterém byl účastník řízení vyzván, aby se vyjádřil i k dalším stížnostem, jež Úřad obdržel po provedené kontrole. Nutno podotknout, že i v průběhu celého správního řízení byla obchodní sdělení neustále zasílána a stížnosti na tyto nevyžádané zprávy byly podávány. V rámci správního řízení byl účastník řízení vyzván k vyjádření se k předmětnému zasílání celkem 3×. Ani na jednu výzvu opět nikterak nereagoval, ačkoli mu byla veškerá oznámení

řádně doručována prostřednictvím datové schránky. Vzhledem ke skutečnosti, že ani v rámci správního řízení účastník řízení důkazní břemeno, které spočívalo v tom, zda byl dán souhlas k zasílání obchodních sdělení, neunesl, má správní orgán za prokázané, že účastník řízení porušil výše popsaným jednáním povinnosti stanovené v § 7 odst. 2 zákona č. 480/2004 Sb., a tím spáchal správní delikt podle § 11 odst. 1 písm. a), neboť opakovaně šířil obchodní sdělení bez souhlasu adresátů. Při stanovení výše sankce bylo jako ke skutečnosti zvyšující závažnost jednání účastníka řízení přihlédnuto z hlediska intenzity správního deliktu k tomu, že k rozesílání nevyžádaných obchodních sdělení docházelo v delším časovém období a dále k množství adresátů obchodních sdělení. Správní orgán za přitěžující skutkovou okolnost považuje skutečnost, že obchodní sdělení byla zasílána opakovaně i jednotlivým jejich adresátům a v pěti případech byla obchodní sdělení zasílána dokonce po výslovném prokazatelném odmítnutí dalšího zasílání obchodních sdělení. Za přitěžující okolnost je třeba považovat také to, že pro odesílání nevyžádaných obchodních sdělení bylo použito více e-mailových adres, což pro adresáty znamenalo více potíží při blokování odesílacích adres. Další přitěžující okolností, ke které správní orgán při stanovení výše sankce přihlédl, byla skutečnost, že rozesílání obchodních sdělení je součástí předmětu podnikatelské činnosti účastníka řízení, a tím spíš by měl účastník řízení dodržovat příslušné právní předpisy. Po souhrnném zhodnocení všech okolností uložil správní orgán sankci ve výši 300.000 Kč. Rozhodnutí nabylo právní moci a dne 16. září 2016 též vykonatelnosti. Sankce nebyla doposud zaplacena, proto Úřad postoupil podklady k vymáhání pokuty Celnímu úřadu pro hlavní město Prahu.

Ostatní dozorová činnost





• STÍŽNOSTNÍ A KONZULTAČNÍ AGENDA

V průběhu roku vstoupila v účinnost změna právní úpravy některých zákonů dotýkajících se zpracování osobních údajů, což se významně promítlo jak ve spektru obdržených dotazů, tak ve způsobu posuzování a vyhodnocování obdržených stížností a podnětů odborem pro styk s veřejností, který v rámci působnosti Úřadu dle § 29 odst. 1 písm. c) a h) zákona č. 101/2000 Sb. vyhodnocuje a určuje postupy u přijatých stížností a podnětů a správcům, subjektům údajů a dalším zainteresovaným subjektům poskytuje písemné, telefonické a osobní konzultace.

V prvé řadě lze jmenovat novelu zákona č. 634/1992 Sb., o ochraně spotřebitele, která v ustanovení § 20z institucionalizuje informační databáze o bonitě a důvěryhodnosti spotřebitele. Jde tak o zcela novou právní úpravu „dlužnických registrů", dříve právně de facto neupravených (kromě tzv. bankovního registru v § 38a zákona č. 21/1992 Sb., o bankách), které nově mohou bez souhlasu subjektu údajů zpracovávat osobní údaje pro účely ochrany práv a právem chráněných zájmů prodávajících a spotřebitelů za současného dodržování zákonem o ochraně spotřebitele definovaných podmínek a povinností. Role odboru pro styk s veřejností tak v tomto směru byla zejména vzdělávací, kdy tazatele a stěžovatele informoval o této nové právní úpravě a tuto novou právní úpravu zohledňoval i při vyřizování stížností a konzultací.

Dalším právním předpisem, který ovlivnil konzultační a stížnostní činnost, byl zákon č. 112/2016 Sb., o evidenci tržeb, v jehož souvislosti zaznamenal Úřad zvýšenou nespokojenost podnikajících fyzických osob se zpřístupňováním jejich rodných čísel v důsledku uvádění tohoto údaje jako součásti daňového identifikačního čísla na účtence. Dle ustanovení § 20 odst.1 písm. b) zákona č. 112/2016 Sb. je poplatník povinen uvádět své daňové identifikační číslo na účtence, vydávané tomu, od koho evidovaná tržba plyne. Tedy každému zákazníkovi, který může s účtenkou jako dokumentem dále disponovat. Konstrukce daňového identifikačního čísla na základě rodného čísla je stanovena v § 130 odst. 3 zákona č. 280/2009 Sb., daňový řád.

Dalším právním předpisem, který ovlivnil především konzultační činnost, byl zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Předmětem konzultací spojených s tímto zákonem byl zejména rozsah osobních údajů zveřejňovaných ke splnění povinnosti uveřejňovat dokumenty stanovené zákonem o registru smluv.

Činnost odboru pro styk s veřejností v konzultační a stížnostní agendě však nebyla ovlivněna pouze na základě změn zákonné úpravy, ale i na základě úpravy názorů Úřadu, vyjadřovaných formou stanovisek.

Od počátku roku 2016, v souvislosti s vydáním stanoviska Úřadu č. 1/2016 Umístění kamerových systémů v bytových domech, byla v rámci konzultační agendy vysvětlována změna přístupu Úřadu k problematice kamerových záznamů v bytových domech, jejímž cílem bylo umožnit využití těchto záznamů k legitimnímu účelu ochrany života, zdraví a majetku, za současného důsledného dodržení povinností vyplývajících ze zákona č. 101/2000 Sb. tak, aby pořizované záznamy nemohly být zneužívány k soustavnému sledování osob, zejména obyvatel domu, kde byl kamerový záznam instalován. Změna stanoviska ovlivnila i posuzování přijatých podnětů a stížností na kamerové systémy v bytových domech.

Problematika kamer v bytových domech však tvoří pouze část z celkového množství dotazů a stížností na kamerové systémy. Dalšími oblastmi jsou kamerové systémy na veřejném prostranství, ve vozidlech a v neposlední řadě i na pracovištích, kde však mohou s ohledem na zákon č. 262/2006 Sb., zákoník práce, uplatnit působnost zejména orgány inspekce práce.

Tenké hranice mezi právem na informace a právem na ochranu soukromí se střetávají i ve stížnostní a konzultační agendě, ve které Úřad řeší dotazy na vztah zákona o ochraně osobních údajů a zákona o svobodném přístupu k informacím při poskytování informací o fyzických osobách povinnými subjekty podle zákona o svobodném přístupu k informacím i možnosti dalšího nakládání s osobními údaji získanými žadatelem v postavení příjemce osobních údajů. Stížnostní agendy se často dotýkají podněty na zveřejnění adresních údajů žadatelů o informaci, přičemž odborem pro styk s veřejností bylo v těchto případech, zejména pokud šlo např. o malou obec bez dostatečného právního vědomí a nejednalo se o velký rozsah zveřejnění, přikračováno k informování povinného subjektu o nemožnosti zveřejňovat identifikační údaje tazatele a v drtivé většině případů došlo k rychlé a efektivní nápravě ke spokojenosti stěžovatele.

Uvedený postup odpovídá možnosti, která vyplývá od 1. ledna 2016 z organizačního řádu, který umožňuje odboru pro styk s veřejností ve vhodných případech informovat správce o jeho zákonných povinnostech. Tento postup odbor pro styk s veřejností využíval, pokud se jednalo o bagatelní porušení zákona č. 101/2000 Sb., resp. mírnou nevědomost správce. Na základě informativních dopisů došlo v desítkách případů k rychlé a efektivní nápravě ve prospěch subjektů údajů bez nutnosti formálního trestání ve správním řízení či započetí kontrolního procesu.

Trendu elektronizace státní správy se odbor pro styk s veřejností snažil vyhovět zejména aktualizací a doplněním odpovědí na často kladené otázky, tvořících samostatnou rubriku na webových stránkách Úřadu, které umožňují poskytnout rychlou informaci pro návštěvníky stránek a odstraňují v některých případech nutnost dotazovat se Úřadu. Zároveň byl vydán soubor návodů pro řešení problémů s osobními údaji na internetu a byly odborem pro styk s veřejností pro zvýšení informativnosti veřejnosti publikovány články na aktuální témata.

Nastupujícím trendem ke konci roku byl vzrůstající počet dotazů na Obecné nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, které sice nabude účinnosti až 25. května 2018, avšak především správci již započali zjišťovat informace, jaké nové povinnosti bude pro ně nařízení představovat, tak, aby mohli zpracování osobních údajů uzpůsobit novým povinnostem. Vzhledem k tomu, že konkrétní podoba některých postupů je i na celo-evropské úrovni v přípravné fázi, mohla být na některé dotazy poskytnuta pouze rámcová odpověď.

Tématy desítek osobních konzultací poskytnutých v budově Úřadu správcům osobních údajů z řad veřejné správy i soukromoprávním subjektům byly např. zpracování osobních údajů účastníků přijímacího řízení na vysokých školách, možnosti využívání cloudových služeb při uchovávání citlivých údajů o zdravotním stavu, zpracování osobních údajů v rámci činnosti politické strany nebo hnutí, evidence oprávněných přístupů k Registru pro léčivé přípravky s omezením, záměr vytvoření tzv. Centrálního registru Robinsonů za účelem vyloučení obtěžujících volání účastníky služeb elektronických komunikací, využití GPS pro optimalizaci trasy poštovních doručovatelů, projekt zaměstnanecké karty pro cizince, elektronické odbavení cestujících v hromadné dopravě, předávání osobních údajů do třetích zemí v souvislosti s činností banky.

Veřejností oceňované osobní konzultace, okamžitě při příchodu poskytované v prostorách Úřadu pracovníky odboru pro styk s veřejností, se týkaly zejména provozování kamerových

systémů na veřejnosti, v bytových domech a k možnosti ochrany vlastní nemovitosti kamerovým systémem a dále stovek různorodých případů, které problematika zpracování a ochrany osobních údajů v životě přináší.

• POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

Úřad uložil v roce 2016 pokuty za správní delikty a přestupky v souhrnné výši 7 458 000 Kč, z toho za nevyžádaná obchodní sdělení 1 320 000 Kč.

Společnost T-Mobile Czech Republic a.s. – nedostatečné zabezpečení osobních údajů zákazníků

V roce 2016 bylo předmětem správního řízení vedeného Úřadem, posuzováno z hlediska výše uložené sankce, zatím nejzávažnější protiprávní jednání, za které uložil pokutu ve výši 3,6 milionů Kč.

Předmětem tohoto řízení byla skutečnost, že při zpracování osobních údajů svých zákazníků společnost T-Mobile Czech Republic a.s. (dále také „účastník řízení") nezajistila, aby nedošlo k úniku osobních údajů těchto fyzických osob, a to v rozsahu jméno, příjmení, datum narození, adresa, telefonní číslo, kód zákazníka, tarif, název, kategorie a značka zařízení, údaj o průměrné útratě, platební metodě, popř. čísle účtu a kódu banky. Dle zjištění Úřadu došlo k tomuto úniku a ohrožení dat vzhledem k nepřijetí dostatečných opatření k zabezpečení osobních údajů obsažených v elektronické interní databázi společnosti T-Mobile Czech Republic a.s., jehož důsledkem bylo odcizení dat zákazníků z uvedené databáze zaměstnancem dané společnosti, který měl oprávněný přístup do systému a s daty pracoval.

Správní řízení bylo zahájeno na základě oznámení účastníka řízení v dané věci, které zaslal Úřadu dne 13. června 2016, ve spojení s informacemi publikovanými ve veřejných sdělovacích prostředcích téhož dne. V době zahájení správního řízení byl již případ vyšetřován Policií České republiky, a to na základě trestního oznámení učiněného účastníkem řízení.

Z tiskové zprávy zveřejněné účastníkem řízení dne 13. června 2016 označené „T-Mobile – vyjádření k úniku dat" vyplývá mj., že účastník řízení k věci uvedl, že jeden z jeho zaměstnanců (člen malého týmu, který se zákaznickými daty běžně pracoval) se pokusil odcizit a následně prodat zákaznická data. Dále účastník řízení uvedl, že ihned po zjištění podezření na trestnou činnost podnikl všechny nutné kroky v součinnosti s Policií České republiky. K tomu doplnil, že danému zaměstnanci byl bez prodlení zrušen pracovní poměr a bylo zahájeno vyšetřování orgány činnými v trestním řízení. Dále pak zdůraznil, že jde o případ selhání jednotlivce, nikoli o systémovou či procesní chybu.

Ze spisového materiálu vyplynulo, že předmětná interní databáze obsahovala ke dni 30. června 2016 osobní údaje 1 193 497 zákazníků (fyzických osob), přičemž účastník řízení nezajistil, aby nedošlo k ohrožení těchto osobních údajů obsažených v předmětné databázi.

Účastník řízení jako správce osobních údajů odpovídá za dodržování povinností stanovených pro jejich zpracování zákonem č. 101/2000 Sb. Mezi uvedené povinnosti náleží mj. povinnost stanovená v § 13 odst. 1 uvedeného zákona, tedy přijmout taková opatření, 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.

Povinnost dle § 13 odst. 1 zákona č. 101/2000 Sb. a této povinnosti odpovídající skutková podstata správního deliktu je přitom formulována jako odpovědnost za následek. Dojde-li tedy k následku předvídanému v § 13 odst. 1 zákona č. 101/2000 Sb. (neoprávněnému přístupu k osobním údajům apod.), což je v této věci nepochybné, znamená to, že se správce osobních údajů dopustil také správního deliktu.

Obecně lze konstatovat, že skutková podstata správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. je naplněna již v situaci, kdy zpracovávaným osobním údajům hrozí (v důsledku nepřijetí či neprovedení dostatečných organizačních a technických opatření) riziko nesprávného či neoprávněného zpracování. V případě, kdy jsou osobní údaje bez jakéhokoli právního titulu již zpřístupněny třetím osobám (v daném případě byly nabídnuty, včetně jejich vzorku, ke koupi třetímu subjektu), nelze o naplnění uvedené skutkové podstaty pochybovat.

V této souvislosti považoval Úřad za významnou skutečnost, že reakci účastníka řízení na zjištěné neobvyklé chování uživatele databáze nelze posoudit v daném případě jako dostatečnou ani včasnou. Včasnost totiž v tomto případě nelze dle názoru Úřadu odvíjet od okamžiku, kdy se účastník řízení o úniku dozvěděl v daném případě od spolupracující agentury.

Dle zjištění Úřadu měl účastník řízení přijata opatření k zabezpečení osobních údajů klientů, která však nebyla dostatečná. V důsledku toho měly osoby s oprávněným přístupem do informačního systému a k osobním údajům zákazníků bez dalšího možnost kopírovat data zákazníků na datové nosiče, popř. v omezeném rozsahu rovněž posílat prostřednictvím e-mailových zpráv. Účastník řízení uvedl, že bezpečnostní incident nenastal v důsledku nedostatečných technicko-organizačních opatření, případně jejich selhání, ale v důsledku protiprávního excesivního chování jedince, nicméně dle názoru Úřadu příčinou, že k bezpečnostnímu incidentu a k ohrožení osobních údajů došlo, byla skutečnost, že nedostatečným způsobem zabezpečil ochranu osobních údajů obsažených v uvedené databázi. V důsledku nedostatečného zabezpečení osobních údajů bylo možné a proveditelné odcizení osobních údajů zákazníků z interní databáze zaměstnancem, který byl oprávněn k přístupu k osobním údajům zákazníků vedeným v elektronické interní databázi.

Účastníkem řízení byly předloženy vnitřní předpisy přijaté ve vztahu k zabezpečení ochrany osobních údajů zákazníků, které se zaměřovaly na ochranu osobních údajů před jejich získáním neoprávněnými uživateli. Předmětné vnitřní předpisy upravovaly základní oprávnění a povinnosti ve vztahu k zabezpečení informací obsažených v informačních systémech a databázích včetně přístupových oprávnění. Daná pravidla se týkala především zamezení přístupu neoprávněných osob do informačních systémů, popř. zamezení přístupu zaměstnanců, kteří nepotřebují informace nezbytně nutně k výkonu práce (řízení přístupu k citlivým informacím). Účastník řízení však nedoložil žádný dokument, vnitřní předpis, ani nedoložil přijetí opatření, která by byla schopna účinným způsobem zamezit osobě oprávněné k přístupu k osobním údajům zákazníků v neoprávněném ukládání takovýchto údajů na externí média, popř. jejich zaslání e-mailem.

Odpovědnost za správní delikt je postavena na objektivní odpovědnosti (tedy bez ohledu na zavinění), přičemž zákon č. 101/2000 Sb. upravuje v § 46 odst. 1 liberační důvod, jehož naplněním se pachatel správního deliktu může odpovědnosti zprostit. Účastník řízení tedy za správní delikt neodpovídá, jestliže prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil (důkazní břemeno spočívá na účastníku řízení, tj. k prokázání liberace musí navrhovat důkazy). Za vynaložení veškerého úsilí, které bylo možno požadovat, nelze považovat jakékoliv úsilí, které správce vynaloží, ale musí se ve vztahu ke každému,

konkrétně posuzovanému případu jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit (zákon používá kritérium veškeré úsilí, které bylo možno požadovat, a nikoliv např. spravedlivě požadovat, požadovat s ohledem na poměry atp.).

Dle názoru Úřadu nebylo možné v daném případě aplikovat liberační ustanovení (§ 46 odst.1 zákona č. 101/2000 Sb.), jelikož ze strany účastníka řízení se nejednalo o vynaložení maximálně možného úsilí k ochraně osobních údajů, tj. zabránění porušení jeho právní povinnosti spočívající v zabezpečení zpracovávaných údajů (vnitřní předpisy přijaté účastníkem řízení, stanovení přístupových práv k osobním údajům zákazníků a do systému účastníka řízení včetně vymezení pravidel pro export dat na externí média zaměstnanci účastníka řízení, nelze považovat v daném případě za dostatečné). Vyústěním uvedených skutečností pak bylo ohrožení osobních údajů zákazníků účastníka řízení, které byly následně odcizeny jeho zaměstnancem.

Z vyjádření zaslaných účastníkem řízení vyplývá, že z jeho strany byla přijata dodatečná nápravná opatření, která mají zamezit dalšímu úniku osobních údajů (a to i přes tvrzení účastníka řízení, že neshledal v daném případě selhání jeho systémů či interních technicko-organizačních bezpečnostních mechanismů a že se jednalo o typický případ selhání jednotlivce), což významně podpořilo závěr Úřadu týkající se neaplikovatelnosti liberačního ustanovení.

Podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. se právnická osoba jako správce dopustí správního deliktu tím, že při zpracování osobních údajů nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů.

Vzhledem k tomu, že účastník řízení svým jednáním při zpracování osobních údajů ohrozil větší počet osob (svých zákazníků) neoprávněným zasahováním do jejich soukromého a osobního života v souvislosti s přijetím nedostatečných opatření k zabezpečení jejich osobních údajů, naplnil výše popsaným jednáním rovněž kvalifikovanou skutkovou podstatu správního deliktu podle § 45 odst. 2 písm. a) zákona č. 101/2000 Sb. Dle uvedeného ustanovení se právnická osoba jako správce nebo zpracovatel osobních údajů dopustí správního deliktu tím, že při zpracování osobních údajů některým ze způsobů podle § 45 odst. 1 téhož zákona ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života. Ze shromážděného spisového materiálu bylo přitom patrné, že došlo k ohrožení osobních údajů v databázi účastníka řízení, která v době, kdy došlo k incidentu vyvolanému zaměstnancem účastníka řízení, obsahovala údaje více než jednoho milionu zákazníků – fyzických osob.

Jako k přitěžujícím okolnostem při určení výše sankce přihlédl Úřad v souladu s § 46 odst. 2 zákona č. 101/2000 Sb. k rozsahu osobních údajů, které byly protiprávním jednáním účastníka řízení ohroženy. Úřad zohlednil skutečnost, že v případě, pokud by daný rozsah údajů skutečně získaly k volné dispozici třetí subjekty, mohli být lidé, o jejichž osobní údaje se jednalo, vystaveni velmi obtěžujícím situacím spočívajícím s největší pravděpodobností v opakovaném obtěžování nabídkami zboží či služeb. Nelze však vyloučit ani závažné zneužití těchto osobních údajů například pro uzavření různého typu smluv bez vědomí dotčených subjektů údajů.

Jako polehčující okolnosti posoudil Úřad okolnosti protiprávního jednání, a to přijetí nápravných opatření účastníkem řízení k zabránění opakování dané situace (provedení kontroly systému a nastavených procesů a přijetí opatření k zajištění dodatečné nápravy závadného stavu, tj. omezení zápisu zákaznických dat na externí média zaměstnanci, opětovné proškolení zaměstnanců), množství a charakter přijatých opatření k zabezpečení zpracovávaných osobních údajů, ačkoliv nebyla dostatečná a ve svém důsledku nezabránila odcizení osobních údajů, a skutečnost, že ztráta dispozice nad předmětnými údaji byla přímým následkem trestné činnosti zaměstnance účastníka řízení.

Vzhledem k výše uvedenému dospěl správní orgán v dané věci k závěru, že společnost T-Mobile Czech Republic a.s. porušila povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., čímž spáchala správní delikt podle § 45 odst. 1 písm. h) a odst. 2 písm. a) zákona č. 101/2000 Sb., neboť nepřijala opatření pro zajištění bezpečnosti zpracování osobních údajů, a při zpracování osobních údajů ohrozila větší počet osob svým neoprávněným zasahováním do soukromého a osobního života.

• POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

Soudnímu přezkumu bylo v roce 2016, ostatně tak jako v předchozích letech, předloženo větší množství rozhodnutí Úřadu. Nicméně v roce 2016 bylo vyhlášeno jen několik rozsudků, a řada rozhodnutí Úřadu proto na soudní přezkum stále čeká. Pokud jde o konkrétní poznatky z předmětné soudní praxe za rok 2016, lze poukázat na následující rozsudky, týkající se zejména zveřejňování osobních údajů prostřednictvím internetu, provozování kamerových systémů a některých procesních záležitostí:

1. Účelem provozování kamerového systému při ochraně majetku je pouze shromáždění údajů pro jejich eventuální předání zákonem k tomu určeným orgánům k dalším úkonům, nikoliv jejich budoucí zveřejnění. Vyšetřování a postihování trestné činnosti, do něhož lze zahrnout i páchání přestupků, je plně v kompetenci orgánů státu. Právo na ochranu majetku by mělo být realizováno prostřednictvím předání získaných údajů Policii ČR.
   Zveřejnění takto získaných údajů na sociální síti, a to bez ohledu na skutečnost, zda by tento postup posléze vedl k odhalení pachatele či nikoli, je již překročením vymezené hranice.

Nejvyšší správní soud svým rozsudkem č.j. 3 As 118/2015 ze dne 8. června 2016 na základě kasační stížnosti podané Úřadem zrušil rozsudek Městského soudu v Praze č.j. 11A 77/2012-38 ze dne 19. května 2015. Uvedený rozsudek Městského soudu v Praze pak zrušil předchozí rozhodnutí Úřadu, kterými byla provozovateli kamerového systému uložena pokuta v celkové výši 5.000 Kč za dva správní delikty – neoznámení záměru zpracovávat osobní údaje prostřednictvím kamerového systému a dále za zpracovávání osobních údajů v rozporu s účelem, k němuž byly shromážděny. Druhý delikt měl spočívat v tom, že provozovatel kamerového systému zveřejnil na sociální síti Facebook fotografii z kamery zachycující osobu podezřelou z krádeže, aniž k tomu měl její souhlas a aniž by tento postup za této situace umožňoval zákon. Právě spáchání tohoto druhého deliktu bylo předmětem sporu.

Městský soud v Praze po provedeném testu proporcionality dospěl ve svém rozsudku k závěru, že jednání provozovatele kamerového systému nebylo možno sankcionovat, neboť jeho zájem na ochraně majetku v daném případě převýšil zájem na ochraně osobních údajů pachatele krádeže zachyceného kamerovým systémem. Nejvyšší správní soud při posouzení právní otázky, zda došlo k neoprávněnému nakládání s osobními údaji, dal ovšem za pravdu názoru Úřadu. Nezpochybnil přitom právo na ochranu majetku prostřednictvím kamerového systému, neztotožnil se však s dalším postupem provozovatele kamerového systému ve věci. Nejvyšší správní soud totiž konstatoval, že účelem provozování kamerového systému při ochraně majetku je pouze shromáždění údajů pro jejich eventuální předání zákonem k tomu určeným orgánům

k dalším úkonům, nikoliv jejich budoucí zveřejnění. Vyšetřování a postihování trestné činnosti, do něhož lze zahrnout i páchání přestupků, je přitom plně v kompetenci orgánů státu. V daném případě tedy mělo být právo na ochranu majetku realizováno prostřednictvím předání získaných údajů Policii ČR a překročením vymezené hranice již bylo zveřejnění takto získaných údajů na sociální síti, a to bez ohledu na skutečnost, zda tento postup posléze vedl k odhalení pachatele či nikoliv.

Dle názoru Nejvyššího správního soudu nelze na věc uplatnit výjimku zakotvenou v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., neboť počínání provozovatele kamerového systému ve výše popsaném rozsahu nebylo nezbytné pro ochranu jeho práv nebo právem chráněných zájmů. V daném případě tak došlo ke zpracování osobních údajů v rozporu s účelem, ke kterému byly shromážděny, tedy k porušení ustanovení § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. a naplnění skutkové podstaty správního deliktu podle tohoto zákona. Za této situace nebyl dán žádný prostor pro test proporcionality, tak jak ho provedl Městský soud v Praze. Právo na ochranu majetku bylo dostatečně saturováno právem provozovatele kamerového systému na instalaci a používání kamerového systému za zákonem stanovených podmínek a na případné další použití údajů získaných snímáním sledovaného prostoru státními orgány k tomu určenými. Jakékoliv další nakládání s osobními údaji takto shromážděnými bez souhlasu dotčených subjektů nelze ničím odůvodnit.

Nejvyšší správní soud ve svém rozsudku vytkl Městskému soudu v Praze také nejasnou formulaci jeho právního názoru ohledně posouzení skutku jako správního deliktu.

2. Kamerový systém neslouží zaměstnavatelům pouze k ochraně majetku a kontrole zaměstnanců, nýbrž především k ochraně zaměstnanců.

V rozsudku čj. 5A 107/2013-38 ze dne 18. října 2016 se Městský soud v Praze zabýval aplikací ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. ve spojení s ustanovením § 316 odst. 2 zákoníku práce. Jednalo se o případ, kdy zaměstnavatel (provozovatel autobusové dopravy) zpracovával osobní údaje prostřednictvím jedné stacionární kamery instalované uvnitř přední části autobusu, zabírající jeho zaměstnance, řidiče a stewarda.

Soud se zcela ztotožnil s testem proporcionality provedeným Úřadem, kdy byly poměřovány zájmy zaměstnavatele, tj. ochrana jeho majetku a života a zdraví zaměstnanců a cestujících a na druhé straně právo zaměstnanců na ochranu jejich soukromí na pracovišti. Ze zásady přiměřenosti využívání kamerového systému vyplývá jeho podpůrné využití pro zpracování osobních údajů, tj. kamerové systémy lze využít pouze, pokud se jiná opatření směřující k prevenci, ochraně anebo zabezpečení nevyžadující pořizování obrazových záznamů ukážou být nedostatečnými či nepoužitelnými. Při dopravních nehodách však lze k důkazu použít materiál z již nainstalovaných kamer, umístěných po stranách autobusu, před autobusem a taktéž svědectví cestujících.

Městský soud v Praze měl dále shodně s Úřadem za to, že nepřetržitým monitorováním prostoru kabiny řidiče nelze přispět k ochraně zdraví zaměstnanců či zvýšení bezpečnosti cestujících, jelikož samo o sobě žádnému závadnému jednání nezabrání. Zároveň soud považoval za důležité zopakovat názor Úřadu, že u některých osob by se vlivem neustálého snímání kamerami mohl vytvořit velký a nezvladatelný tlak, který by byl ve svém důsledku kontraproduktivní, neboť by mohl vést ke zcela opačnému než zamýšlenému účelu ochrany majetku, zdraví, životů osob a bezpečnosti silničního provozu. Za přijatelnou formu monitoringu pokládá soud snímání prostoru kabiny řidiče pouze po dobu, kdy v něm dochází k nakládání s finanční

hotovostí. Ve shodě s Úřadem pak soud konstatoval, že výše uvedený způsob zpracovávání osobních údajů zaměstnavatelem nesplňuje zákonem stanovené podmínky uvedené v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Rozsudek čj. 5A 107/2013-38 ze dne 18. října 2016 však byl ze strany provozovatele autobusové dopravy napaden kasační stížností.

3. Úřad pro ochranu osobních údajů je oprávněn přezkoumávat v rámci své dozorové pravomoci postup při zpracovávání osobních údajů při plnění povinnosti podle zákona o svobodném přístupu k informacím. Ustanovení § 8b zákona č.106/1999 Sb. zásadně nedává prostor pro úvahu, zda na základě principu proporcionality informace o příjemcích veřejných prostředků poskytnout, neboť toto řeší již samotné ustanovení § 8b odst. 3 zákona č.106/1999 Sb.

Městský soud v Praze ve svém rozsudku čj. 10A 147/2013-72 ze dne 27. září 2016 při posuzování vztahu ustanovení § 8b zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a ustanovení § 5 odst. 1 písm. f) a § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. dal za pravdu Úřadu ohledně oprávněnosti jeho přezkumu postupu u zpracovávání osobních údajů při plnění povinnosti podle zákona o svobodném přístupu k informacím v rámci dozorové činnosti dle § 29 zákona č. 101/2000 Sb. Úřad je, dle názoru soudu, oprávněn učinit si úsudek o tom, zda došlo k naplnění dispozice ustanovení § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. Poskytnutí informací podle § 8b zákona č. 106/1999 Sb. představuje splnění právní povinnosti podle tohoto zákona. Pouze oprávněné poskytnutí takové informace však naplní dispozici ustanovení § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. Úřad proto musí být oprávněn učinit si úsudek o tom, zda plnění informační povinnosti žalobce podle § 8b zákona č. 106/1999 Sb. nevybočilo z limitů nastavených tímto ustanovením.

Co se týká merita věci, soud posuzoval případ, kdy Úřad uložil pokutu ve výši 100.000 Kč orgánu státu za zveřejnění jmen, příjmení a hrubých příjmů jeho zaměstnanců, neboť postup státního orgánu při zpracování osobních údajů na základě ustanovení § 8b zákona č. 106/1999 Sb. shledal v rozporu s právem dotčených subjektů na soukromí. V rozhodnutích Úřadu byl vysloven závěr, že bylo povinností státního orgánu před poskytnutím a následným zveřejněním osobních údajů svých zaměstnanců provést test proporcionality ve vztahu k jednotlivým zaměstnancům a teprve na tomto základě dojít k závěru, zda poskytnutí informace je či není v případě konkrétního zaměstnance v rozporu s jeho právem na soukromí, i s odkazem na evropskou judikaturu. Úřad v této souvislosti též upozornil, že při zveřejňování, resp. poskytování informací, které mají charakter osobních údajů, je třeba hodnotit, zda platná právní úprava obstojí ve vztahu k právu na soukromí dle čl. 8 Evropské úmluvy o ochraně lidských práv a svobod (dále „EÚLP"), tedy zda zásah do práva na soukromí (příjemců veřejných prostředků) je v souladu se zákonem a nezbytný v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných. Současně je třeba přihlédnout k tomu, zda odepření takové informace není omezením práva na svobodu projevu (práva vyhledávat informace) dle čl. 10 EÚLP.

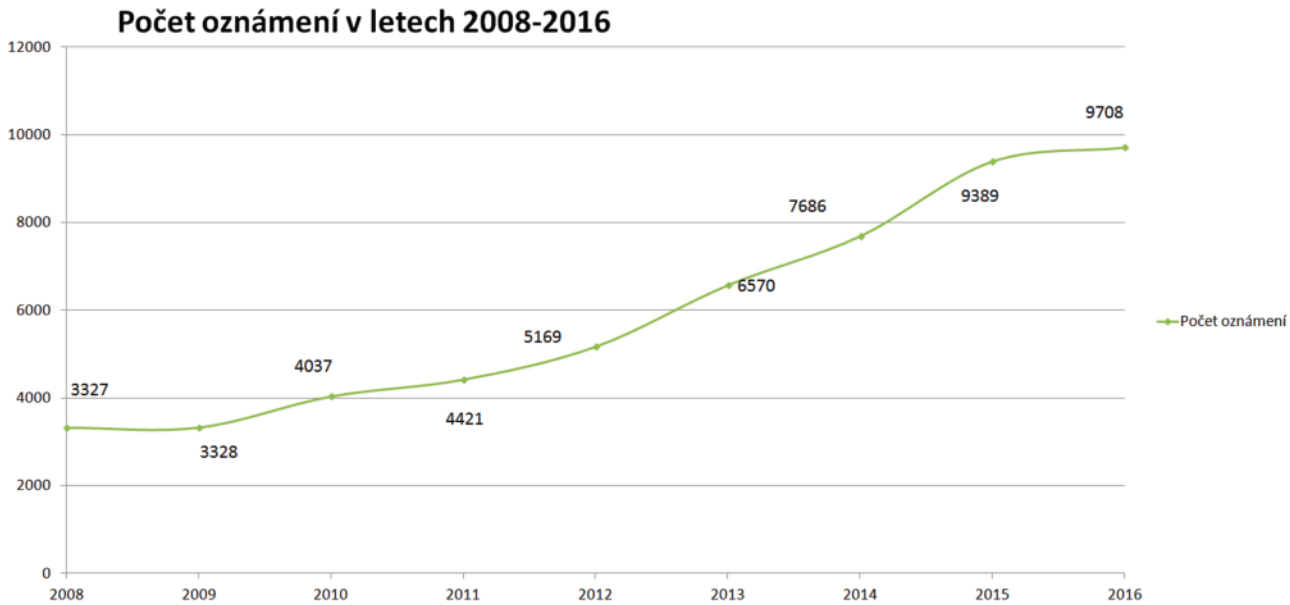
Dle názoru Úřadu je ustanovení § 8b zákona č. 106/1999 Sb. v rozporu s ústavním pořádkem České republiky. Protiústavnost citovaného ustanovení spatřuje Úřad v tom, že nijak nerozlišuje mezi příjemci veřejných prostředků, ačkoliv v době, kdy jsou ročně veřejné prostředky přerozdělovány v míře blížící se 50 % HDP, je zřejmé, že je nutné mezi jednotlivými situacemi rozlišovat.

Dle Úřadu je přitom zjevné, že na základě tohoto ustanovení dochází k zásahu do práva na soukromí a informační sebeurčení osob, tedy do práva garantovaného čl. 10 Listiny základních práv a svobod, neboť jsou třetím osobám poskytovány, resp. zveřejňovány, informace týkající se osobních a majetkových poměrů příjemců veřejných prostředků. Uvedené ustanovení přitom není dostatečně určité ani předvídatelné v otázce vymezení příjemce veřejných prostředků, resp. situace, kdy je zde legitimní zájem veřejnosti o informace a kdy převáží právo na soukromí. Z výše uvedeného důvodu Úřad navrhl, aby Městský soud v Praze podle článku 95 odst. 2 Ústavy podal Ústavnímu soudu ČR návrh na zrušení ustanovení § 8b zákona č. 106/1999 Sb. Alternativně Úřad navrhl, aby Městský soud v Praze ze stejných důvodů a zejména s přihlédnutím k rozsudku Soudního dvora Evropské unie Rechnungshof v. Österreichischer Rundfunk ve spojených věcech C-465/00; C-38/01; C-139/01 předložil Soudnímu dvoru dle čl. 267 Smlouvy o fungování Evropské unie předběžnou otázku k posouzení toho, zda lze ustanovení § 8b zákona č. 106/1999 Sb. vykládat v souladu s čl. 6 písm. c) a čl. 7 písm. c) směrnice 95/46/ES tak, že ukládá bez rozlišení poskytnout osobní údaje o příjmu každého zaměstnance veřejné sféry.

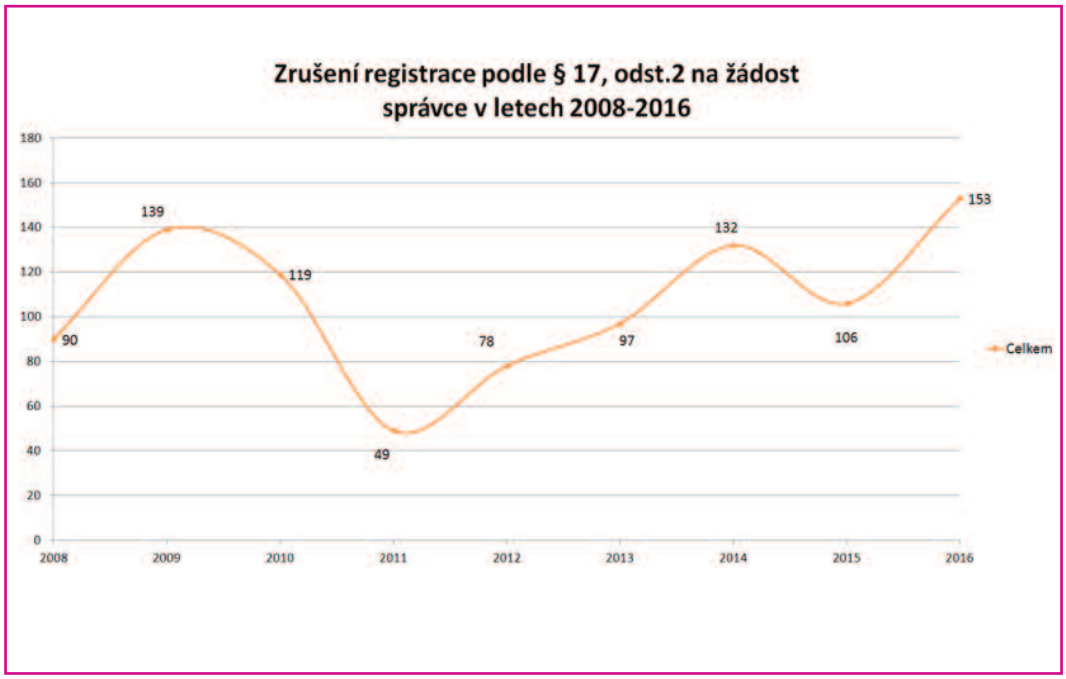
Městský soud v Praze v otázce posouzení, zda došlo k překročení limitů informační povinnosti podle § 8b zákona č. 106/1999 Sb., ovšem dospěl k názoru, že závěr Úřadu spočívá na nesprávném právním posouzení věci. Soud neshledal prostor pro předložení věci Ústavnímu soudu podle čl. 95 Ústavy ČR či pro předložení předběžné otázky Soudnímu dvoru EU podle čl. 267 Smlouvy o fungování Evropské unie. Svůj závěr odůvodnil tím, že nemá důvod jakkoli se odchylovat od právního názoru Nejvyššího správního soudu, vysloveného v rozhodnutí č.j. 8 As 55/2012-62 ze dne 22. října 2014, a to zejména s ohledem na závěry rozsudku Nejvyššího správního soudu č.j. 1 Afs 140/2008-77 ze dne 8. ledna 2009, který konstatoval, že podmínkou právní jistoty jako jednoho ze základních atributů právního státu je relativní stabilita judikatury. Z rozhodnutí č.j. 8 As 55/2012-62 ze dne 22. října 2014 pak vyplývá, že ustanovení § 8b zákona č. 106/1999 Sb. zásadně nedává prostor pro úvahu, zda na základě principu proporcionality informace o příjemcích veřejných prostředků poskytnout, neboť toto řeší již samotné ustanovení § 8b odst. 3 zákona č. 106/1999 Sb. Nicméně se připouští výjimečné případy pro korektivní princip zásady přiměřenosti, a to za situací, v nichž by jinak nebylo možno dosáhnout ústavní konformity aplikace ustanovení § 8b zákona č.106/1999 Sb. Podle Městského soudu v Praze tak sice nelze vyloučit, že přinejmenším někteří z okruhu zaměstnanců, jejichž osobní údaje byly zveřejněny, mohou případně spadat pod korektivní dosah limitovaného testu proporcionality v pojetí Nejvyššího správního soudu (prima facie řidiči či údržbáři), Úřad však úvahu korespondující se závěry Nejvyššího správního soudu do svého rozhodnutí (logicky) nevtělil a je zároveň zjevné, že do výroku rozhodnutí o správním deliktu zahrnul na druhé straně zaměstnance, kteří rovněž prima facie představují typické zástupce činností, jež užití korektivního testu proporcionality vylučují.

• REGISTRACE

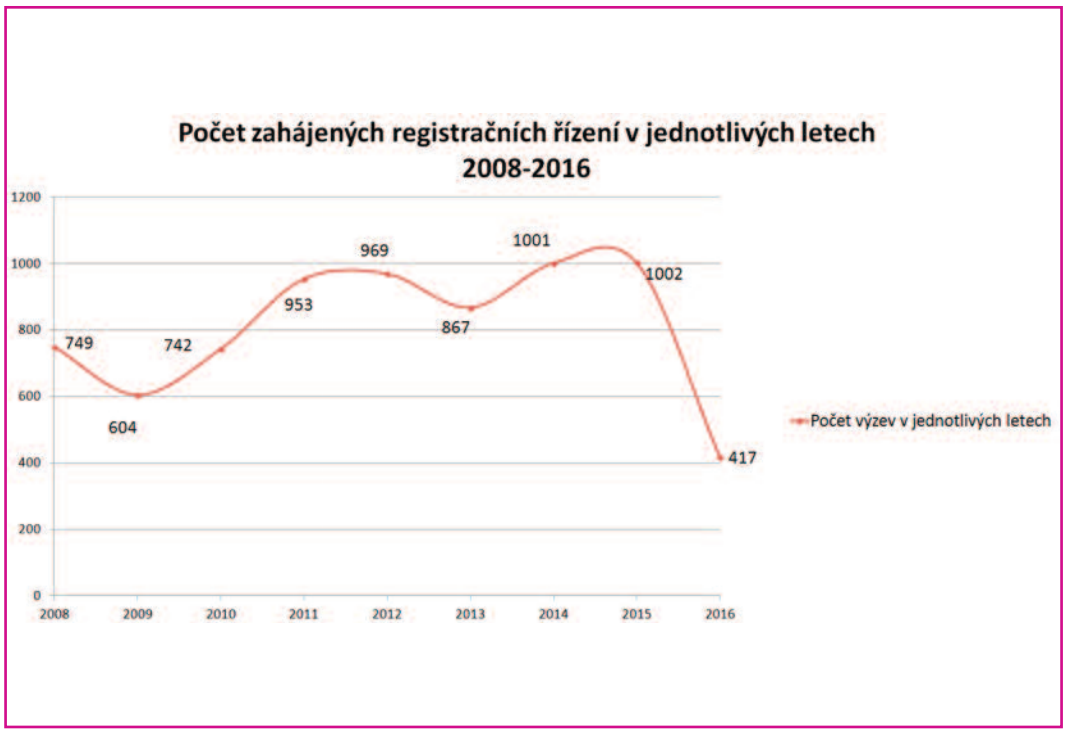
V roce 2016 pokračoval trend z předchozích let, kdy rostl počet podaných oznámení o zpracování osobních údajů, v některých letech až o desítky procent za rok. Za posledních devět let tak narostl počet přijatých oznámení o 292 %.



V případě, že oznámení neobsahuje všechny náležitosti, které jsou nezbytné pro samotné posouzení zpracování, je správci zaslána výzva k doplnění informací. V roce 2016 Úřad zahájil celkem 417 řízení o registraci podle § 16 odst. 4 zákona o ochraně osobních údajů. V případě počtu zahájených registračních řízení došlo v letošním roce k významnému úbytku, který byl způsoben především úpravou části registračního formuláře týkající se kamerových systémů viz níže. Dalším faktorem bylo postupné upozaďování významu registru vzhledem k tomu, že nové obecné nařízení o ochraně osobních údajů účinné od května 2018 již s obecnou oznamovací povinností v současné podobě nepočítá. Zatímco v předchozích letech tvořil počet zahájených registračních řízení cca 17 % z celkového počtu přijatých oznámení, v letošním roce je to pouze 4,3 %.

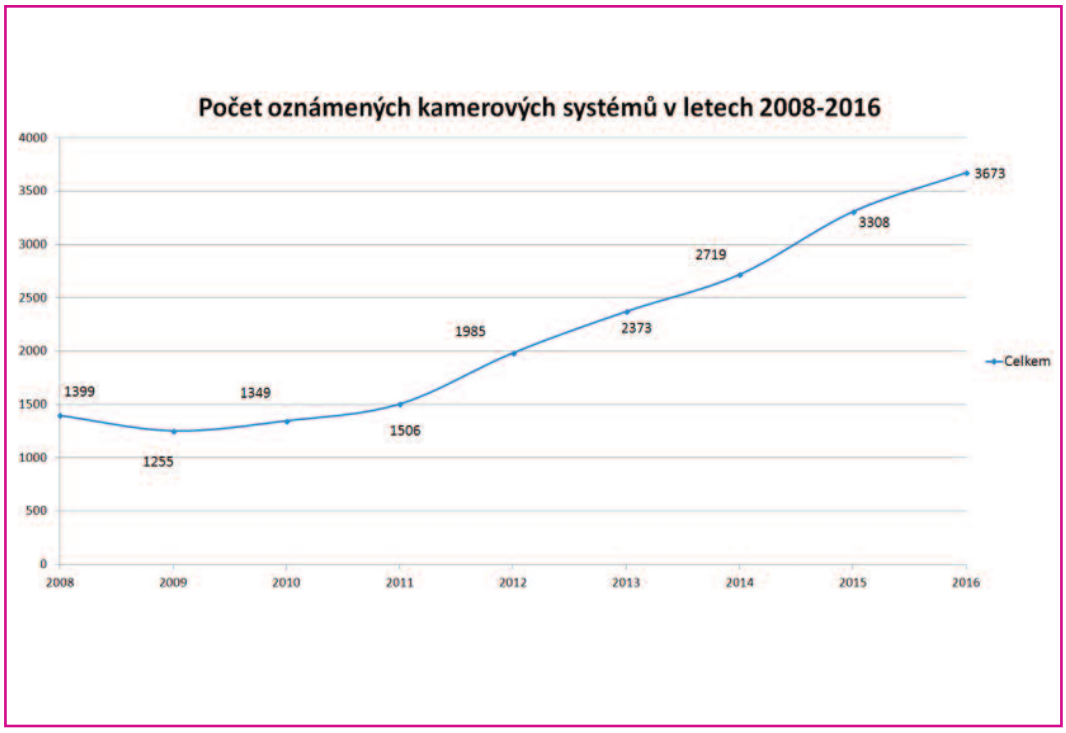


Vedle posuzování přijatých registračních oznámení vydává Úřad rovněž rozhodnutí o zrušení registrace podle § 17a odst. 2 zákona č. 101/2000 Sb. V letošním roce bylo zrušeno celkem 153 zpracování na žádost správce, nejčastěji z důvodů zániku či sloučení společnosti, zrušení podnikatelské činnosti, nebo ukončení zpracování osobních údajů. Z grafu níže vyplývá, že rovněž v tomto případě zaznamenal Úřad navýšení počtu žádostí správců o zrušení registrace.



Podle § 19 zákona č. 101/2000 Sb. má správce zapsaný v registru zpracování povinnost po ukončení své činnosti Úřadu sdělit, jak naložil s osobními údaji. Jelikož tato povinnost ze strany správců není zpravidla plněna, přistoupil Úřad na základě informací z Registru osob a Registru obyvatel k vyřazování spisů již neexistujících registrovaných subjektů z veřejného registru, čímž dochází k „vyčištění" veřejného registru zpracování vedeného služebním úřadem o tisíce zpracování, které již neprobíhají, neboť původní oznamovatel/správce zanikl nebo, v případě fyzických osob, zemřel.

Nejčastějším druhem zpracování (cca 38 % z celkového počtu přijatých oznámení), které se v tomto roce objevovalo, bylo podobně jako v letech minulých zpracování prostřednictvím kamerových systémů. Jak ukazuje graf níže, i zde má počet oznámených zpracování vzestupnou tendenci. Celkem je v registru zpracování osobních údajů zapsáno 3673 subjektů, které podaly oznámení o zpracování osobních údajů kamerovými systémy. Od roku 2008 tak tvoří tato oznámení pravidelně cca jednu třetinu všech došlých oznámení o zpracování.



V roce 2016 došlo rovněž k úpravě části formuláře oznámení o zpracování osobních údajů, které se týkalo kamerových systémů. Bylo zvoleno řešení pomocí zaškrtávacích políček, případně doplněné upřesňujícím textovým popisem. Řešení umožňuje správci jednoduše popsat charakteristiky kamerového systému (umístění, režim, doba uchování, informovanost subjektů údajů, přijatá opatření k ochraně osobních údajů), pouhou volbou z nabízených možností. Možnosti byly stanoveny na základě dlouhodobého sledování nejčastěji oznamovaných parametrů kamerových systémů. V případě popisu technicko-organizačních opatření se zpracování osobních údajů kamerovými systémy jeví natolik specifické, že bylo odděleno do zvláštního bodu. Pokud správce volí neobvyklé nebo problematické charakteristiky kamerového systému, je nucen doplnit komentář, který je popisuje a v některých případech i zdůvodňuje, proč byly vybrány. Tento postup by měl směřovat správce k tomu, aby při návrhu kamerového systému volili

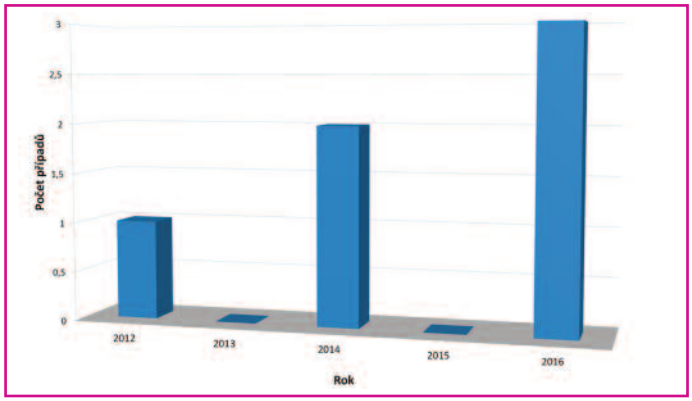
bezproblémová řešení z hlediska ochrany osobních údajů. Úřadu pak přináší zmenšení administrativy spojené s přijímáním oznámení o zpracování osobních údajů (méně dotazů, méně výzev na doplnění oznámení).

V letošním roce docházelo k nárůstu oznámení týkajících se umístění kamerových systémů v prostředcích městské hromadné dopravy některých velkých měst. Účelem instalace kamerového systému do vozidel MHD, případně kamer zabírajících prostor před dopravním prostředkem, je ochrana 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, případně i ochrana zaměstnanců před napadením. Toto řešení je možné za určitých podmínek, kterými jsou omezení nasazení (nasazení na kritických spojích nebo pouze na spojích v rámci hranice města), zvýšená rizika (v dopravních prostředcích dochází k nárůstu trestné činnosti či ničení nebo poškozování majetku), dostatečné zabezpečení (zejména řešení, kdy je možný přístup ke kamerovým záznamů pouze za fyzické přítomnosti Policie ČR) a pravidelné revize nasazení kamer spojené se změnami počtu kamer na základě výsledků jejich nasazení.

V souvislosti s rozvojem informačních technologií se stále častěji objevují zvláštní způsoby zpracování prováděné prostřednictvím těchto nových technologií. Týká se to zejména stále častěji používání biometrických systémů, které se používají jako součást bezpečnostních opatření pro kontrolu osob vstupujících do budov, resp. některých pracovišť, ověření přístupových práv při práci s počítačem, docházkové systémy, ale stále více i v reklamě a marketingu. V roce 2016 Úřad obdržel oznámení o zpracování osobních údajů osob vstupujících do škol, a to na základě zpracování charakteristik otisků prstů (využití šablony) za účelem ochrany žáků a studentů ve školách. Vzhledem k tomu, že z oznámení bylo zřejmé, že již aktivně probíhá, byl dán podnět k zahájení kontroly.

Narušení bezpečnosti osobních údajů v elektronických komunikacích

Ani v letošním roce nedošlo oproti letům minulým k navýšení počtu oznámení, jak z grafu vyplývá. Po pěti letech zkušeností lze konstatovat, že povinné subjekty plní tuto zákonem danou povinnost pouze velmi sporadicky. S obdobnou situací se potýká i většina ostatních členských zemí EU. Jeden z hlavních důvodů nezájmu správců oznamovat případy narušení je možné shledávat v obavách oznamovatelů z případných sankcí, pokud by se přiznali, že k narušení bezpečnosti osobních údajů v jejich společnosti došlo. Naopak neoznámení případného incidentu sankcionováno není. V tomto ohledu přinese změnu nové obecné nařízení o ochraně osobních údajů, které za neoznámení narušení osobních údajů předpokládá sankci až do výše 10 mil. eur.



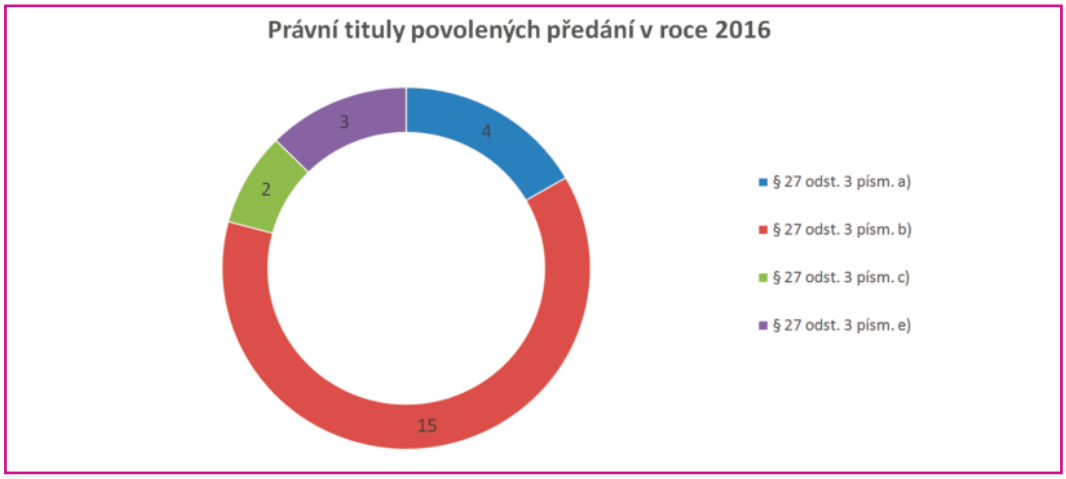
V roce 2016 došlo k oznámení tří takových případů. Nejvýznamější z nich se týkal odcizení osobních údajů zákazníků (v řádech stotisíců osob) telekomunikační společnosti jejím zaměstnancem. Odcizená data byla zaměstnancem nabídnuta ke koupi jiné společnosti. Vzhledem k problematickému nastavení technicko-organizačních opatření dotčenou telekomunikační společností jí byla udělena pokuta ve výši 3,6 milionů Kč, z maximální možné sazby 10 milionů Kč.

• PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

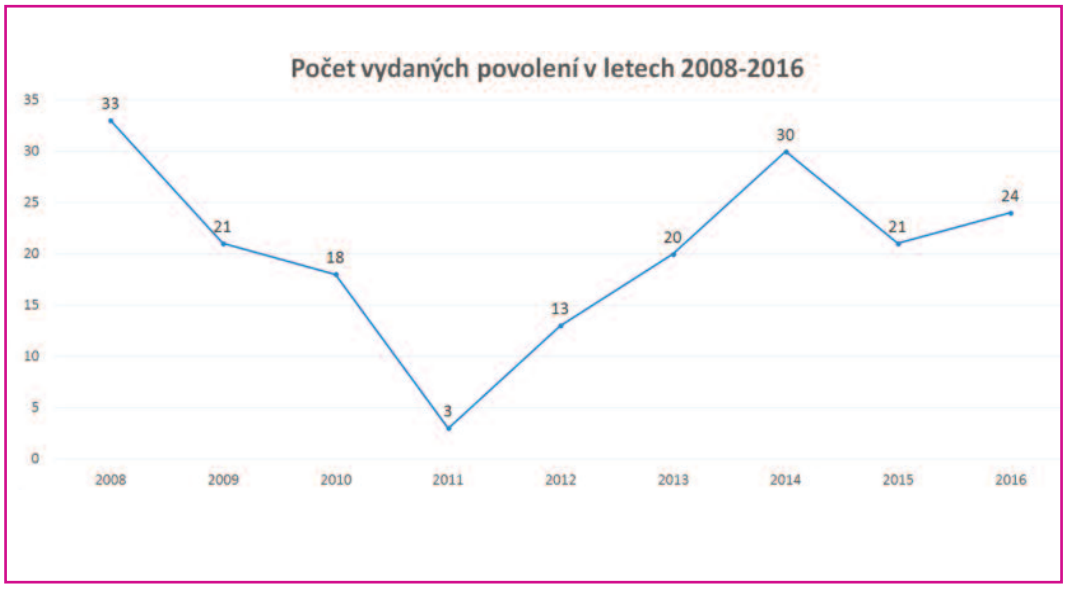
V roce 2016 Úřad vydal 24 povolení k předání osobních údajů do třetích zemí podle § 27 odst. 4 zákona č. 101/2000 Sb.

Nejčastějším právním titulem, na jehož základě Úřad povolení vydal, bylo 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 15 případech.

Třikrát 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. Čtyřikrát bylo právním titulem povolení ustanovení § 27 odst. 3 písm. a), tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů. Ve dvou případech vydal Úřad povolení pro zpřístupnění katastrálních údajů na základě splnění podmínek daných ustanovením § 27 odst. 3 písm. c) zákona č. 101/2000 Sb.



Byl tak potvrzen trend známý již z předchozích let, kdy se odpovědní správci osobních údajů nespoléhají na souhlas subjektů údajů, ale řeší předání údajů do třetích zemí s nedostatečnou úrovní ochrany osobních údajů s použitím nástrojů, které zajistí předaným údajům adekvátní úroveň ochrany i v dané třetí zemi. Těmito nástroji jsou vedle uvedených závazných vnitropodnikových pravidel především standardní smluvní doložky. Při použití standardních smluvních doložek podle rozhodnutí Evropské komise přitom není ani nutné žádat Úřad o povolení, protože předání probíhá v režimu ustanovení § 27 odst. 2 zákona č. 101/2000 Sb. na základě rozhodnutí Evropské unie.



Geograficky výrazně převažovala nad předáními do jedné konkrétní země předání do více zemí nebo lépe řečeno do velkého počtu poboček v mnoha zemích, ve kterých typicky působí skupina, do níž patří i český správce osobních údajů jako pobočka nadnárodní skupiny, přičemž tato skupina zajišťuje ochranu osobních údajů sdílených v rámci skupiny právě výše uvedenými závaznými vnitropodnikovými pravidly. Jiným modelovým případem jsou cestovní kanceláře, které předávají osobní údaje klientů svým partnerským organizacím, které zajišťují v zahraničních turistických destinacích ubytování, dopravu a další služby cestovního ruchu.

Provizorium po zrušení rozhodnutí Komise o bezpečném přístavu

Jednoznačně nejsledovanějším procesem a nejvýraznější změnou v oblasti předávání osobních údajů byla tvorba nového nástroje předávání osobních údajů do Spojených států amerických, tzv. „štítu soukromí".

Potřeba vytvoření nového nástroje předávání osobních údajů do Spojených států amerických vyvstala v důsledku zrušení programu Safe Harbor jako nástroje zajišťujícího adekvátní ochranu osobních údajů ve Spojených státech amerických. „Zasloužil se" o to Soudní dvůr Evropské unie, když v rozsudku ve věci C-362/14 Maximillian Schrems v. Data Protection Commissioner ze dne 6. října 2015 prohlásil za neplatné rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu" a s tím souvisejících „často kladených otázek" vydaných Ministerstvem obchodu Spojených států amerických.

V důsledku tohoto rozsudku již nebylo možné nadále považovat závazek příjemce osobních údajů ve Spojených státech amerických dodržovat zásady „bezpečného přístavu" (Safe Harbor) za dostatečnou záruku ochrany osobních údajů předaných do Spojených států amerických.

Pro nastalé provizorium vydala v rámci koordinace postupu dozorových orgánů jednotlivých členských zemí Evropské unie Pracovní skupina podle čl. 29 směrnice Evropského parlamentu a Rady 95/46/ES (dále jen „WP29") prohlášení ze dne 16. října 2015. V tomto prohlášení WP29 vyzvala Evropskou komisi k jednáním se Spojenými státy o vytvoření nového nástroje bezpeč-

ného předání osobních údajů. WP29 zároveň potvrdila, že do té doby je nutné zajistit předání osobních údajů do Spojených států amerických, které se ukáže být nezbytně nutným k naplnění stanovených účelů, jinými nástroji, jimiž lze zajistit odpovídající úroveň ochrany osobních údajů ve třetích zemích s nedostatečnou úrovní ochrany osobních údajů, mezi kterými se jako nejvhodnější jeví standardní smluvní doložky nebo závazná podniková pravidla.

Na dané rozhodnutí reagoval Úřad doporučením, které bylo publikováno na webových stránkách Úřadu. Zároveň v průběhu října 2015 rozeslal doporučující sdělení všem cca 220 správcům osobních údajů, z jejichž zaregistrovaných oznámení o zpracování osobních údajů podle § 16 zákona č. 101/2000 Sb. vyplynulo, že v rámci zpracování může docházet k předání osobních údajů do Spojených států amerických společnostem zapsaným v programu Safe Harbor.

Analýza toků osobních údajů do třetích zemí ke dni 16. února 2016

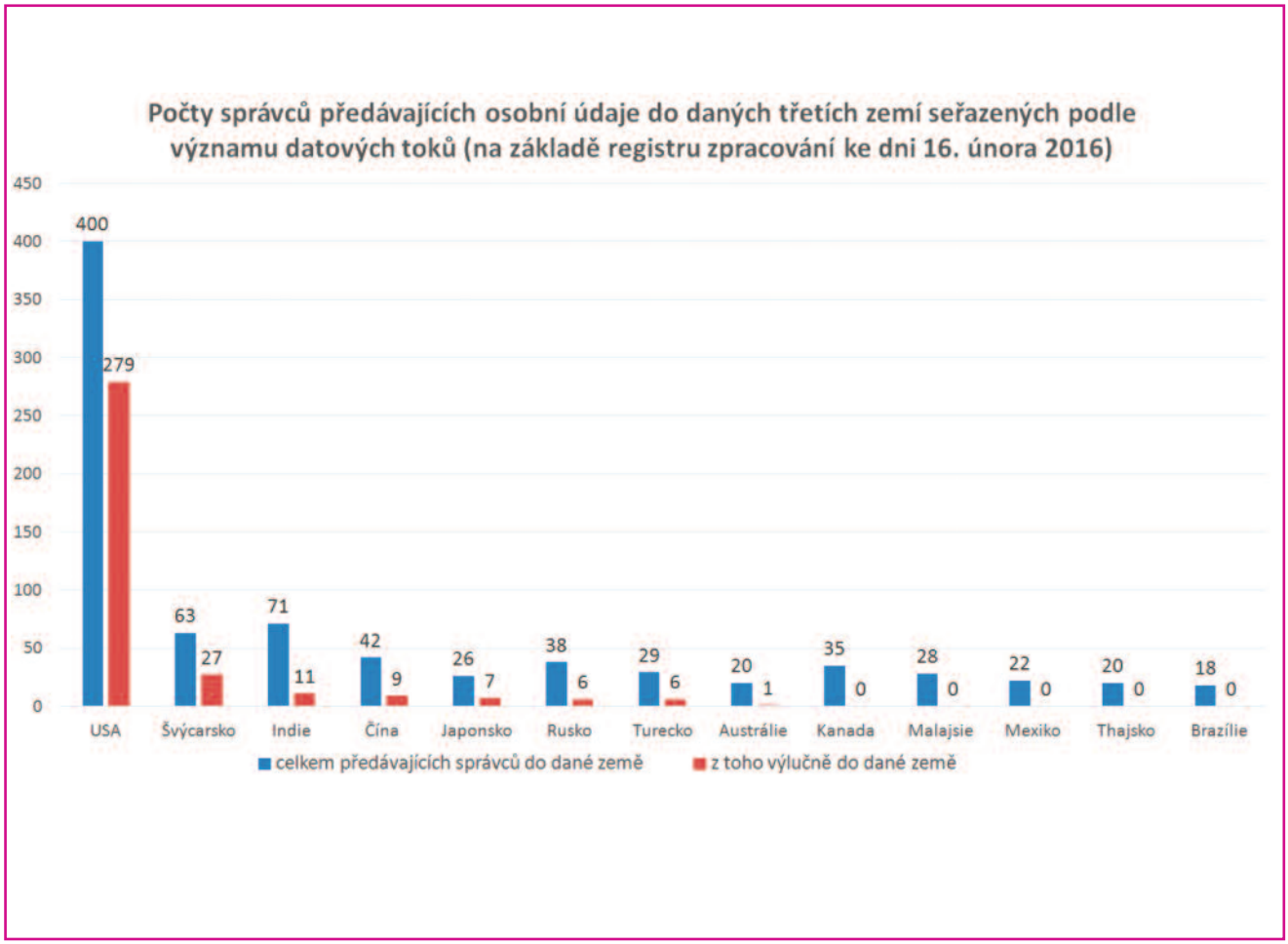
Aby bylo možné získat alespoň rámcovou představu o tocích osobních údajů z Evropské unie do Spojených států a jejich významu ve srovnání s jinými zeměmi, provedl Úřad rozbor údajů o předáních osobních údajů do zahraničí obsažených v registru zpracování. V rámci plnění oznamovací povinnosti podle § 16 zákona č. 101/2000 Sb. poskytují totiž správci osobních údajů základní údaje o tom, zda hodlají realizovat předání údajů do třetích zemí mimo Evropskou unii, případně do kterých zemí a zda přitom využijí nástroje standardních smluvních doložek. Úřad analýzu aktualizoval a upřesnil k datu 16. února 2016, přičemž se ukázalo, že jde o unikátní analýzu i v rámci celé Evropské unie. Proto považujeme za vhodné zveřejnit na tomto místě výsledky této analýzy.

V registru se ke dni 16. února 2016 nalézalo 1922 správců osobních údajů, kteří měli v některém ze svých aktuálně zaregistrovaných oznámení podle § 16 zákona č. 101/2000 Sb. uvedeno, že předávají osobní údaje do třetích zemí. Velká část z tohoto počtu správců spadá na oznámení z prvních let po vzniku Úřadu, kdy správci neoznamovali konkrétní třetí země, do nichž hodlají osobní údaje předat, ani použití standardních smluvních doložek. To je hlavní důvod, proč má analýza, co se týče absolutních čísel, pouze orientační hodnotu, přičemž však zároveň neztrácí vypovídací hodnotu pro srovnání počtu předání do jednotlivých třetích zemí.

Hlavní výsledek analýzy je shrnut v následující tabulce třinácti třetích zemí, do nichž jsou osobní údaje předávány nejčastěji. V tabulce je přitom v celkovém počtu správců předávajících údaje do dané třetí země rozlišen počet správců osobních údajů, kteří předávají údaje výlučně do dané třetí země, a počet správců, kteří v rámci svých předání předávají osobní údaje vedle dané třetí země i do dalších třetích zemí. Zdá se přitom, že počty správců, kteří předávají výlučně do dané země, lépe reflektují význam dané země jako reálné cílové země toků údajů, ve které sídlí mateřské společnosti a velcí zpracovatelé osobních údajů. Proto jsou v grafu vycházejícím z tabulky země seřazeny podle významu těchto cílových třetích zemí, do kterých jsou osobní údaje předávány.

třetí země	Počet správců předávajících osobní údaje do dané třetí země		
	celkem	výlučně do dané země	i do jiných třetích zemí
USA	400	279	121
Indie	71	11	60
Švýcarsko	63	27	36
Čína	42	9	33
Rusko	38	6	32
Kanada	35	0	35
Turecko	29	6	23
Malajsie	28	0	28
Japonsko	26	7	19
Mexiko	22	0	22
Austrálie	20	1	19
Thajsko	20	0	20
Brazílie	18	0	18

Tabulka: Třetí země seřazeny podle počtu správců předávajících osobní údaje do dané třetí země na základě registru zpracování ke dni 16. února 2016



Z uvedené tabulky a grafu vyplývá, že Spojené státy americké jsou naprosto dominantním příjemcem toku osobních údajů předávaných z České republiky mimo Evropskou unii. Spojené státy předstihly v počtu předávajících správců z České republiky šestinásobně za nimi následující Indii a Švýcarsko. Co se týče významu datových toků, překonaly Spojené státy druhé Švýcarsko dokonce desetinásobně a zhruba třicetinásobně i každou z následující skupiny pěti třetích zemí v pořadí Indie, Čína, Japonsko, Rusko, Turecko. Ukázalo se zároveň, že kromě uvedených sedmi zemí už neexistuje žádná další třetí země, která by hrála významnou roli jako příjemce toků osobních údajů z České republiky, a to ani v tabulce uvedená Austrálie, Kanada, Malajsie, Mexiko, Thajsko a Brazílie, ani další za nimi v počtu předávajících správců následující země, kterými jsou Srbsko (17), Egypt (15), Filipíny (14), Norsko (14), Chorvatsko do vstupu do Unie (14), Argentina (13), Jižní Afrika (13), Jižní Korea (12) atd.

Předání osobních údajů do Spojených států amerických byla vyhodnocena i z hlediska právního titulu předání. Znovu je třeba upozornit, že údaje v registru zpracování nemohou odrážet přesný aktuální stav dané problematiky, protože registrační povinnost podle § 16 zákona jen nepřímo souvisí s povinnostmi správce předávajícího osobní údaje do zahraničí podle § 27 zákona. Přesto lze konstatovat, že většina z cca 220 oslovených správců, kteří podle svých zaregistrovaných oznámení předávali ještě v říjnu 2015 osobní údaje do Spojených států amerických na základě zapojení příjemců v programu Safe Harbor, nejenže zareagovala na změněnou situaci a zajistila ochranu předaných osobních údajů jiným způsobem, ale promítla tuto skutečnost i do registru zpracování a provedla změnu svých zaregistrovaných oznámení v uvedeném smyslu. Většina správců přitom evidentně využila institut standardních smluvních doložek.

V posledních letech přitom Úřad nejčastěji vydává povolení na základě předložených závazných vnitropodnikových pravidel (BCR) skupiny, v jejímž rámci je předání osobních údajů do třetích zemí realizováno v režimu § 27 odst. 3 písm. b) zákona č. 101/2000 Sb. Úřad v současné době vydává povolení na omezenou dobu, zpravidla na tři roky. Ke dni 16. února 2016 Úřad evidoval 35 platných povolení k předání osobních údajů do třetích zemí na základě BCR, z tohoto počtu 34 povolení zahrnovalo předání osobních údajů do Spojených států amerických (z tohoto počtu pak 10 povolení výlučně do USA, 24 povolení i do dalších zemí).

Analýza toků osobních údajů do třetích zemí provedená na základě údajů v registru zpracování ke dni 16. února 2016 ukázala, že většina z cca 220 oslovených správců vzala vážně doporučení Úřadu a zajistila předání osobních údajů do USA standardními smluvními doložkami anebo závaznými podnikovými pravidly. Prokázalo se tak, že je v zásadě možné při předání osobních údajů do USA nahradit zrušené rozhodnutí Komise o bezpečném přístavu stávajícími alternativními nástroji.

Analýza zároveň prokázala, že Spojené státy americké jsou zdaleka nejdůležitější cílovou zemí toku osobních údajů z České republiky mimo Evropskou unii. Tento význam Spojených států amerických jako příjemce osobních údajů z České republiky lze vysvětlit dvěma základními faktory. Prvním faktorem je skutečnost, že ve Spojených státech sídlí mnohé mateřské společnosti a centrály firemních poboček působících v České republice. Druhým faktorem je skutečnost, že rovněž většina velkých společností zajišťujících služby informační společnosti různého typu včetně cloudových služeb sídlí a spravuje shromážděné údaje ve Spojených státech amerických. Přitom míra použití amerických softwarových platforem, sociálních sítí a cloudových řešení v České republice a v celé Evropské unii, neoddělitelně spojená s toky osobních údajů do USA, je natolik rozšířená, že se v tomto aspektu nemůže Spojeným státům žádná jiná třetí země ani vzdáleně přiblížit.

Tyto důvody včetně politického i hospodářského přesahu významu transatlantických toků osobních údajů vedly pracovní skupinu WP29 i Evropskou komisi k závěru, že je nutné co nejdříve přijmout nový robustní nástroj ochrany osobních údajů předaných do USA, který nahradí stávající program Safe Harbor a který zajistí obnovení důvěry obyvatelstva Evropské unie v adekvátní ochranu osobních údajů předávaných do Spojených států amerických.

Privacy Shield

Po měsících intenzivních jednání s představiteli Spojených států amerických ohlásila Evropská komise dne 2. února 2016 vznik nového nástroje pro bezpečné transatlantické toky osobních údajů, tzv. Euroamerického štítu soukromí (Privacy Shield) a předložila k dalšímu posouzení Evropské radě, Evropskému parlamentu a také pracovní skupině WP29 návrh příslušného rozhodnutí Komise.

Skupina WP29 shrnula své kritické připomínky a návrhy změn ve Stanovisku 1/2016 k návrhu rozhodnutí Komise o odpovídající ochraně osobních údajů poskytované štítem EU-USA na ochranu soukromí ze dne 13. dubna 2016. Vedle kritiky nepřehlednosti a nekonzistentnosti mezi jednotlivými dokumenty, tvořícími rámec navrhovaného programu Privacy Shield, chybějících definicí používaných pojmů a řady dalších konkrétních připomínek k zásadám a způsobu fungování navrhovaného programu Privacy Shield vyjádřila WP29 obavu, že právní rámec Spojených států amerických i přes řadu legislativních změn reagujících na Snowdenovo zveřejnění praktik amerických bezpečnostních složek nevylučuje plně možnost hromadného přístupu k předaným osobním údajům obyvatel Evropské unie ze strany státních orgánů Spojených států amerických. Podobným způsobem se k věci vyjádřil i evropský komisař ochrany osobních údajů ve svém tiskovém prohlášení ze dne 30. května 2016.

Na tomto místě je třeba zdůraznit, že v rámci dalšího vyjednávání Evropské komise s americkými partnery o definitivní podobě textu výše uvedeného rozhodnutí včetně zásad štítu soukromí byly výše zmíněné kritické připomínky pracovní skupiny WP29 do značné míry zohledněny.

Rozhodnutí o odpovídající úrovni ochrany osobních údajů zajištěné „euroamerickým štítem soukromí" přijala Evropská komise dne 12. července 2016.

Jádro štítu soukromí představuje Annex II výše uvedeného rozhodnutí Komise. Annex II obsahuje plný text zásad štítu soukromí, k jejichž dodržování se zavazují američtí dovozci osobních údajů z Evropské unie zapsaní do seznamu štítu soukromí. Systém štítu soukromí je přitom vystavěn v podstatě stejným způsobem, jakým fungoval systém bezpečného přístavu. Štít soukromí však oproti bezpečnému přístavu má navíc řadu prvků, které zajišťují reálnou ochranu osobních údajů a uplatnění práv subjektů údajů. Mezi tyto prvky patří:

- závazek federálního ministerstva obchodu (Department of Commerce), že transparentním způsobem povede webové stránky se seznamem organizací zapojených do štítu soukromí; že bude provádět kontroly, zda organizace plní své povinnosti vyplývající z přihlášení se k zásadám štítu soukromí včetně zveřejněné privacy policy a každoročního obnovení certifikace, a že v případě neplnění bude přistupovat k vyškrtnutí organizace ze seznamu štítu soukromí;
- každoroční společný audit fungování štítu soukromí za účasti Evropské komise, federálního ministerstva obchodu a federální obchodní komise (Federal Trade Commission);
- výslovné uvedení odpovědnosti organizace za předání osobních údajů dalším stranám, přičemž tito další příjemci v případě správců musí poskytovat stejnou úroveň ochrany osobních údajů, v případě zpracovatelů musí být předání zajištěno smlouvou;

- proces řešení stížností subjektů údajů v arbitrážním řízení před třemi zvolenými arbitry z „arbitrážního panelu“ (příloha 1 Annexu II);
- institut nezávislého ombudsmana pro řešení stížností na zpracování osobních údajů americkými zpravodajskými službami a žádostí o přístup k datům podávaných evropskými subjekty údajů prostřednictvím evropských vládních institucí dohlížejících na činnost zpravodajských služeb (Annex III).

Program štítu soukromí začal prakticky fungovat od 1. srpna 2016. Od tohoto dne se americké společnosti mohou přihlásit u Ministerstva obchodu Spojených států počínaje k účasti v programu Privacy Shield. Seznam zapsaných společností s dalšími informacemi lze nalézt na webových stránkách https://www.privacyshield.gov/welcome Ministerstva obchodu Spojených států.

Praktickým důsledkem tohoto rozhodnutí je možnost bezproblémového předání osobních údajů těm americkým společnostem, které se přihlásí k dodržování zásad štítu soukromí. Předávající správce osobních údajů nemusí žádat Úřad o povolení ve smyslu § 27 odst. 4 zákona č. 101/2000 Sb., neboť předání osobních údajů proběhne v režimu ustanovení § 27 odst. 2 zákona č. 101/2000 Sb. „na základě rozhodnutí orgánu Evropské unie“. Právní stav je tedy analogický se stavem před zrušením rozhodnutí Safe Harbor.

Evropská komise rovněž vydala „průvodce štítem soukromí“, kde občané členských států naleznou obecný návod, jak podat stížnost a uplatnit další práva subjektů údajů vůči americkým firmám přihlášeným v programu štít soukromí.

Kvalitu práce odvedené vyjednávacími týmy prověří Evropský soudní dvůr, který pod značkou T-670/16 řeší žalobu na zrušení rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů zajištěné „euroamerickým štítem soukromí“ podanou v září 2016 irským sdružením ochránců soukromí Digital Rights Ireland.

• SCHENGENSKÁ SPOLUPRÁCE

Právní úprava rozsáhlých evropských informačních systémů, mezi něž patří Schengenský informační systém druhé generace (SIS II), Vízový informační systém (VIS), Eurodac a Celní informační systém (CIS), klade velký důraz na oblast ochrany osobních údajů a aktivní plnění s tím souvisejících povinností dozorových orgánů. V České republice je tímto dozorovým orgánem Úřad pro ochranu osobních údajů. Kromě dohledu a kontroly související s plněním požadavků na zákonné zpracování osobních údajů ze strany správce v rámci výše zmíněných systémů se Úřad zabýval také vznikem nových informačních systémů, a to právě z pohledu zpracování osobních údajů. Příkladem lze uvést tzv. EES systém (Systém vstupu/výstupu) zaměřený na zpracování osobních údajů příslušníků třetích států s právem krátkodobého pobytu na území Evropské unie. Dalším nově vznikajícím systémem je systém ETIAS, v rámci kterého budou zpracovávány osobní údaje osob ze třetích zemí, které nemají ve vztahu k Evropské unii vízovou povinnost. S ohledem na velké množství osobních a citlivých údajů zpracovávaných v těchto typech systémů je nezbytné zajistit odpovídající míru ochrany práv subjektu údajů, neboť dodržování principů ochrany osobních údajů představuje primární předpoklad transparentního fungování informačních systémů v rámci schengenské spolupráce.

Činnost jednotlivých koordinačních skupin v oblasti schengenské, vízové a celní spolupráce

Hlavní aktivitou koordinačních skupin v roce 2016 byla příprava společných modelů inspekcí, které povedou ke sjednocení kontrolních postupů jednotlivých států podílejících se na využívání informačních systémů.

V rámci koordinační skupiny, která dohlíží nad zákonností zpracování dat v systému Eurodac, byl vypracován a schválen jednotný model kontrolních dotazů pro národní inspekce systému Eurodac. Cílem společného formátu kontrol realizovaných v jednotlivých členských státech má být výstup, který umožní porovnat fungování a správu systému z pohledu ochrany osobních údajů.

Koordinační skupina pro dohled nad systémem CIS (Celní informační systém) připravuje rovněž společný formát kontrol. Česká republika přitom byla určena, aby plnila funkci zpravodaje při jeho přípravě. V rámci činnosti této skupiny byla rovněž vypracována jednotná příručka pro uplatnění práva na přístup k údajům zpracovávaným v CIS včetně formulářů určených subjektům údajů pro jeho realizaci. Tento dokument bude na jaře roku 2017 zpřístupněn jednak na internetových stránkách Úřadu a dále na internetových stránkách Celní správy České republiky v sekci Evropská unie/CIS.

Aktuální problémy řešené v rámci koordinačních skupin

Koordinační skupina pro systém Eurodac (Eurodac SCG) se aktuálně zabývala problematikou návrhu přepracovaného nařízení o zřízení systému Eurodac. Komisaři pro migraci, vnitřní věci a občanství, panu Dimitrisi Avramopoulosovi, byl jménem všech členů koordinační skupiny zaslán dopis na podzim roku 2016 vyjadřující obavy z navrhovaných změn. Především návrh na snížení věkové hranice osob, kterým jsou otisky prstů odebírány, ze čtrnácti na šest let, uchovávání fotografií žadatelů v centrálním systému s cílem budoucího využití pro software umožňující rozpoznávání obličejů na základě biometrických identifikátorů a prodloužení lhůty pro uchování osobních údajů, představuje naprosto zásadní změny, které je potřeba uvést do souladu se základními principy ochrany osobních údajů.

Koordinační skupina pro vízový informační systém (VIS SCG) v rámci změn reagujících na přijetí nového schengenského hodnotícího mechanismu (nařízení Rady EU č. 1053/2013) připravuje samostatnou kapitolu věnovanou vízovému informačnímu systému, která bude nově zařazena do dokumentu koordinační skupiny pro schengenský informační systém s cílem aktualizovat jednotná doporučení pro schengenská hodnocení.

Dále se uvedená koordinační skupina zabývala implementací článku 41 nařízení č. 767/2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy, který ukládá vnitrostátním orgánům dozoru povinnost provést nejméně jednou za čtyři roky audit zpracování údajů ve vnitrostátním systému VIS. Pomocí dotazníkového šetření bylo zjišťováno, zda byl audit proveden, jakým způsobem a jaká vzešla doporučení pro správce systému.

Koordinační skupina pro celní informační systém (CIS) připravila v uplynulém roce mimo jiné jednotný dokument upravující obecná pravidla zpracování osobních údajů v CIS. V rámci brožury jsou rovněž přehledně definována pravidla pro uplatnění práv subjektů údajů v jednotlivých členských státech včetně České republiky. Tento dokument byl upraven s ohledem na národní právní úpravu a na jaře roku 2017 bude uveřejněn na internetových stránkách Úřadu jako informace pro veřejnost v rubrice Informační systémy EU (Schengen).

Počty podnětů, stížností, dotazů a jejich vyřízení

Během loňského roku obdržel Úřad celkově 10 podnětů týkajících se zpracování osobních údajů v SIS II. Ve všech případech šlo o realizaci práva subjektu údajů na přístup k údajům v SIS II, a to ať už prostřednictvím uplatnění práva na informace či uplatnění práva na výmaz osobních údajů ze systému. Hlavní rolí Úřadu je přezkoumávat postup správce osobních údajů na národní úrovni, jímž je Policie České republiky, přičemž pouze v jednom případě byly shledány skutečnosti nasvědčující porušení práv subjektu údajů.

Úřad dále obdržel 17 podání, v rámci kterých se žadatelé dotazovali na vízovou politiku České republiky či na průběh vyřizování svých vízových žádostí. Vzhledem k tomu, že uvedené nespadá do zákonem svěřené působnosti Úřadu, byli jednotliví žadatelé odkázáni na Ministerstvo zahraničních věcí, do jehož gesce daná problematika náleží. Úřad v této souvislosti průběžně objasňoval své kompetence svěřené zákonem č. 101/2000 Sb., jakož i unijními právními předpisy.

Hodnocení úrovně ochrany osobních údajů

V každém státě schengenského prostoru jsou pravidelně hodnoceny základní aspekty schengenské spolupráce, jako je ochrana vnitřních a vnějších hranic, policejní spolupráce a rovněž úroveň ochrany osobních údajů při využívání SIS II, a to v souladu s nařízením Rady (EU) č. 1053/2013 ze dne 7. října 2013 o vytvoření hodnotícího a monitorovacího mechanismu k ověření uplatňování schengenského acquis a o zrušení rozhodnutí výkonného výboru ze dne 16. září 1998, kterým se zřizuje Stálý výbor pro hodnocení a provádění Schengenu.

Hodnotící týmy jsou vždy vytvářeny ad hoc k jednotlivým evaluacím a jsou složeny ze zástupců Evropské komise a expertů ze členských států. Hodnotící tým na základě předložených dokumentů a kontroly na místě, která obvykle zahrnuje návštěvu policejního útvaru, jenž zajišťuje národní část schengenské databáze, orgánu pro ochranu osobních údajů a dalších dotčených orgánů (Ministerstvo zahraničních věcí pro oblast vydávání schengenských víz, azylový úřad, Ministerstvo vnitra jako gesční orgán schengenské spolupráce), připraví zprávu shrnující jeho poznatky o souladu praxe v daném členském státě s požadavky schengenského acquis.

V roce 2016 byli zaměstnanci Úřadu jako národní experti nominováni do tří evaluačních misí, do Lucemburska (leden 2016), Řecka (květen 2016) a na Maltu (září 2016).

Analytická činnost

VZNIK ANALYTICKÉHO ODDĚLENÍ

V polovině roku 2016 bylo v Úřadu zřízeno analytické oddělení, které postupně začalo plnit své funkce a začleňovat se do činnosti Úřadu. Úřad se tak zařadil mezi orgány státní správy, které kladou důraz na to, aby se složitými či komplexními otázkami ve své působnosti zabývaly systémově. Obecně analýza označuje myšlenkovou činnost, která je používána k řešení problémů (*problem-solving*) nebo k učinění závěru o možnostech řešení. Právní analýza může sloužit k nalezení správného nebo spravedlivého řešení problému, určit možné varianty řešení nebo shledat nutnost změny právní úpravy. Východiskem pro její zpracování je zpravidla platná právní úprava, soudní judikatura a akty aplikace práva; v úvahu je obvykle vzato i právo EU, případně právní úprava v členských státech EU. Uvedené postupy používá rovněž analytické oddělení Úřadu.

Ve druhé polovině loňského roku věnovalo nově vzniklé oddělení pozornost jak obecným otázkám ochrany osobních údajů, tak ochraně osobních údajů ve vztahu k jednotlivým dílčím oblastem právní úpravy. Jednalo se mj. o otázku ochrany osobních údajů v katastru nemovitostí, vztah služebního zákona a povinnosti mlčenlivosti, postavení zmocněnce pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů či o stanovení principů, které by měly být zohledněny při vydávání e-jízdenek (smart cards). V souvislosti s vyjádřením k ústavním stížnostem Úřad zpracoval analýzu zveřejňování platů státních úředníků a upozornil na specifika ochrany osobních údajů v archivech postkomunistických zemí, se kterým počítá i právo EU. Níže jsou uvedeny některé z podstatných závěrů vybraných analýz.

1. Ochrana osobních údajů v katastru nemovitostí

Úřad věnoval zvýšenou pozornost ochraně osobních údajů v katastru nemovitostí. Konkrétně se zabýval tím, zda je zmíněná ochrana dostatečná, pokud došlo k případům poškození majetkových práv jednotlivých občanů (odcizení nemovitosti či pokus o její odcizení) v důsledku podvodného jednání osob, které zneužily osobní údaje vlastníků získané z katastru nemovitostí. Ve zmíněném

kontextu má přitom význam jak ochrana osobních údajů, tak princip veřejnosti či publicity katastru nemovitostí. Jejich vztah by měl být vzájemně vyvážený. Na jedné straně by informace o nemovitosti měly být dostupné všem subjektům, které potřebují z oprávněných důvodů znát vlastníka nemovitosti; na druhé straně by tyto informace měly být třetím subjektům či veřejnosti dostupné jen v nezbytném rozsahu a nad tento rámec by neměly být poskytovány (princip minimalizace údajů). Níže jsou uvedeny některé z úvah určujících pro analýzu:

- Při hledání vyváženosti mezi principem veřejnosti katastru nemovitostí a právem na ochranu osobních údajů není snadné najít optimální řešení. Relevantní právní úprava obou zákonů je v předmětné otázce obecná a neobsahuje výslovnou odpověď. Princip veřejnosti katastru se v českých zemích tradičně uplatňoval prostřednictvím přístupu k pozemkovým knihám. Rovněž v současnosti se v ČR uplatňuje velmi liberální přístup, který spočívá v možnosti třetích osob získat z katastru úplné informace o právních vztazích k nemovitosti nezávisle na vlastníkovi. K tomu slouží i veřejnost sbírky listin, na jejichž podkladě byly zápisy provedeny. Široká možnost nahlížení do katastru nemovitostí a sbírky listin nebyla ovšem dosud podrobena přezkumu z hlediska ústavněprávních principů, případně z hlediska principů ochrany osobních údajů.

- Styčným bodem problematiky ochrany osobních údajů a katastru nemovitostí je např. situace, kdy subjekt údajů požaduje po katastru nemovitostí informaci o tom, kdo byl příjemcem informací o zpracování jeho osobních údajů (laicky řečeno vlastník chce vědět, kdo požadoval informace o jeho nemovitosti). V současné době katastr nemovitostí takovou informaci o příjemci neposkytuje. K tomuto závěru přispělo i dřívější stanovisko Úřadu, podle nějž v uvedené situaci není třeba sdělovat jméno osoby příjemce informace, ale postačí sdělit kategorii příjemce či příjemců (viz § 12 odst. 2 písm. d) zákona č. 101/2000 Sb.). Ovšem pokud jde o zpřístupnění osobních údajů pouze kategorii příjemců (bez jejich individuálního ztotožnění), ve zkoumaném kontextu nemá takové sdělení žádnou vypovídací hodnotu a v podstatě se rovná odepření informace (jako kategorie příjemců mohou být označeni např. potenciální kupující).

- Z výše uvedených důvodů Úřad přehodnotil svůj předchozí přístup k otázce sdělení příjemce informace a dospěl k závěru, že v těchto situacích by mělo být důsledně uplatňováno **právo na přístup subjektu údajů k informacím** (*right of access*) podle § 12 zákona o ochraně osobních údajů. Citované ustanovení uvádí, že požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat. Pravidlem je, že přístup k informaci o příjemci (kategorii příjemců) má být udělen v plném rozsahu, pokud se neuplatní výjimka. Ta může být výslovně stanovena zákonem č. 101/2000 Sb., případně může být ve zvláštním zákoně komplexní úprava poskytování informací o zpracování osobních údajů, což jsou zejména případy státních databází, jako je např. evidence obyvatel. O takové situace se však v případě katastru nemovitostí nejedná, a informace o příjemci informace by tedy měly být poskytnuty.

- **Za vyvážené řešení vztahu ochrany osobních údajů a publicity katastru nemovitostí** lze z hlediska Úřadu považovat, pokud bude nahlížení jako princip možné, avšak osobní údaje budou efektivněji chráněny než dosud. Systémové řešení tohoto problému by mohlo spočívat v poskytování informací z katastru subjektům, u kterých lze doložit právní zájem. Výhledově

lze zvážit toto legislativní řešení. Další variantou řešení by bylo zachování dosavadního práva nahlížet do katastru, ale nikoliv poskytovat listiny s osobními údaji, pakliže není dán právní důvod pro poskytnutí těchto informací. Aktuálně se jeví jako nejsnáze proveditelné výše popsané dílčí opatření, které by realizovalo tzv. právo na přístup podle § 12 odst. 2 zákona č. 101/2000 Sb. Sdělení jména příjemce informace je přitom technicky možné a opatření má význam v tom, že v určitém rozsahu eliminuje okruh osob, které do katastru nahlíží nikoliv s čistými úmysly.

- Nad rámec výše uvedeného Úřad uvádí, že považuje za problematický i samotný institut placeného hlídání změn v katastru jako placené služby. Zastává totiž názor, že pokud státní správa garantuje princip veřejnosti katastru, měla by garantovat i zajištění opatření, která zamezí či omezí zneužívání poskytnutých údajů. Princip veřejnosti by neměl potenciálně znamenat ohrožení vlastnictví jiných osob. Příslušné státní orgány by měly zajistit systematická opatření eliminující nebezpečí zneužití osobních údajů, přičemž tato opatření by měla směřovat ke všem občanům (např. bezplatné zaslání sms zpráv, doručování informací o převodu vlastnictví do vlastních rukou, nikoliv na základě fikce doručení, zamezení přeposílání poštovních zásilek pouze na základě telefonického ohlášení změny adresy).

Závěrem lze shrnout změny, které mohou být v oblasti katastru nemovitostí potenciálně žádoucí z pohledu ochrany osobních údajů:
– listinné dokumenty by měly být poskytovány jen těm subjektům, které mají oprávněný zájem (zde by se jednalo o změnu právní úpravy);
– subjekt údajů by měl dostat informaci o zpracování jeho osobních údajů poskytnutých příjemci údajů (lze na základě stávající právní úpravy);
– měly by být anonymizovány osobní údaje v listinných dokumentech;
– měla by být přijata opatření, která učiní nadbytečnými placené služby hlídání změn v katastru nemovitostí.

2. Otázka zveřejňování platů státních úředníků (vyjádření k ústavní stížnosti sp. zn. IV. ÚS 1378/16)

Předmětem ústavní stížnosti byl nesouhlas stěžovatelů s poskytnutím informací o jejich platech na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a návrh na zrušení § 8b téhož zákona. Stěžovatelé dovozovali, že poskytnutí informace o jejich platech je závažným zásahem do jejich soukromí, s nímž nesouhlasí. Úřad byl požádán Ústavním soudem, aby se k návrhu vyjádřil jako ústřední správní úřad pro oblast ochrany osobních údajů. Některé z jeho závěrů k předmětné problematice jsou obsahem následujícího textu:

- Právní úprava otázky zveřejňování platů v orgánech veřejné správy se vyznačuje vysokou mírou citlivosti z hlediska subjektů, o nichž jsou podávány informace, je předmětem odborných diskusí a je provázena značným mediálním zájmem. Ve své podstatě se jedná o střet práva na informace a práva na ochranu osobních údajů. Z hlediska srovnávacího práva obecně platí, že vztah obou dotčených práv, pokud jde o to, kterému z nich dát přednost, může být hodnocen různě a vyskytuje se více variant řešení. Kromě zaujetí kategorického názoru v otázce, zda platy zaměstnanců zveřejnit či nikoliv, existují i kompromisní řešení spočívající ve stano-

vení absolutní hranice příjmu, od které se příjmy zveřejňují, zveřejnění příjmů v závislosti na druhu zastávané funkce či podle složek platu. Lze nicméně konstatovat, že v Evropě převažuje přístup spočívající v nezveřejňování platů konkrétních osob, byť ve střednědobém horizontu se zvyšuje počet zemí, které upřednostnily právo na informace o platu ve vztahu k vedoucím pracovníkům.[1]

- Pokud jde o Českou republiku, přístup ke zveřejňování platů se postupně vyvíjel, a to jak pokud jde o právní úpravu, tak o soudní judikaturu zejména Nejvyššího správního soudu (NSS), která důvody pro přednost postupně shledala jak u práva na ochranu informací, tak u práva na ochranu soukromí. Přijetím rozhodnutí rozšířeného senátu NSS č. j. 8 As 55/2012 dne 22. 10. 2014 došlo ke sjednocení rozporné judikatury, když tento senát zaujal poměrně radikální přístup k otázce zveřejňování platů zaměstnanců ve veřejné správě. Rozšířený senát dospěl k závěru, že plat, mzda či jiné ohodnocení vyplacené z veřejných prostředků jsou v zásadě vždy, až na několik málo výjimek, příjmem veřejných prostředků ve smyslu § 8b zákona č. 106/1999 Sb. Z tohoto důvodu by měly být ve většině případů zveřejněny. Rozhodnutí formulovalo dva okruhy výjimek z povinnosti zveřejňovat výši platů, a to pokud se osoby na činnosti podílí nepřímo a nevýznamně, a dále pokud nevyvstávají pochybnosti, zda jsou prostředky vynakládány hospodárně.

- Úřad pro ochranu osobních údajů respektuje výše uvedené rozhodnutí NSS. Pokud byl ovšem požádán Ústavním soudem o vyjádření k projednávané věci, a mohl tak učinit bez ohledu na platnou judikaturu, považoval za nezbytné upozornit na několik zásadních aspektů, kterým by měla být věnována pozornost v otázce konfliktu mezi právem na informace a právem na ochranu osobních údajů. Těmito hledisky je zejména posouzení vztahu dotčených základních práv na základě testu proporcionality, zohlednění významu práva na soukromí jednotlivce, i pokud je státním zaměstnancem, způsob omezení práva na soukromí, rozsah poskytování konkrétních osobních údajů při zveřejňování platů, případně zohlednění závěrů plynoucích z judikatury ESD.

- Při posuzování je především na místě vyjít z toho, že v případě poskytování informací o platu či odměně státních zaměstnanců jde o střet mezi informační povinností a právem na ochranu soukromí. Ústavní soud v těchto případech obvykle judikuje, že je potřeba s přihlédnutím ke všem okolnostem pečlivě zvážit, zda není jednomu základnímu právu dávána neoprávněně přednost před druhým, přičemž musí být současně šetřeno smyslu a podstaty základních práv (čl. 4 odst. 4 Listiny). K tomuto posouzení se používá **test proporcionality** (posouzení potřebnosti, vhodnosti a proporcionality v užším smyslu).

- V předmětném rozhodnutí NSS sice obecně zmínil, že k posouzení slouží test proporcionality a teoreticky jej popsal, nicméně samotné posouzení na základě tohoto testu neprovedl, když se omezil na konstatování, že je vždy třeba dát přednost jednomu z uvedených práv, v tomto případě právu na informace. Doplnil, že test proporcionality v tomto případě není třeba provádět, neboť jej provedl již zákon. Dále NSS uvedl, že právo na ochranu soukromí není absolutní a může být omezeno, aniž by totéž uvedl o právu na informace. NSS tedy jednostranně upřednostnil právo na informace a nevzal dostatečně v úvahu právo na soukromí.

1 Parlamentní institut: Přístup veřejnosti k platům vysokých úředníků ve vybraných státech. Informační podklad č. 5.3, 24. prosinec 2011.

- Pokud v daném případě nebyl proveden test proporcionality, nemohl být ani minimalizován zásah do práva na ochranu soukromí. Přitom povinné subjekty poskytují při sdělení informace o platu pracovníka i řadu osobních údajů, jimiž jsou nejen výše, účel a podmínky poskytnutých veřejných prostředků, ale také jméno, příjmení, rok narození a obec, kde má příjemce trvalý pobyt. V této souvislosti je třeba poukázat na potenciální nebezpečí zneužití poskytnutí uvedených osobních údajů. Ohrožena může být bezpečnost osob sdělením bydliště, informace mohou být získávány za účelem poškození osoby (informace může např. prostřednictvím mailu požadovat někdo jiný než osoba podepsaná pod žádostí) či informace mohou být zneužity v pracovněprávních vztazích k získání pracovníka, jemuž je nabídnut vyšší plat.

Úřad závěrem *pro futuro* navrhl, že **východiskem pro posuzování, zda je osobní údaje potřebné poskytnout, by mohl být důsledně účel práva na svobodný přístup k informacím, jímž je *řádné, účelné a hospodárné používání veřejných prostředků***. Toto kritérium se také používá v judikatuře ESD. Uvedeného cíle by bylo možné v řadě případů dosáhnout podrobným zveřejňováním relevantních informací v předem předepsané struktuře, aniž by musely být zveřejňovány osobní údaje zaměstnanců, jako je např. rok narození nebo bydliště.

3. **Přístup k údajům v archivech (vyjádření k ústavní stížnosti Pl. ÚS 3/14)**
Úřad poskytl na žádost Ústavního soudu stanovisko k ústavní stížnosti zahájené na návrh Nejvyššího soudu ČR, v níž bylo požadováno vyslovení protiústavnosti § 37 odst. 11 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (§ 37 odst. 6 ve znění účinném do 30. června 2009). Podle tohoto ustanovení se na archiválie vzniklé před 1. lednem 1990 z činnosti vojenských soudů a prokuratur všech stupňů, bezpečnostních složek podle zákona o Ústavu pro studium totalitních režimů a o Archivu bezpečnostních složek, jakož i mimořádných lidových soudů, Státního soudu, Národního soudu a společenských organizací a politických stran sdružených v Národní frontě, případně z činnosti dalších subjektů citovaných v zákoně, vztahuje výjimka spočívající v tom, že k jejich použití není požadován předchozí písemný souhlas osoby, k níž se archiválie vztahují.

- Úřad zaujal v uvedených souvislostech stanovisko, že z pohledu ochrany osobních údajů je proces zpřístupnění dokumentů se vztahem k minulosti zpracováním osobních údajů se specifickým účelem, kterým je významný společenský zájem vyrovnání se s minulostí. V tomto procesu hrají zásadní roli konkrétní informace o různých osobách, situacích a způsobu rozhodování v totalitním režimu. Mnohé osobní údaje byly represivními složkami totalitního státu shromažďovány a zpracovávány metodami neslučitelnými se zásadami právního státu, mají specifickou vypovídací hodnotu a jsou nezbytné k poznání minulosti. Jejich společným jmenovatelem je dokumentování povahy, fungování a metod používaných totalitním režimem.

- Z hlediska časového lze konstatovat, že citlivost a zneužitelnost archivních materiálů klesá, a tím se také snižuje riziko zásahů do soukromí dotčených osob. Skutečnost, že řadu informací nelze, nejen pro časový odstup, ale i kvůli dobovým metodám práce, spolehlivě ověřit či vyvrátit, vyvažuje demokratický právní režim, v němž je s dokumenty a údaji z totalitního režimu zacházeno zásadně odlišně než s aktuálními osobními údaji občanů zpracovávanými dnes veřejnou správou. Uvedené se týká i údajů o odsouzení, které je dnes nutno v případě

politických a zpolitizovaných trestných činů nahlížet optikou rehabilitačních zákonů (informace o odsouzení získaná ze spisu Státní bezpečnosti nemá význam obdobný výpisu či opisu z Rejstříku trestů).

- Dále Úřad v uvedených souvislostech ve svém doplňujícím stanovisku k ústavní stížnosti upozornil na relevantní text vztahující se k problematice archivů v již platném Nařízení Evropského parlamentu a Rady (EU) 2016/679/ES ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti a se zpracováním osobních údajů a o volném pohybu těchto údajů, které bude účinné od 25. května 2018. Nařízení ve své preambuli na rozdíl od dosud platné směrnice Evropského parlamentu a Rady (EU) 95/46/ES výslovně připouští výjimku z režimu zpracování osobních údajů v archivech ve vztahu k poskytnutí informací souvisejících s politickým chováním za bývalých totalitních režimů. Odstavec č. 158 preambule uvádí, že „**členské státy by rovněž měly mít možnost stanovit, že osobní údaje mohou být dále zpracovávány pro účely archivace, například s cílem poskytnout konkrétní informace související s politickým chováním za bývalých totalitních režimů**, s genocidou, zločiny proti lidskosti, zejména holocaustem, nebo válečnými zločiny". Podle Úřadu by Ústavní soud měl vzít v úvahu výše uvedenou možnost při posuzování předmětné problematiky.

Úřad uzavřel, že zrušení napadeného ustanovení by prakticky znamenalo, že archiválie, včetně těch, které se zabývají obdobím nesvobody před rokem 1989, by nemohly být zpřístupněné badatelům. Prakticky by se tak zastavilo historické bádání o tomto období dějin, přičemž toto bádání má svůj zcela neopomenutelný význam zejména z hlediska poučení příštích generací a jejich výchovy k demokracii a hodnotám právního státu.

4. **Ochrana osobních údajů při využívání elektronických karet ve veřejné dopravě**

Právní otázky spojené s ochranou soukromí a osobních údajů hrají stále významnější roli při vývoji systémů integrovaných/interoperabilních inteligentních jízdenek. S tím, jak se inteligentní karty používají na více místech a je na nich uloženo stále více dat, jsou osobní údaje potenciálně dostupné většímu počtu osob a organizací. Podnikatelské subjekty spravující karty mohou často monitorovat cestovní chování jednotlivých uživatelů služby. Tyto informace mohou být využívány ke zlepšení přepravních tras a cestovních řádů, ale obecně mohou být použity bez výslovného souhlasu zákazníka také pro marketingové, případně jiné účely. S ohledem na to je od vlastníků systémů požadováno splnění velkého počtu technických a procedurálních opatření na ochranu soukromí a osobních údajů zákazníků. Kromě toho se jeví jako užitečné dodržovat určité obecné zásady, k nimž dospěly i některé mezinárodní organizace nebo jejich pracovní skupiny zabývající se touto problematikou (např. Pracovní skupina podle článku 29, případně v jejím rámci speciální skupina pro e-jízdenky v městské hromadné dopravě). Obecně je doporučováno, aby z hlediska posouzení dopadů na ochranu osobních údajů byly informační systémy dopravních společností navrženy a realizovány tak, aby braly v úvahu právo zákazníků na ochranu jejich osobních údajů prostřednictvím dodržování principů, jako je anonymita, transparentnost, minimalizace dat a doby uchovávání, viz níže:

• *Anonymita*

Subjekty provozující elektronické karty by měly nabídnout alternativní způsoby, aby zákazníci mohli cestovat anonymně (bez zbytečných překážek), např. při zaplacení v hotovosti nebo na základě anonymního elektronického lístku. Pokud není anonymita z technických důvodů možná, měla by být dodržena následující doporučení:

• *Ochrana osobních údajů a transparentnost*

Výše uvedené subjekty by měly při používání systémů elektronických jízdenek poskytnout subjektům údajů jednoznačné informace o zpracování osobních údajů, které provádějí. Měl by být brán ohled na subjekty údajů, aby snadno porozuměly konkrétním účelům sledovaným těmito společnostmi, věděly, jaké druhy osobních informací jsou o nich shromažďovány a ukládány, a jak jsou tyto informace používány.

• *Minimalizace dat a doba uchovávání*

Co se týče konkrétně zpracování údajů týkajících se pohybu uživatelů, informační systémy subjektů provozujících elektronické karty by měly být navrženy a realizovány s pomocí přednostního využívání anonymních dat. Používají-li (přímo či nepřímo) identifikovatelné informace, informace by měly být uloženy nejkratší možnou dobu a poté automaticky vymazány (informace by zpravidla neměly být uchovávány po dobu delší než několik dní po uložení) a mělo by být přihlédnuto k zákonným účelům, kterých má být dosaženo prostřednictvím zpracování údajů.

• *Bezpečnost*

Zabezpečení přístupu k osobním údajům by mělo obsahovat kontrolní systém, který by zakazoval zneužití informací. Subjekty provozující elektronické karty by měly zajistit ochranu soukromí registrovaných uživatelů při zpřístupňování svých databází obchodním partnerům nebo dokonce i vlastním zaměstnancům.

Legislativní činnost

OBECNĚ

I v roce 2016 ÚOOÚ pokračoval v politice transparentnosti a zveřejňoval důležitá stanoviska k návrhům právních předpisů a vládních koncepčních dokumentů na webu Úřadu; na nejdůležitější upozornil též v novinkách na hlavní stránce – k NZIS, podpoře sportu, III. koncepční novele nového zákoníku práce, evidenci obyvatel a rodným číslům, DNA, blahopřání jubilantům obcemi, ČOI a trestní odpovědnosti právnických osob.

Celkem 20 příspěvků zveřejněných k návrhům právních předpisů lze zobecnit takto:

- Pokračuje trend přechodu od listin k elektronickým dokumentům. Je však komplikován tím, že řada elektronických dokumentů nejsou strukturované texty („strojově čitelné", jak zní *terminus technicus* EU), nýbrž pouhé obrázky. V roce 2016 nabylo účinnosti nařízení eIDAS (CELEX 32014R0910) a jeho prováděcí zákon (č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce).
- Spíše neblahým trendem je, že stále více dozorových úřadů si přeje přejímat pravomoci policie, zejména možnost skrytého sledování či zřízení tajného agenta, a to bez povolení soudu. ÚOOÚ se domnívá, že dozorové úřady mají fungovat otevřeně, expertně řešit zejména systémové (koncepční) problémy, a že boj s trestnou činností má zůstat Policii České republiky.
- U několika rezortů přetrvává stav, že ÚOOÚ je opomíjen jako povinné připomínkové místo. ÚOOÚ tato pochybení vyhodnocuje a dotčené rezorty žádá o zlepšení spolupráce, aby byl zcela naplněn již platný, ale zatím neúčinný, článek 36 odst. 4 GDPR: *„Členské státy konzultují s dozorovým úřadem během přípravy návrhu legislativního opatření, které má přijmout vnitrostátní parlament, nebo návrhu regulačního opatření založeného na takovém legislativním opatření, jež souvisí se zpracováním."*

Bodem 4 usnesení vlády č. 820 ze dne 14. listopadu 2012 bylo s účinností od 1. ledna 2013 zavedeno pro věcné záměry zákonů a návrhy všech celostátních právních předpisů (zákonů, vládních nařízení a vyhlášek) zhodnocení současného

stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů (DPIA). Trvalé upozorňování na smysl a náležitosti DPIA nebo opakované vysvětlování DPIA se v roce 2016 již u některých nejvyšších správních úřadů příznivě projevilo, např. obecně u **Státního úřadu pro jadernou bezpečnost** nebo konkrétně u návrhu novely **zákona o stavebním spoření** z pera ministerstva financí.

Příklady DPIA

Předkladatel někdy DPIA odbude formálním konstatováním, protože věcně nesprávně určí rozsah návrhem dotčeného zpracování osobních údajů, a to i u návrhů, které zakládají rozsáhlá zpracování osobních údajů. Např. v návrhu změny **nového trestního zákoníku** pro boj s financováním a podporou terorismu, rasismu, xenofobie a jiné nesnášenlivosti, ministerstvo spravedlnosti uvedlo, že *„návrh v této oblasti stávající úpravu nikterak nemění, dopady na problematiku ochrany soukromí a osobních údajů se nepředpokládají"*. Ve skutečnosti skutková podstata trestného činu podněcování k nenávisti nebo násilí vůči skupině osob nebo k omezování jejich práv a svobod nově definovaná v § 356 odst. 1 dopadne společně s trestní represí na ochranu citlivých údajů; týká se to jakéhokoli nakládání s takovými osobními údaji, a to bez ohledu na jejich věcnou správnost. Trestněprávní ochrana má být nově výslovně poskytnuta i jednotlivci a je rozšířen a i jinak zpřesněn výčet citlivých údajů, které jsou před nakládáním v rámci účelů definovaných samotným označením skutkové podstaty trestného činu chráněny.

DPIA je důležité také pro členy zákonodárného sboru – bez něho je prakticky vyloučeno dovodit důsledky budoucího zpracování osobních údajů a jeho napojení na jiná zpracování. Příkladem je návrh novely **zákona o občanských průkazech**. V závěrečné zprávě z hodnocení dopadů regulace (RIA) nebyly identifikovány žádné, v obecné části důvodové zprávy pouze pozitivní, dopady, ačkoliv návrh zákona ve skutečnosti na negativní důsledky zčásti reagoval. Jedním z přímých důsledků je, že držitel občanského průkazu se strojově čitelnými údaji a kontaktním elektronickým čipem bude nově muset občanský průkaz chránit před rizikem ohrožení dat v identifikačním certifikátu v kontaktním elektronickém čipu. Toto ohrožení vede ke zneplatnění občanského průkazu a vyžaduje vydání nového občanského průkazu, jež je zpoplatněno. Přitom platí, že možnosti držitele chránit data v identifikačním certifikátu jsou omezené, pokud bude občanský průkaz používat na základě nových ustanovení zákona o informačních systémech veřejné správy a daňového řádu. Některým z toho vyplývajícím rizikům ohrožení není držitel schopen čelit a ani to po něm nelze spravedlivě požadovat. Dosah a význam důsledků pro všechny, kdo mají povinnost občanský průkaz se strojově čitelnými údaji a kontaktním elektronickým čipem mít, je umocněn tím, že povinnost mají všichni občané, kteří dosáhli věku 15 let, a že ho mohou mít i občané, jejichž svéprávnost byla omezena. Dále je třeba určit důsledky plynoucí z uvedeného ohrožení pro držitele, byť se projeví a materializují mimo věcnou působnost přímo novelizovaného zákona.

V roce 2016 nabyl účinnosti problematický § 20 **zákona o ochraně spotřebitele**, zakotvující informační databázi o bonitě a důvěryhodnosti spotřebitele ze zákona. Je potvrzením toho, že opomíjení ochrany osobních údajů a DPIA je problémem iniciativních (poslaneckých, senátních a krajských) návrhů zákonů obecně.

U sedmi návrhů **mezinárodních smluv**, které byly předloženy k posouzení v různých fázích sjednávání, např. úmluvy Rady Evropy o boji proti manipulaci se sportovními soutěžemi, bylo konstatováno plné respektování zásad ochrany osobních údajů a pouze k jedné z nich byla vznesena dílčí připomínka.

Veřejný pořádek

Zvláště významným byl návrh zákona nepřehledně označený jako „*kterým se mění zákon o Policii České republiky a zákon o Generální inspekci bezpečnostních sborů*", tedy návrh zákona o (národní databázi) **DNA**. Návrh pouze legalizuje současný stav, tedy jednostranně upřednostňuje bezpečnostní hledisko nad ochranou soukromí. ÚOOÚ nemůže souhlasit s enormním rozsahem národní databáze DNA (všechny úmyslné trestné činy, kromě čtyř přečinů, místo takových, kde je biologická stopa, tj. u násilné, majetkové a mravnostní trestné činnosti), enormní dobou uchování (až 80 let od spáchání trestného činu) a přetrvávání zásadní věcné chyby („budoucí identifikace") v zákoně o policii.

Národní bezpečnost

U návrhu novely **zákona o Vojenském zpravodajství** ÚOOÚ požadoval, kromě jiného, návrh doplnit a rozšířit o ustanovení zakotvující dozor nad zpracováním osobních údajů zpravodajskými službami České republiky. Důvodem bylo, že návrh zákona rozšiřuje primární přístup k provozním a lokalizačním údajům vznikajícím z provozu sítí a služeb elektronických komunikací v oblasti, která je explicitně vyňata z dozorové působnosti ÚOOÚ. Ministerstvo obrany připomínce nevyhovělo. Přitom však reformu dozoru nad zpravodajskými službami navrhl úřad vlády v návrhu novely **zákona o zpravodajských službách České republiky**. Předlohu však opomněl zaslat na ÚOOÚ k vyjádření.

Potřeba stálého a kompetentního dozoru nad zpracováním osobních údajů je přitom 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.

ÚOOÚ se podílel na transpozici směrnice 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (**směrnice o NIS**). Nebyly identifikovány problémy ve vztahu k ochraně osobních údajů. Klíčové v praxi bude vyřešit koordinaci ohlašování případů porušení zabezpečení osobních údajů podle článku 33 GDPR, oznámení narušení bezpečnosti osobních údajů podle článku 3 odst. 3 směrnice o soukromí a elektronických komunikacích a ohlášení incidentů se závažným dopadem na kontinuitu základních služeb podle článku 14 odst. 3 směrnice o NIS.

Kvalifikace a podnikání

U návrhu novely **zákona o uznávání výsledků dalšího vzdělávání** DPIA obsahovalo meritorně nesprávné hodnocení vztahu k ochraně osobních údajů. Tam, kde je zakládán informační systém veřejné správy zpracovávající osobní údaje žadatelů a uchazečů, nelze bez další argumentace konstatovat, že „*návrh se dotýká oblasti ochrany soukromí a nakládání s osobními údaji pouze okrajově*". Zatímco účel zpracování veškerých údajů a rozsah zpracovávaných údajů byly vymezeny dostatečně, uchovací doba a přístupnost údajů z jednotlivých evidencí zahrnovaných do zakládaného informačního systému jako „součásti" nebyly upraveny ani implicitně. Obojí je přitom zásadní náležitostí každého zpracování osobních údajů, mj. i jako informace pro subjekty údajů a rámec pro uplatňování jejich oprávnění. Veřejná správa by rovněž měla být transparentní.

ÚOOÚ se podařilo dosáhnout shody s ministerstvem průmyslu a obchodu nad návrhem novely **živnostenského zákona**. Živnostenské úřady sice budou poskytovat sestavy z živnostenského rejstříku, ale tyto sestavy bude zakázáno dále publikovat. MPO rovněž vyhodnotí svou praxi nahlížení do spisů o trestním odsouzení.

6 Vyřizování stížností podle § 175 správního řádu

V souladu s § 175 zákona č. 500/2004 Sb., správní řád, mají dotčené osoby zákonem stanovené právo obrátit se na správní orgán se stížností, pokud se domnívají, že správní orgán postupoval nesprávně, nebo s podnětem na nevhodné chování úředních osob. Ustanovení § 175 zákona č. 500/2004 Sb. je institut, který slouží k ochraně práv dotčených osob pro případ, že jim zákon neposkytuje jiný prostředek ochrany, kterým se míní zejména odvolání nebo další řádné či mimořádné opravné prostředky.

Stížnostmi podle § 175 zákona č. 500/2004 Sb. se Úřad zabýval i v roce 2016, ve kterém vyřídil celkem 33 stížností. Ve většině případů stěžovatelé vyslovili nesouhlas s vyřízením jejich předchozího podnětu adresovaného Úřadu, ve kterém bylo ze strany stěžovatelů vzneseno podezření z nezákonného zpracování osobních údajů. Tyto podněty byly vyhodnoceny a následně řešeny jako stížnost podle § 175 zákona č. 500/2004 Sb. Z celkového počtu těchto stížností byly 2 posouzeny jako důvodné a 11 stížností bylo posouzeno jako částečně důvodné. Zbylých 18 stížností bylo shledáno bezdůvodnými. Při porovnání celkového počtu stížností s předchozím rokem lze konstatovat, že celkový počet stížností nepatrně klesl.

Dvacet stížností směřovalo proti postupu odboru pro styk s veřejností, jehož náplní je vyřizovat stížnosti a podněty, které jsou Úřadu adresovány. Převážná většina stížností byla ze strany stěžovatelů podána z důvodu jejich nesouhlasu s vyřízením předchozího podnětu, kdy byl podnět odborem pro styk s veřejností odložen bez dalšího opatření. Pokud stěžovatel podá stížnost podle ustanovení § 175 zákona č. 500/2004 Sb., dochází pak k prošetření jeho předchozího podnětu a způsobu jeho vyřízení ze strany uvedeného útvaru. V případě odboru pro styk s veřejností byly analytickým oddělením 2 stížnosti posouzeny jako důvodné a 6 stížností jako částečně důvodné. Zbylých 12 stížností bylo posouzeno jako bezdůvodné. V případě, že po přezkoumání podnětu stěžovatele

bylo shledáno podezření z porušení zákona č. 101/2000 Sb., následoval zákonem stanovený postup, kdy tyto podněty jsou postoupeny buď inspektorovi Úřadu k provedení kontroly, nebo oddělení správních činností k zahájení správního řízení pro podezření ze spáchání správního deliktu či přestupku.

Ve třech případech se stěžovatelé na Úřad obrátili se stížností proti postupu oddělení správních činností, přičemž ve všech případech byly dané stížnosti posouzeny jako bezdůvodné.

V deseti případech se stěžovatelé obrátili na Úřad se stížností proti závěrům kontrolních postupů Úřadu nebo postupu při vedení kontroly inspektory Úřadu, kdy z tohoto celkového počtu bylo 5 stížností posouzeno jako částečně důvodné a 3 stížnosti jako bezdůvodné. Ve výše uvedených případech byl stěžovatel informován o výsledku šetření, příp. zjištěném pochybení a dalším postupu v dané konkrétní věci. Dvě stížnosti Úřad obdržel na konci roku 2016 a bude se jimi zabývat v roce 2017.

Ve všech případech byl příslušný útvar Úřadu informován o vyřízení stížnosti, a pokud byl jeho postup shledán nesprávným nebo částečně nesprávným, byl vyzván k tomu, aby přijal taková opatření, aby v obdobných případech již nedocházelo ke stejnému pochybení.

Úřad obdržel v roce 2016 několik stížností podnikatelů, že držitelé doménových jmen v rámci své činnosti nakládají s jejich osobními údaji, aniž by k tomu byl udělen ze strany podnikatelů souhlas. Tyto osobní údaje jsou totožné s údaji obsaženými ve veřejně dostupném živnostenském rejstříku. Veřejnost části údajů z rejstříku, tj. také širokou dostupnost v prostředí internetu, stanoví zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon). V případě, že se jedná o kopírování osobních údajů uvedených ve veřejné části živnostenského rejstříku a následné zveřejnění na doménách, které daného podnikatele nepoškozují, informují o podnikatelích v České republice, není tento postup v rozporu s právním titulem uvedeným v § 5 odst. 2 písm. d) zákona č. 101/2000 Sb., který dovoluje dále zpracovávat údaje, oprávněně zveřejněné v souladu se zvláštním předpisem, tedy s živnostenským zákonem. Úřad, vědom si závažnosti uvedeného problému, kdy právní úprava otevírá prostor pro další zpracování a komerční využívání údajů, zaslal připomínky gestorovi právní úpravy živnostenského rejstříku, Ministerstvu průmyslu a obchodu. V připomínkách bylo mj. uvedeno: *„ÚOOÚ má řadu stížností podnikatelů na soukromoprávní kopie živnostenského rejstříku, které jsou indexovány v internetovském vyhledávači, takže veřejnosti i bez cílené žádosti zpřístupňují všechny identifikační údaje podnikatelů – fyzických osob, nikoliv jen na základě úmyslného dotazu, jak by bylo žádoucí. Na základě privátní autonomie, tedy toho, že podnikatel je vlastníkem údajů, které o něm veřejná správa zpracovává, by měl být umožněn opt out z takového předávání. Jako nejvhodnější řešení pro nově zapisované podnikatele se jeví zřízení seznamu „robinsonů" podle § 5 odst. 9 zákona o ochraně osobních údajů, kde by již při zápisu podnikatele mu bylo dáno na výběr, zda si přeje či nepřeje umožnit předávání svých údajů soukromému sektoru. U stávajících podnikatelů by to měla být nová žádost o opt out."* Existují i případy, kdy jsou osobní údaje podnikatelů dále využívány ke komerčním účelům. Tímto problémem se Úřad v současné době zabývá a analyzuje zákonnost takových postupů.

Tak jako v předchozím roce ani jeden z celkového počtu 33 podnětů, které Úřad obdržel od stěžovatelů, nesměřoval proti nevhodnému chování úředních osob. Na základě tohoto zjištění je možné konstatovat, že Úřad při vyřizování podaných podnětů, kontrolní činnosti i ve správním řízení komunikuje s veřejností při ochraně jejích práv a právem chráněných zájmů na profesionální úrovni a v souladu s principy dobré správy.

Styky se zahraničím a mezinárodní spolupráce

V oblasti zahraniční spolupráce se Úřad soustředil především na činnost v rámci Pracovní skupiny podle článku 29 (WP29), která je poradním orgánem Evropské komise pro otázky ochrany osobních údajů. V tomto roce se Úřad rozhodl posílit přímé zastoupení ve vybraných podskupinách WP29. Specialisté Úřadu tak pracují v těchto formacích:

Podskupina pro spolupráci – byla zřízena v souvislosti s přípravou na Obecné nařízení o ochraně osobních údajů a řeší otázky budoucí spolupráce mezi úřady, kterou toto nařízení posiluje zavedením nových mechanismů součinnosti, především na poli řešení stížností a šetření případů s mezinárodním aspektem.

Podskupina pro technologie – zabývá se vlivem nových technologií na soukromí jednotlivce a jejich soulad s předpisy na ochranu osobních údajů.

Podskupina pro mezinárodní předávání – řeší problematiku mezinárodních toků dat.

Podskupina pro hranice, cestování a vynucování práva – zabývá se hlavně vlivem různých bezpečnostních technologií a opatření na ochranu osobních údajů.

Podskupina pro e-government – řeší otázky ochrany osobních údajů při elektronizaci státní správy.

Podskupina pro klíčová ustanovení směrnice 95/46/ES – pracuje na legislativních otázkách přechodu od dosavadní směrnice 95/46/ES na nově schválené Obecné nařízení o ochraně osobních údajů, které ji v květnu 2018 nahradí.

Kromě toho je Úřad zastupován přímo předsedkyní na pravidelných plenárních zasedáních.

Úřad rozvíjel také bilaterální spolupráci s partnerskými úřady. Především to bylo formou konzultací konkrétních témat korespondenční formou. Počátkem listopadu proběhla v Praze dvoudenní pracovní schůzka se zástupci partnerského úřadu z Maďarska. Jednání se zaměřilo na dvě hlavní témata: svobodný přístup k informacím versus ochrana osobních údajů a praktické kroky pro období přechodu na Obecné nařízení o ochraně osobních údajů.

Kromě různých jednorázových akcí se zástupci Úřadu účastnili těchto vybraných, každoročně pořádaných mezinárodních konferencí:

- Setkání úřadů ze zemí střední a východní Evropy – Sarajevo, květen 2016
  Na programu byla témata: kamerové sledování, ochrana soukromí na pracovišti, zpracování biometrických dat.
- Jarní konference komisařů ochrany dat – Budapešť, květen 2016
  Dvoudennímu zasedání dominovalo téma právě schváleného Obecného nařízení o ochraně osobních údajů.
- Seminář k výměně zkušeností z dozorové činnosti – Podgorica, říjen 2016
  Akce je tradičně zaměřena na diskusi o praktických poznatcích z oblasti kontroly, řešení stížností a sankcionování.
- Mezinárodní konference komisařů ochrany dat a soukromí – Marrakeš, říjen 2016
  Nosným tématem byla umělá inteligence a její dopady do soukromí jednotlivce.
- Specialista na legislativu se jako lektor účastnil dvoudenního semináře o ochraně osobních údajů v systému sociálního zabezpečení. Akce financovaná Evropskou komisí prostřednictvím kanceláře TAIEX proběhla v září v Ankaře.

Pokračovala i aktivní účast ve Společném kontrolním orgánu Europolu, který je samostatným dozorovým orgánem zástupců států zapojených do fungování Evropského policejního úřadu. Zástupce Úřadu se mj. podílel na kontrolách v sídle Europolu v Haagu.

Úřad, sdělovací prostředky a komunikační nástroje

Z hlediska mediálního zájmu o činnost Úřadu měl rok 2016 dva hlavní vrcholy. První byl spojen s vydáním lednového stanoviska č. 1/2016 – Umístění kamerových systémů v bytových domech. Na základě dosavadní praxe Úřad přehodnotil a sjednotil podmínky pro kamerové sledování v případech, které nevyvolávají zásadní problémy a při splnění všech daných pravidel nezasahují nepatřičně do soukromí. Především bylo třeba vysvětlovat, že využití základního právního důvodu pro pořizování kamerového záznamu v bytovém domě, kterým je ochrana práv a právem chráněných zájmů (ochrana zdraví, ochrana majetku před vandalismem), není založeno na souhlasu obyvatel domu s pořízením a uchováváním záznamu, tedy, jednoduše řečeno, že SVJ nebo bytové družstvo žádné souhlasy v takovém případě nepotřebuje. Musí ovšem plnit ve stanovisku uvedené podmínky, zejména důkladné zabezpečení kamerových systémů. Občasné dezinterpretace objevující se také v médiích se podařilo eliminovat.

Druhým vrcholem, s nímž byl spojen největší zájem médií, se stalo koncem června zahájené správní řízení se společností T-Mobile Czech Republic a.s. v souvislosti s odcizením zákaznických dat. Úřad v něm konstatoval, že považuje za prokázané, že společnost jako správce osobních údajů svých klientů nepřijala dostatečná opatření k zabezpečení osobních údajů obsažených v elektronické interní databázi, která obsahovala osobní údaje zhruba 1,2 milionů zákazníků – fyzických osob. V důsledku nepřijetí dostatečných opatření došlo k odcizení uvedených dat jejím zaměstnancem. Společnost tím porušila povinnost přijmout taková opatření, 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, a tím spáchala správní delikt. Kauzu vzhledem k jejímu charakteru a také uložené pokutě 3,6 mil. Kč, tedy vůbec nejvyšší Úřadem uložené pokutě, veřejnosti přiblížil v menším či větším rozsahu skutečně široký okruh médií, ať už tištěných, audiovizuálních nebo elektronických. Dělo se tak ve věcné, informativní rovině.

V průběhu roku média zaregistrovala další témata se vztahem k Úřadu a o nichž Úřad informoval. Jednalo se například o diskuze kolem novely zákona o zdravotních službách, problematiku nahlížení do archivních materiálů StB, rozhodnutí Nejvyššího správního soudu ve věci ekolo, ke konci roku také problematiku DIČ na účtenkách EET. Z širšího hlediska zájmu médií o problematiku ochrany osobních údajů je možné zmínit zejména Evropskou komisí schválený nový nástroj pro předávání dat do USA, tzv. štít EU-USA na ochranu soukromí. V neposlední řadě to bylo v květnu v Úředním věstníku Evropské unie zveřejněné obecné nařízení o ochraně osobních údajů, na jehož přípravě se Česká republika od roku 2012 podílela a které nabude účinnosti v členských státech EU v květnu 2018.

ŠÍŘENÍ ZNALOSTÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

V květnu Úřad uspořádal ve spolupráci s Právnickou fakultou Univerzity Karlovy mezinárodní konferenci na téma práva na informační sebeurčení, kterému nebyla dosud v ČR věnována samostatná konference. Uvedené téma má přitom zcela zásadní význam v souvislosti s rozmachem moderních informačních technologií. Předsedkyně Úřadu pro ochranu osobních údajů JUDr. Ivana Janů v úvodním slovu zdůraznila význam konference především v rozpracování samotného pojmu práva na informační sebeurčení a nastínění možných interpretací a přístupů, a to zejména v kontextu současného vývoje informačních technologií a připravované změny evropského práva, kterou přináší obecné nařízení o ochraně osobních údajů.

Téma informačního sebeurčení bylo na konferenci zpracováno z různých pohledů, zejména z pohledu teorie, judikatury, ale i praxe. Kvalitu mezinárodní konference zajistila vysoká úroveň přednášejících. Pojem práva na informační sebeurčení v německém právním řádu vysvětlil prof. Dr. Rolf Schwartmann z Technické vysoké školy v Kolíně nad Rýnem, příspěvek na téma Právo na informační sebeurčení a jeho projevy v judikatuře Soudního dvora EU přednesl prof. JUDr. Jiří Malenovský, CSc., soudce Soudního dvora Evropské unie. Dopolední blok zakončil prof. Dr. Michael Ronellenfitsch, emeritní profesor Univerzity v Tübingenu přednáškou Německá praxe práva na informační sebeurčení, se zvláštním důrazem na rozhodování spolkového pověřence pro ochranu dat.

V odpoledním panelu vystoupili emeritní soudce Ústavního soudu prof. JUDr. Pavel Holländer, DrSc., s příspěvkem Právo na informační sebeurčení a jeho projevy v judikatuře ústavního soudu a dva zástupci Úřadu pro ochranu osobních údajů, PhDr. Miroslava Matoušová (Střet práva s realitou) a Mgr. et Mgr. Vít Zvánovec (Informační sebeurčení v kontextu ústavního a občanského práva).

S úvodním projevem vystoupila předsedkyně Úřadu rovněž na konferenci LAW FIT o právu a IT pořádanou Fakultou informačních technologií ČVUT, nad níž převzala záštitu. V červnu Úřad uspořádal ve svém sídle diskuzní kulatý stůl k využívání online kamer a dalších sledovacích zařízení, která zachycují a dále přenášejí obrazové záznamy fyzických osob. Diskuze se zúčastnili experti na ochranu soukromí a ochranu osobních údajů ze soukromého i veřejného sektoru, neziskového sektoru i akademické sféry a zástupci bezpečnostních společností, které online kamery a obdobné sledovací systémy v praxi instalují či provozují. Hlavní otázkou bylo, zda je možné a vhodné i online sledovací systémy chápat jako nástroje pro zpracování osobních údajů a regulovat je v režimu zákona o ochraně osobních údajů, a to mimo jiné s ohledem na medializované případy údajného narušení zabezpečení online kamerových systémů a zveřejnění na internetu. Poznatky k problematice byly shrnuty v dokumentu, který byl následně předložen k odborné diskuzi.

Kulatý stůl k využívání online kamer a dalších sledovacích zařízení, 14. června 2016

V únoru 2016 byla ukončena dvouletá mediální spolupráce, v jejímž rámci bylo publikováno téměř 50 článků a řada videovizitek, jejichž smyslem bylo zvýšit povědomí o ochraně osobních údajů v jednotlivých segmentech a reagovat na aktuální komunikační potřeby Úřadu v době většího dopřávání pozornosti například otázkám bezpečnosti. Všechny příspěvky jsou dostupné rovněž na webových stránkách Úřadu v rubrice Média.

Přednáškové činnosti se v průběhu roku věnovali odborníci z řad zaměstnanců Úřadu. Jednalo se úhrnem o zhruba 25 vystoupení na konferencích nebo samostatných přednášek, a to v mnoha oblastech. Již tradičně se jednalo o kamerové systémy, dále o přednášky pro zástupce obcí, problematiku data breaches, oblast zdravotnictví, ochranu osobních údajů v pracovním právu a další.

V roce 2016 byla vydána a na webových stránkách publikována tři stanoviska Úřadu: již zmiňované stanovisko č. 1/2016 – Umístění kamerových systémů v bytových domech, dále stanovisko č. 2/2016 – Ke zpracování osobních údajů účastníků při poskytování finanční podpory z evropského sociálního fondu a stanovisko č. 3/2016 – Evidence návštěvníků při vstupech do budov a kopírování dokladů. Vydány byly dvě částky Věstníku Úřadu pro ochranu osobních údajů (71 a 72).

Úřad již tradičně věnoval v rámci osvětové činnosti pozornost dětem a mládeži. U příležitosti mezinárodního Dne ochrany osobních údajů, který je připomínán 28. ledna, vyhlásil jubilejní X. ročník soutěže pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!". Vítězové dvou tematických a dvou věkových kategorií byli pozváni ke slavnostnímu ocenění, které jim bylo předáno z rukou předsedkyně JUDr. Ivany Janů. Zvláštní uznání za dlouhodobou práci s dětmi v rámci soutěže získala ZŠ a MŠ Ludgeřovice. Partnery soutěže, kteří se spolupodíleli na předávání informací o soutěži zejména do škol a knihoven, byly časopis Řízení školy, Svaz knihovníků a informačních pracovníků, Český rozhlas a SaferInternet.

Setkání s vítězi X. ročníku soutěže pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“ a jejich doprovodem z řad rodičů a učitelů, 13. června 2016

U příležitosti zahájení školního roku vydal Úřad osvětové letáky určené pro děti a mládež, které jsou v elektronické podobě dostupné rovněž na webových stránkách v rubrice Pro mládež. Letáky byly distribuovány zájemcům z řad základních a středních škol z celé republiky, navázána byla v tomto ohledu také spolupráce s olomouckým Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého. Úřad se stal rovněž partnerem Školního vzdělávacího diáře 2016/2017, do nějž přispěl informacemi o ochraně osobních údajů a soukromí. Diář byl v nákladu 15 tisíc kusů distribuován do škol.

KNIHOVNA ÚŘADU

Knihovna Úřadu čítá 2300 svazků. Funguje jednak jako zázemí pro zaměstnance (nacházejí se zde publikace potřebné pro jejich práci), současně je také prezenčně k dispozici odborné veřejnosti (ať již studentům či odborníkům z praxe) a po telefonické domluvě je možno si návštěvu knihovny domluvit a potřebné materiály si zde prostudovat. V roce 2016 do knihovny přibylo 82 nových titulů, z toho čtyři darem.

WEBOVÉ STRÁNKY ÚŘADU

Webové stránky jsou základním komunikačním nástrojem. Veřejnost má jejich prostřednictvím možnost seznámit se s činností Úřadu v jednotlivých oblastech jeho působnosti. V roce 2016 byla zásadním způsobem doplněna rubrika Poradna, přičemž smyslem bylo jednoduchým a dostupným způsobem zpřístupnit těm, kteří se v nejrůznějších životních situacích dostanou do

styku s problematikou ochrany osobních údajů, přehledné údaje o tom, jak postupovat. Jedná se například o informace, jakým způsobem je možné požádat správce osobních údajů o vysvětlení určité situace a vyzvat jej k nápravě, jak postupovat v případě problémů s údaji na internetu, jak je možné bránit se zveřejnění citlivých nahrávek, jak je možné zažádat o opravu či odstranění údajů, ale také o uvedení případů, které Úřad z hlediska své kompetence není oprávněn řešit.

Nově byla zřízena rubrika Obecné nařízení EU, do níž jsou, a i nadále budou, doplňovány všechny relevantní informace k obecnému nařízení o ochraně osobních údajů. Vedle textu nařízení a základních údajů je zde k dispozici rejstřík k obecnému nařízení, převodní tabulka mezi zákonem o ochraně osobních údajů a obecným nařízením o ochraně osobních údajů a také obsah nařízení. Vypracované obsahy byly na webových stránkách doplněny rovněž k dalším vybraným právním předpisům. Souvislý přehled s podrobnými informacemi o kontrolách je nově průběžně zveřejňován v rubrice Dozorová činnost. Připravována je mobilní verze webu, se střednědobým výhledem pro přípravu responzivního webu.

Informační systém ORG

Rokem 2016 vstoupil informační systém ORG, který spravuje Úřad pro ochranu osobních údajů, již do pátého roku provozu. Informační systém ORG je částí Systému základních registrů a propojuje zbývající registry systému.

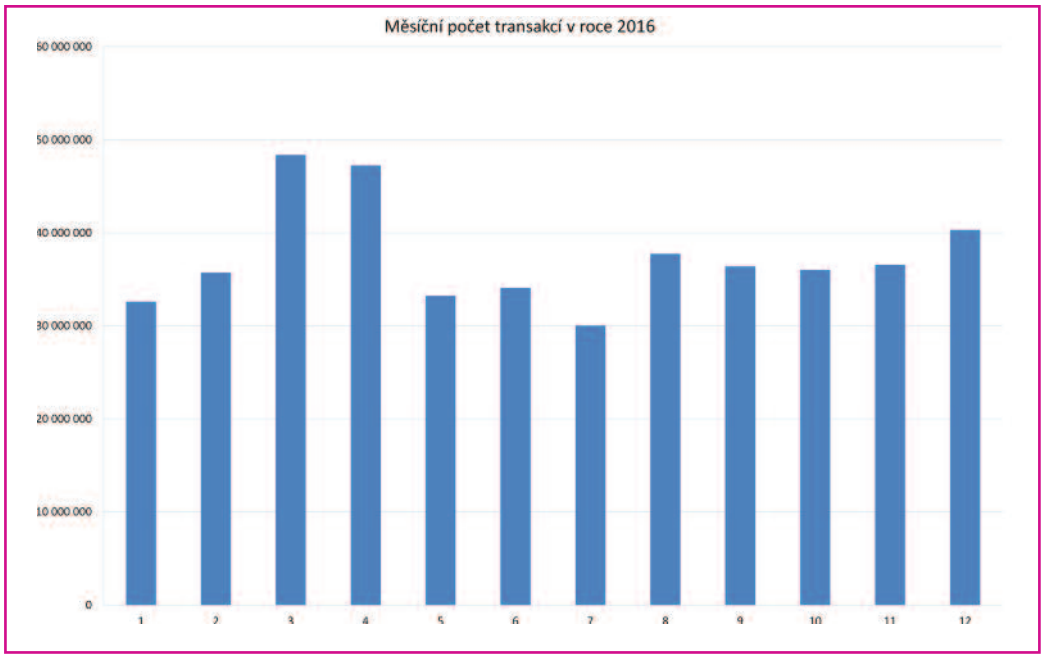
Informační systém ORG vznikl na základě zákona č. 111/2009 Sb., o základních registrech, a přinesl Úřadu úkol zajistit bezpečnou identifikaci občanů v systému Základních registrů prostřednictvím zdrojových a agendových identifikátorů fyzických osob. Informační systém ORG šifrovaně vytváří a překládá agendové identifikátory z jedné agendy do agendy druhé a vede jejich seznam.

Základní registry obsahují aktuální referenční údaje o občanech, právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci a zjednodušují tak komunikaci občanů s úřady. Systém základních registrů ukládá potřebné údaje do registrů. Údaje z těchto registrů jsou pak přístupné oprávněným osobám po celé republice. Pro zvýšení bezpečnosti a ochrany dat spravují jednotlivé registry různé orgány a úřady. Fyzické uložení dat je z bezpečnostních důvodů na různých místech České republiky.

Protože je kladen mimořádný důraz na bezpečnost, kvalitu, rychlost a spolehlivost spojení jednotlivých částí, není Systém základních registrů centralizován na jednom místě. Při nedostupnosti registru ORG by byl ochromen chod celého systému s dopadem na spokojenost koncových uživatelů a jejich klientů.

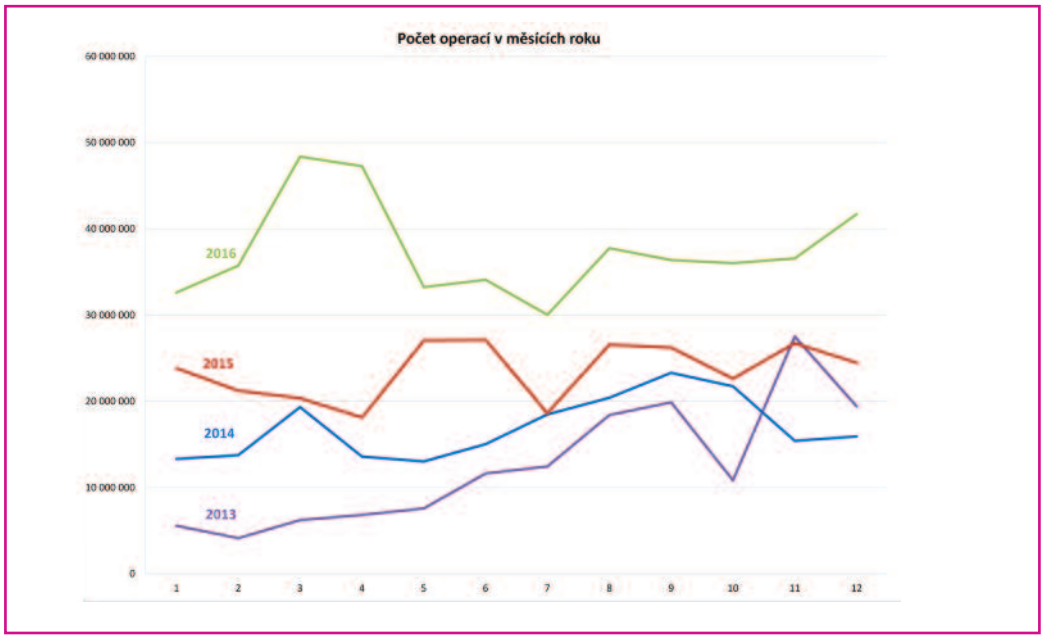
Informační systém ORG je využíván hlavně orgány veřejné správy a zjednodušuje komunikaci mezi občany a úřady. V provozu je 24 hodin denně, 7 dní v týdnu.

Na dalším grafu jsou počty transakcí v jednotlivých měsících roku 2016. Maximální zatížení bylo v jarních měsících březen a duben. Nárůst oproti únoru je 35%.



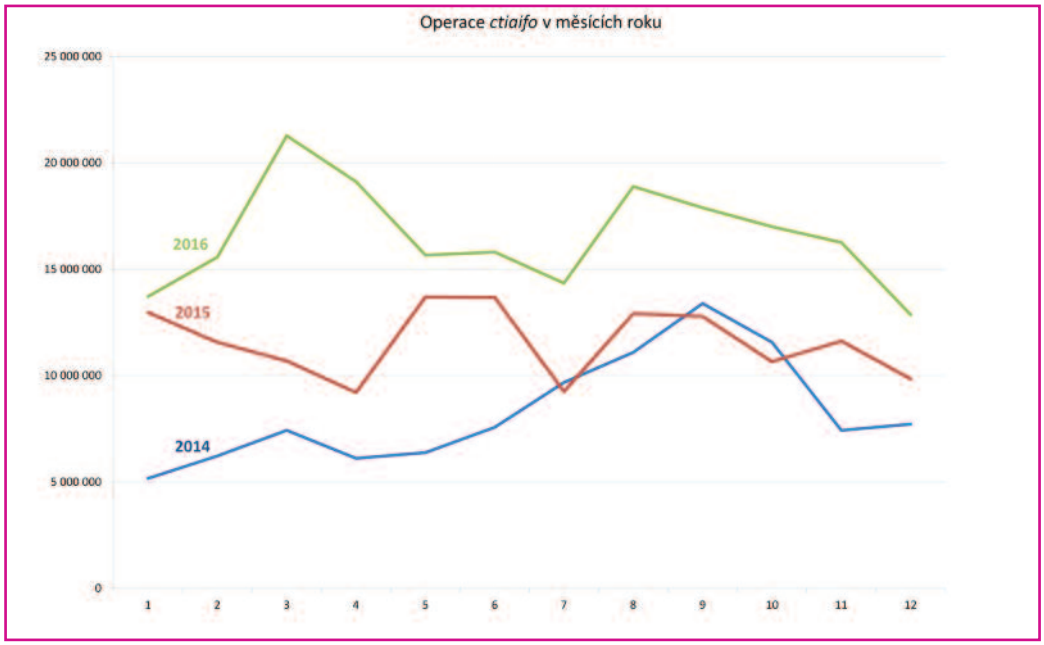
Přestože rozsah uložených dat o každém jedinci je přesně definován a počet lidí se u nás dramaticky nemění, každým rokem stoupá počet operací zpracovaných registrem ORG zhruba o 30 %. Z tohoto nárůstu je patrné, že využití registrů je stále rozšířenější a používanější. Další a další subjekty a agendy využívají služeb Základních registrů, a tím i registru ORG. Nárůsty 49 % a 33 % mezi prosincem a lednem v roce 2014/2015 a 2015/2016 jsou dány pravděpodobně platností nových zákonů a vyhlášek.

Graf „Počet operací v měsících roku" představuje průběh využívání registru ORG během jednotlivých let provozu registru.

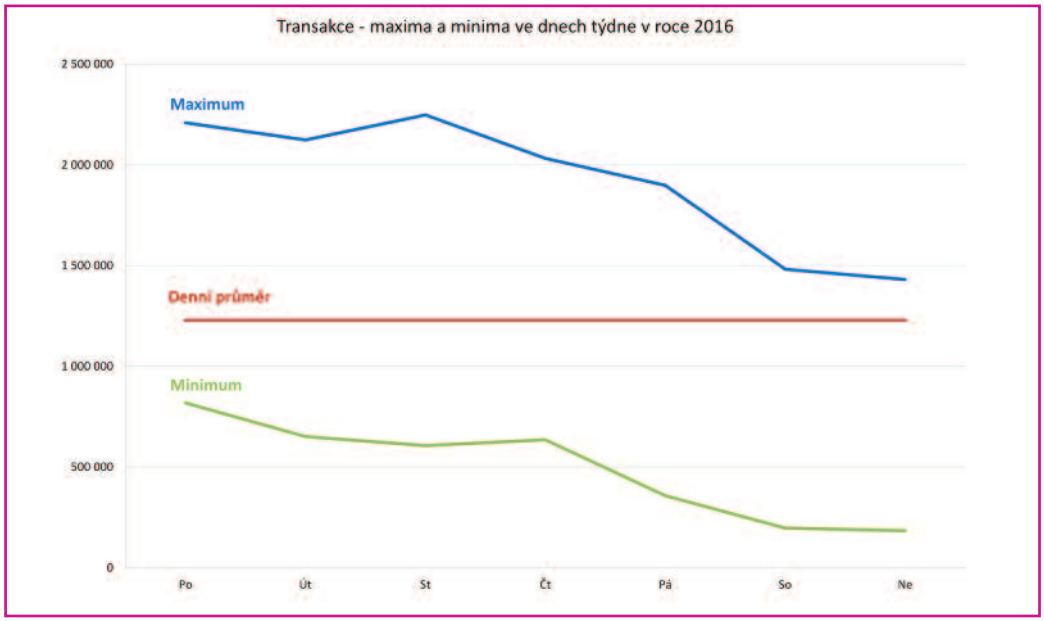


Za povšimnutí stojí každoroční vzestup počtu transakcí v srpnu a září. Průběh počtu transakcí v intervalu květen až říjen je v letech 2015 a 2016 téměř totožný s tím rozdílem, že v roce 2016 je nárůst v jednotlivých měsících cca 30% proti roku 2015. Období červenec–říjen má téměř identický průběh ve všech letech. Je to patrné hlavně v letech 2013, 2015, 2016.

Podobný průběh má i graf „Operace ctiaifo v měsících roku". Tato transakce je nejpoužívanější při práci s registrem ORG. Uvedené grafy jsou pouze pro roky, kdy jsou k dispozici data pro celý rok. Březnové špičky v letech 2014 a 2016 patrně souvisí s volbami. Oba tyto roky byly volební. Podzimní nárůsty jsou pravděpodobně způsobeny začátkem školního roku, žádostmi o rodičovské přídavky, sociální dávky apod.



Denní maximum a minimum v týdnu ukazuje graf „Transakce – maxima a minima ve dnech týdne v roce 2016".



Absolutní maximum za rok 2016 bylo ve středu 5. 10. 2016 s počtem transakcí 2 248 331. Naopak minimum bylo v neděli 7. 2. 2016 s hodnotou 183 953 transakcí. Největší relativní rozdíl je mezi pátečním maximem z 8. 4. 2016 a činí 5,31 násobku minima pátku 1. 1. 2016. Největší absolutní rozdíl je 1 642 508 transakcí mezi středečním minimem z 6. 7. 2016 a středečním maximem 5. 10. 2016. Průměrný denní počet transakcí v roce 2016 je 1 268 919 denně.

V roce 2014 byl přijat zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a prováděcí vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Zároveň vyšlo nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury, doplněné usnesením vlády č. 390/2015, 2. aktualizace Seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu. Informační systém ORG v Systému základních registrů byl označen jako informační systém kritické infrastruktury a je součástí Základních registrů v oblasti e-governmentu.

Toto označení klade mimořádné nároky na technické vybavení a zabezpečení pracovišť, kde je ORG umístěn. Vysoké jsou i nároky na bezchybnost a pracovní postupy při údržbě systému, jeho aktualizaci a zavádění nových funkcionalit a rozšíření. Každý modul a funkce musí projít náročným testováním ve vývojovém a testovacím prostředí systému ORG. Proto jsou téměř každý den nahrávány požadavky vazeb na informační systémy uživatelů do všech prostředí systému ORG.

Probíhají pravidelná školení zaměstnanců, spravujících informační systém ORG, pracovníky firmy TESCO SW a pracovníky SZR.

Na doporučení Správy základních registrů na certifikaci ISMS podle ČSN/ISO 27001:2014 v rámci jednotlivých registrů se Úřad pro ochranu osobních údajů, jako správce IS ORG, rozhodl provést certifikaci ISMS pro IS ORG. Tato certifikace potvrzuje, že IS ORG splňuje náležitosti a požadavky na zajištění bezpečnosti informací.

Jako v předchozích letech se i letos zúčastnila vedoucí oddělení základních identifikátorů přednášek a konferencí, např. v červnu konference správců základních registrů a v září již tradiční konference e-governmentu v Mikulově.

Personální obsazení Úřadu

Počet funkčních míst Úřadu pro ochranu osobních údajů je určen zákonem o státním rozpočtu a systemizací služebních a pracovních míst na příslušný kalendářní rok.

V roce 2016 činil celkový počet systemizovaných míst 104.

Fluktuace zaměstnanců v roce 2016 se v meziročním srovnání s předchozím rokem z 9 % mírně zvýšila na 9,8 %.

V roce 2016 byl postupně dokončen náběh jednotlivých procesů souvisejících s reformou státní služby. Počátkem roku 2016 bylo provedeno první služební hodnocení státních zaměstnanců zařazených k výkonu služby v Úřadu pro ochranu osobních údajů. Na základě provedených služebních hodnocení bylo 18 státních zaměstnanců hodnoceno jako vynikajících a 42 státních zaměstnanců jako dobrých. Žádný státní zaměstnanec nebyl hodnocen jako nevyhovující. Do služebního poměru bylo v roce 2016 nově přijato 6 zaměstnanců, 7 zaměstnanců služební poměr v roce 2016 ukončilo. Do pracovního poměru byli v roce 2016 nově přijati 4 zaměstnanci, 2 zaměstnanci pracovní poměr v roce 2016 ukončili.

V rámci Úřadem zajišťované zvláštní části úřednické zkoušky pro obor služby ochrana osobních údajů bylo vyzkoušeno 7 žadatelů, všichni zkoušení u úřednické zkoušky uspěli.

Ke dni 1. 1. 2016 bylo v Úřadu v evidenčním stavu 101 zaměstnanců, ke dni 31. 12. 2016 byl jejich počet 100.

Průměrný evidenční přepočtený počet zaměstnanců za rok 2016 činil 102.

Dalších 30 osob vykonávalo v Úřadu činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr.

Z tabulky „Členění zaměstnanců ÚOOÚ podle věku a pohlaví“ vyplývá, že v Úřadu pracují převážně zaměstnanci ve věku 50 let a výše, tito zaměstnanci mají kromě odpovídajícího vzdělání i dlouhodobou praxi a velké zkušenosti, mnoho z nich je v Úřadu zaměstnáno od jeho vzniku a svoje zkušenosti předávají novým zaměstnancům, kteří jsou přijímáni na uvolněná funkční místa.

Předpoklad vysokoškolského vzdělání je na dvě třetiny funkčních míst v Úřadu, na zbývající třetinu funkčních míst je předpoklad úplného středoškolského vzdělání.

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 nebo služby. Studentům středních a vysokých škol Úřad poskytuje možnost absolvovat odbornou praxi, a tím podporovat jejich zájem o problematiku ochrany osobních údajů a vyhledávat si tak nové potenciální zaměstnance.

Členění zaměstnanců ÚOOÚ podle věku a pohlaví – stav k 31. prosinci 2016

Celý soubor	muži	ženy	celkem
do 20 let	0,00	0,00	0,00
od 21 do 30 let	3.00	8,00	11,00
od 31 do 40 let	9,00	13,00	22,00
od 41 do 50 let	6,00	6,00	12,00
od 51 do 60 let	12,00	19,00	31,00
61 a více	17,00	8,00	25,00
Celkem	47,00	54,00	101,00

Členění zaměstnanců ÚOOÚ podle vzdělání a pohlaví – stav k 31. prosinci 2016

Celý soubor	muži	ženy	celkem
C – Základní	0	1	1
H – Střední odborné +VL	1	1	2
J – Střední odborné	0	1	1
K – Úplné střední všeobecné	2	4	6
L – Úplné střední odborné + VL	1	2	3
M – Úplné střední odborné	3	13	16
N – Vyšší odborné vzdělání	0	2	2
R – Bakalářské	0	3	3
T – Vysokoškolské	40	27	67
Celkem	47	54	101

Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 400/2015 Sb., o státním rozpočtu České republiky na rok 2016.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

	v tisících Kč
Souhrnné ukazatele	
Příjmy celkem	6 475,91
Výdaje celkem	144 376,48
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	6 475,91
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	0,00
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	6 475,91
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	144 376,48
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	50 743,61
Povinné pojistné placené zaměstnavatelem*)	17 053,23
Převod fondu kulturních a sociálních potřeb	744,23
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	10 205,25
Platy zaměstnanců na služebních místech podle zákona o státní službě	29 916,87
Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	9 410,15
Výdaje spolufinancované z rozpočtu Evropské unie bez SZP celkem	0,00
v tom: ze státního rozpočtu	0,00
podíl rozpočtu Evropské unie	0,00
Výdaje vedené v informačním systému program. financování EDS/SMVS celkem	16 515,64

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

1. Příjmy

Příjmy pro rok 2016 nebyly schváleným rozpočtem stanoveny.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částkou 6 475,91 tisíc Kč.

Jednalo se především o refundace zahraničních cest zaměstnanců Úřadu Evropskou komisí, 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 příjem z prodeje osobního automobilu, o příjmy vztahující se k roku 2015 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2015).

Úhrady za uložené sankce podle zmíněných zákonů byly ve výši 6 048,15 tisíc Kč, přijaté nekap. příspěvky a náhrady týkající se minulých let ve výši 261,76 tis. Kč, převody z ostatních vlastních fondů ve výši 21 tisíc Kč a příjmy z prodeje dlouhodobého hmotného majetku 145,00 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

2. Výdaje

Čerpání výdajů ve výši 144 376,48 tisíc Kč zahrnuje veškeré náklady na platy a související výdaje, kapitálové výdaje, spojené s objektem Úřadu, obnovou vozového parku a informačních systémů, jak samotného Úřadu, tak i IS ORG. Zahrnuje také další běžné výdaje, spojené s chodem Úřadu, tj. zejména položky spojené s nákupem drobného hmotného majetku, materiálu, IT služeb, služeb spojených s provozem budovy a ostatních služeb, cestovného, vzdělávání, údržby a o výdaje související s neinvestičními nákupy.

Výdaje za vodu, plyn, el. energii a PHM činily v roce 2016 1 924,73 tisíc Kč.

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

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

Čerpání rozpočtu na platy zaměstnanců, ostatních výdajů za provedenou práci a souvisejících výdajů, vč. FKSP, a náhrad v době nemoci, ve výši 68 694,52 tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. 12. 2016 byl 102 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 16 515,64 tisíc Kč.

V podprogramu 143V01100 „Pořízení, obnova a provozování ICT ÚOOÚ" bylo v roce 2016 čerpáno celkem 15 903,39 tisíc Kč v ***investičních*** *systémově určených výdajích SR* na následující akce:

	v tis. Kč
akci 143V011000063 „Prodloužení smlouvy Enterprise na používání produktů Microsoft"	2 203,09
akci 143V011000074 „Rozšíření IS ÚOOÚ, kybernetická bezpečnost"	2 709,16
akci 143V011000075 „Úprava IS ORG – 13. etapa"	1 907,67
akci 143V011000076 „Obnova centrálního datového uložiště"	2 939,30

akci 143V011000077 „Úpravy modulu Registr“	74,66
akci 143V011000078 „Úpravy modulu Tescoleg“	69,45
akci 143V011000080 „Úprava IS ORG – 15. etapa“	544,50
akci 143V011000082 „3. DB lokalitou a rozšíření dostupnosti“	3 390,09
akci 143V011000083 „Úprava IS ORG – 16. etapa“	2 065,47

V podprogramu 143V01200 „Reprodukce majetku ÚOOÚ“ bylo v roce 2016 čerpáno celkem 612,25 tisíc Kč v ***investičních*** *systémově určených výdajích SR* na následující akce:

akci 143V012000020 „Zabezpečení objektu – úpravy systému ISP)	89,40
akci 143V012000021 „Rekonstrukce bytové jednotky“	57,00
akci 143V012002016 „Obnova vozového parku“	465,85

Přehled čerpání rozpočtu v roce 2016

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2016 v tis. Kč	Konečný rozpočet 2016 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2016 v tis. Kč	Skutečný konečný rozpočet v %
2211, 2212, 2324, 3113, 4132	Ostatní nedaňové příjmy	0,00	0,00	6 475,91	
	Příjmy celkem	**0,00**	**0,00**	**6 475,91**	
501	Platy Platy zaměstnanců v pracovním poměru vyjma zaměstnanců	48 760,09 9 956,36	49 710,44 10 205,25	49 532,27 10 205,25	99,64 100,00
5011	na služebních místech				
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	29 218,13	29 919,59	29 916,87	99,99
5014	Platy zaměst. odvozov. od platů úst. činitelů	9 585,60	9 585,60	9 410,15	98,17
502	Ostatní platby za provedenou práci	2 245,99	1 745,99	1 211,34	69,38
5021	Ostatní osobní výdaje	2 245,99	1 655,32	1 120,67	67,70
5024	Odstupné	0,00	90,67	90,67	100,00

503	Povin. pojist. plac. zaměstnavatelem	17 491,16	17 602,15	17 053,23	96,88
5031	Povin. pojist. na sociál. zabezp.	12 751,52	12 833,13	12 503,81	97,43
5032	Povin. pojist. na veřej. zdrav. pojišt.	4 739,64	4 769,02	4 549,42	95,40
513	Nákup materiálu	1 595,00	1 858,00	1 579,11	84,98
514	Úroky a ost. fin. výdaje	15,00	45,00	41,55	92,34
515	Nákup vody, paliv a energie	2 400,00	1 982,86	1 924,73	97,07
516	Nákup služeb	19 666,00	19 318,53	14 058,70	72,77
5169	Nákup ostatních služeb	8 242,00	6 806,41	5 298,80	77,85
517	Ostatní nákupy	37 587,33	44 657,90	38 821,72	86,93
5171	Opravy a udržování	35 248,33	42 008,91	37 111,313	88.34
5173	Cestovné	1 700,00	1 925,00	1 270,78	66,01
518	Poskyt. zálohy, jistiny	330,00	540,00	0,00	0,00
519	Výdaje souvis. s neinv. nákupy	2 904,60	2 885,71	2 725,55	94,45
5342	Převody do FKSP	731,40	744,23	744,23	100,00
536	Ost. neinv. transf. jin. veřej. rozp.	22,00	16,04	15,04	93,77
542	Náhrady plac. obyvatelstvu	200,00	200,00	153,44	76,72
5424	Náhrady v době nemoci	200,00	200,00	153,44	76,72
	Běžné výdaje celkem	**133 948,58**	**141 306,86**	**127 860,84**	**90,48**
611	Pořízení dlouh. nehmot. majetku	9 500,00	8 682,96	7 514,30	86,54
612	Pořízení dlouh. hmot. majetku	8 200,00	10 704,29	9 001,34	84,09
	Kapitálové výdaje celkem	**17 700,00**	**19 387,25**	**16 515,64**	**85,19**
	VÝDAJE CELKEM	151 648,58	160 694,11	144 376,48	89,85

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 12. 2016.

INTERNÍ AUDIT

Plán interního auditu ÚOOÚ na rok 2016 ukládal provedení dvou auditorských šetření, v průběhu roku byly na základě oznamovacích dopisů a programů auditů uskutečněny následující audity:

Audit 01/16

Audit vnitřních předpisů a organizační shody s činností ÚOOÚ ze zákona

Účelem auditu bylo prověření a vyhodnocení stavu v auditované oblasti z hlediska vnitřních předpisů, které nastavují pravidla pro fungování a účinnost vnitřního kontrolního systému a jejich souladu s platnou legislativou a potřebami Úřadu. V průběhu auditu byly posouzeny návrhy nových směrnic – Finančního řádu, vnitřního předpisu o zveřejňování smluv a návrhu na doplnění a úpravu konkrétních ustanovení směrnice o zadávání veřejných zakázek malého rozsahu, které reagují na legislativní změny v daných oblastech.

Audit zkonstatoval, že vnitřní předpisy Úřadu v praxi plní úlohu, kterou zákon o finanční kontrole stanoví a ukládá v oblasti účinnosti vnitřního kontrolního systému a po přijetí nově navrhovaných vnitřních předpisů (Finanční řád, Směrnice o uveřejňování v registru smluv), nebo po jejich aktualizaci (úprava směrnice o zadávání veřejných zakázek malého rozsahu, směrnice o pracovních cestách) budou z hlediska vnitřního kontrolního systému v souladu se zákonem o finanční kontrole i s ostatními obecně platnými právními předpisy.

Audit 02/16

Audit vnitřního kontrolního systému

Cílem auditu bylo prověřit a vyhodnotit stav v auditované oblasti z hlediska přiměřenosti a účinnosti vnitřního kontrolního systému a jeho souladu s platnou legislativou, zejména příslušnými ustanoveními zákona č. 320/2001 Sb. o finanční kontrole ve veřejné správě (dále jen zákona o finanční kontrole) a prováděcí vyhlášky č. 416/2004 Sb. Součástí auditu bylo i ověřit plnění doporučení z dřívějších auditů a navrhnout doporučení k nápravě zjištěných nedostatků.

Audit byl ukončen konstatováním, že vnitřní kontrolní systém plní řádně funkci, kterou mu ukládá zákon o finanční kontrole, postupy řídící kontroly stanovené zákonem o finanční kontrole a prováděcí vyhláškou č. 416/2004 Sb., jsou v organizaci nastaveny v souladu s výše uvedenými předpisy a jsou v praxi reálně používány.

Účetní systém Úřadu plně reflektuje a aplikuje do řídící kontroly postupy, které předepisuje ve veřejné správě zákon o finanční kontrole, všechny testované operace byly realizovány v souladu s podpisovým řádem. V průběhu auditu byla konstatována některá administrativní pochybení, u naprosté většiny všech kontrolovaných operací však byl dodržen princip zpětné ověřitelnosti v rámci každé konkrétní operace, což je základní požadavek pro správné fungování vnitřního kontrolního systému.

Při realizaci všech auditů byl kladen důraz na kontrolu dodržování zákonných a vnitřních norem, byla ověřována existence uvědomělého procesu řízení rizik v ÚOOÚ a přiměřenost a účinnost řídících a kontrolních mechanismů auditovaných procesů.

V souladu se zákonem o finanční kontrole Úřad předložil Ministerstvu financí roční zprávu o výsledcích finančních kontrol za předchozí rok.

ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2016 a informace o jejím předání proběhne řádně v termínu do 31. 7. 2017 dle Přílohy č. 4 vyhlášky č. 383/2009 Sb., o účetních záznamech v technické formě vybraných účetních jednotek a jejich předávání do centrálního systému účetních informací státu a o požadavcích na technické a smíšené formy účetních záznamů (technická vyhláška o účetních záznamech). V souladu se sdělením Ministerstva financí k aplikaci některých ustanovení zákona č. 221/2015 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, a v návaznosti na zákon č. 101/2000 Sb., nemá Úřad povinnost schvalovat účetní závěrku auditorem.

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

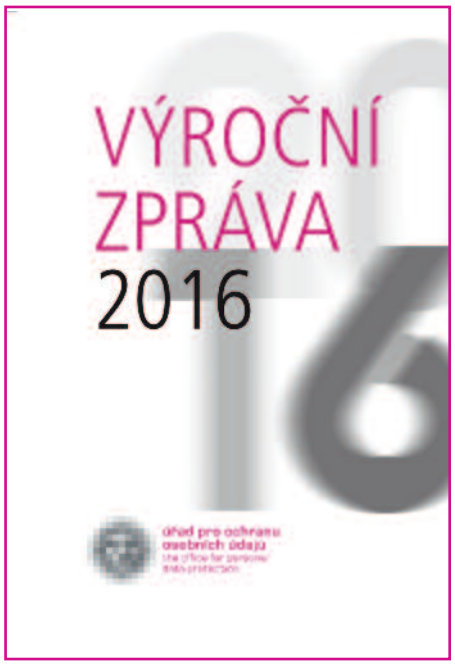
Úřadu bylo v roce 2016 adresováno celkem 53 žádostí o poskytnutí informací, přičemž došlo k mírnému poklesu v porovnání s předchozími lety. V mnoha případech však byl požadován rozsáhlý soubor informací zasahující do mnoha sfér činnosti Úřadu i do oblasti jeho působnosti, tj. ochrany osobních údajů.

Úřad vyhověl 42 žádostem, ve 3 případech byl nucen vydat rozhodnutí o úplném odmítnutí poskytnout požadované informace a částečně bylo odmítnuto 8 žádostí. Důvodem pro úplné nebo částečné odmítnutí byla zejména ochrana osobních údajů osob, které byly obsaženy v požadovaných dokumentech. Dalším důvodem odmítnutí bylo, že požadované informace Úřad neměl k dispozici, resp. neexistovaly, nebo se jednalo o informace, které získal od třetí osoby při plnění úkolů v rámci kontrolní činnosti, případně o informace související s trestním řízením, jejichž poskytnutí zákon č. 106/1999 Sb. zakazuje.

Proti rozhodnutí o částečném odmítnutí podal žadatel o informace v jednom případě rozklad předsedkyni Úřadu, která rozhodnutí prvního stupně potvrdila. Stížnost podle § 16a zákona č. 106/1999 Sb. na postup Úřadu při vyřizování stížností nebyla podána a stejně tak nebyla v této souvislosti podána žádná žaloba.

Pozornost žadatelů byla již tradičně zaměřena především na rozhodovací činnost Úřadu, tj. na výsledky správních řízení, výsledky následných soudních řízení a také na výšku uložených sankcí, resp. jejich souhrn za poslední roky. Značný počet žádostí směřoval ke kontrolní činnosti Úřadu. Žadatelům byly poskytnuty informace o kontrolách provedených inspektory Úřadu u jednotlivých subjektů, o výsledcích těchto kontrol a uložených nápravných opatřeních. Oblastmi, na které byl například zaměřen zájem veřejnosti, byly podmínky provozu kamerových systémů a jejich registrace, zpracování identifikačních čísel vozidel apod.

Další skupina žádostí se týkala organizace Úřadu, jeho personálního a finančního zabezpečení, používaných informačních systémů, ale také výsledků finanční kontroly Úřadu.



Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2016
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 2017 na svých webových stránkách.

Editor: PhDr. David Pavlát, telefon 234 665 286
Redakční zpracování: BcA. Květa Gebauerová, DiS.
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, 2017

ISBN 978-80-210-8507-7