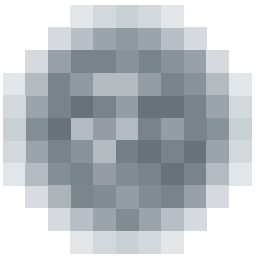
Výroční zpráva 2017



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-8914-3

Úvodní slovo předsedkyně Úřadu

Dámy a pánové,

do Vašich rukou se dostává výroční zpráva Úřadu pro ochranu osobních údajů za rok 2017. Rozhodně Vás nyní nehodlám poučovat, jak tyto řádky číst, a tedy předjímat, co byste v nich anebo snad dokonce i mezi nimi měli nalézt.

Touto výroční zprávou se uzavírá sedmnáctileté období Úřadu pro ochranu osobních údajů založené na zákoně č. 101/2000 Sb., o ochraně osobních údajů. Jak je obecně známo, od 25. května 2018 jej nahradí obecné nařízení Evropského parlamentu a Rady 2016/679 o ochraně osobních údajů. Jednotná ochrana osobních údajů a jejich volný pohyb jsou klíčové pro naplňování čtyř základních svobod, na nichž je fungování Evropské unie založeno. Volný pohyb osob, služeb, zboží a kapitálu je na digitalizované osobní údaje organicky navázán a obecné nařízení (GDPR) jen odráží stav, kdy osobní údaje jsou žádanou komoditou a někdy i nezpochybňovaným platidlem.

V této souvislosti bych proto ráda připomněla, že toto nařízení bylo právě v uplynulém roce účelově démonizováno, vesměs tak, že se používalo k nabízení služeb a uzavírání výhodných nabídek s těmi, kdo jsou vázáni povinnostmi. Úřad pro ochranu osobních údajů se snažil démonizaci čelit, aniž by zároveň

zastíral potřebu přípravy na režim nařízení. Troufám si prohlásit, že ten, kdo ochraně osobních údajů věnoval náležitou pozornost, by neměl mít s aplikací nařízení výrazné problémy.

Tomu by měl přispět i trend méně formálního, zato však věcně podloženého rozhodování, o který Úřad pro ochranu osobních údajů v posledních letech usiloval a který dále pokračoval i v roce 2017 jako pozvolný a cílevědomý proces. Prakticky to znamená, se vší důsledností a i za cenu případného odhlédnutí od pouze formálních hledisek a zaběhlých metodických postupů, primárně posuzovat účel sledovaný zpracováním osobních údajů. To vše při zachování úcty k právu každého z nás domoci se svých důvodných nároků anebo chránit své oprávněné zájmy a soukromí. Uvážlivěji by Úřad postupoval v některých případech z minulosti, jako je ekolo či Kravaře, které uzavřely rozsudky soudu. V obou kauzách by nyní Úřad pokutu neudělil. Nejen tímto způsobem chci vyslat jasný signál veřejnosti, že rozhodování Úřadu se postupně vyvíjí směrem k nepostihování těch, kteří přiměřeným způsobem chrání své právo proti narušiteli.

Vždy je třeba především řádně zkoumat, zda je zpracováním osobních údajů sledován legitimní, právem aprobovaný cíl, či zda není zpracováním neoprávněně zasahováno do sféry jiného. Zároveň je nezbytné vyhodnotit, zda nebyly k dispozici i jiné možnosti, méně zasahující do právní sféry jiných osob, jimiž bylo možné dosáhnout cíle sledovaného zpracováním. Svá práva má hájit především ten, do jehož soukromí bylo zasaženo, což neomezuje ochranu veřejného zájmu Úřadem také v jiných případech. Udělená rekordní pokuta za nevyžádaná obchodní sdělení ve výši 4,25 milionu korun je toho důkazem.

Úřad pro ochranu osobních údajů bude takto přistupovat ke svým úkolům i napříště. Je to jediná cesta, jak do budoucna udržet soulad mezi základními lidskými právy, k nimž patří jak právo na soukromí, tak právo na ochranu osobních údajů, a prudkým technologickým vývojem. Tím mám na mysli rozvoj zpracování genetických a biometrických osobních údajů, umělé inteligence nebo sledovacích systémů a vytváření nových, technologicky podmíněných, osobních údajů v obecně nadšeně přijímaných aplikacích a službách. Bylo by krátkozraké takové systémy plošně zavrhovat, stejně tak jako nekorigovat jejich podobu a používání prostřednictvím vhodných kritérií. V globalizovaném světě není za situace plošného (všeobecného) rozšíření technologií založených na vytváření a využívání osobních údajů jiná reálná možnost ochrany našeho soukromí.

JUDr. Ivana Janů
předsedkyně Úřadu pro ochranu osobních údajů

Obsah

Úřad v číslech 2017

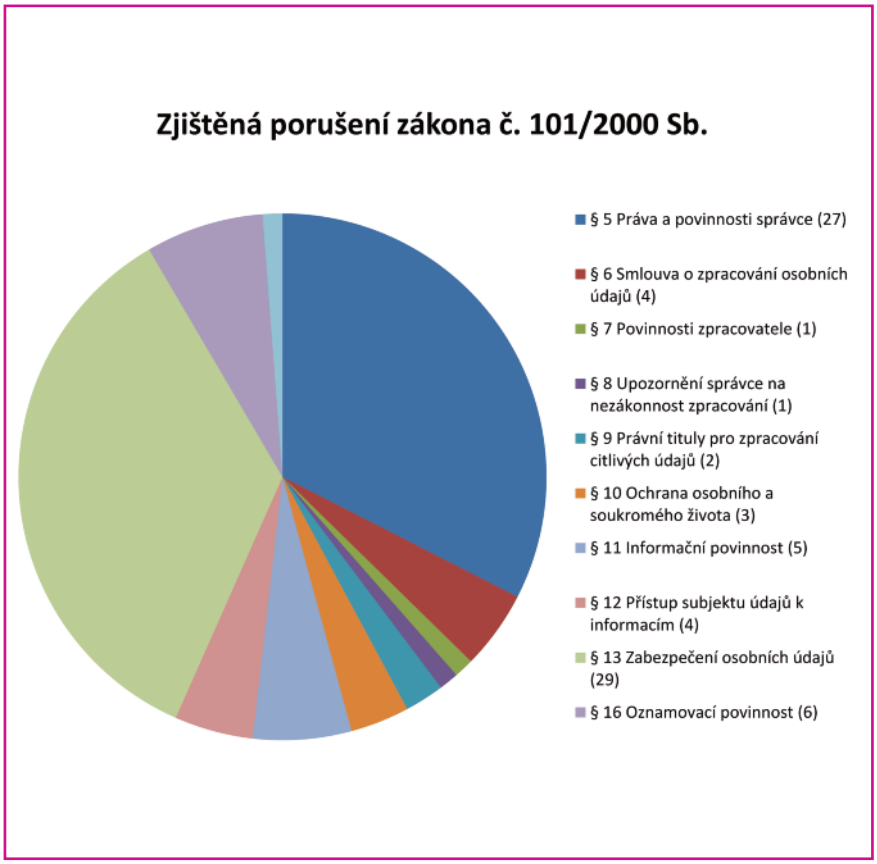
Dotazy a konzultace	ČR	2305
	zahraničí	28
	z toho	
	soukromá sféra	1748
	veřejná správa	557
Podání a stížnosti	přijaté podněty	1684
	z toho informování správce o jeho povinnostech	254
	z toho stížnosti předané ke kontrole nebo správnímu řízení	152
Kontrolní činnost **vyjma kontrol** týkajících se zákona č. 480/2004 Sb.)	zahájeno	100
	ukončeno	110
	z toho z předchozích let	41
	předáno jiným státním úřadům	1
	uložená opatření k nápravě	16
	napadeno námitkami	18
	námitkám vyhověno	0
	nevyhověno	12
	převážně vyhověno	1
	převážně nevyhověno	3
	předkontrolní úkony bez následného zahájení kontroly	27
Nevyžádaná obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	2710
	vyřešených podnětů	2218
	zahájených kontrol	19
	ukončených kontrol	19
	z toho z předchozích let	6
	řízení o sankci	18
	napadeno námitkami	7
	námitkám vyhověno	0
	nevyhověno	5
	převážně vyhověno	1
	převážně nevyhověno	0
	předkontrolní úkony bez následného zahájení kontroly	7

Správní trestání	řízení o sankci za porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb. s právnickými osobami a fyzickými osobami podnikajícími	50
	řízení o sankci za porušení zákona č. 101/2000 Sb. a fyzickými osobami	11
	upuštění od uložení pokuty podle § 40a zákona č. 101/2000 Sb.	34
Rozhodnutí o rozkladech	rozklady napadená rozhodnutí	25
	zamítnutých rozkladů	16
	zrušeno a vráceno k novému projednání	3
	zrušených rozhodnutí a zastaveno řízení	1
	změna rozhodnutí	1
Soudní přezkum (Pozn.: * *celkem od r. 2001*)	podaných žalob k soudu	2 (147*)
	zamítnutých žalob soudem	11
	zrušených rozhodnutí soudem	3
	ukončených/neukončených soudních řízení od roku 2001	127/20
Registrace	přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.)	9241
	zaregistrovaná zpracování	9002
	dosud v řízení	513
	zrušené registrace	156
	oznámení o změně zpracování	887
	řízení podle § 17	31
	zastaveno (nedochází k porušení zákona)	23
	zastaveno z procesních důvodů (např. oznámení vzato zpět)	2
	nepovoleno	1
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	31
	rozhodnutí o povolení předávání	32
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	2
Oznámení podle zákona č. 127/2005 Sb.	došlých oznámení	1
	vyřízených jako opodstatněné	0
	vyřízených jako neopodstatněné	0
Stížnosti podle § 175 správního řádu	přijatých stížností	34
	vyřízených jako důvodné	4
	vyřízených jako částečně důvodné	7
	vyřízených jako bezdůvodné	23

Žádosti podle zákona č. 106/1999 Sb.	přijatých žádostí	30
	zcela vyhověno	24
	částečně odmítnuto	3
	odmítnutých žádostí	3
Publikované materiály	Věstník Úřadu (počet částek)	1
Připomínkované legislativní návrhy	zákony	21
	prováděcí předpisy	88
	návrhy nařízení vlády	16
	návrhy vyhlášek	72
	ostatní	48
	zahraniční materiály	6

Kontrolní činnost Úřadu

Kontrolní činnost Úřadu se provádí na základě kontrolního plánu nebo na základě podnětů a stížností (viz § 31 zákona č. 101/2000 Sb.), některé z kontrol pak probíhají též na základě podnětu předsedkyně Úřadu.



• KONTROLNÍ PLÁN

Kontrolní plán Úřadu je v každém roce sestavován obdobně. Jednu část kontrolního plánu tvoří kontroly, které lze označit jako povinné a pravidelné. Mezi ty patří například kontroly v oblasti Schengenského informačního systému, Vízového informačního systému apod. V roce 2017 bylo přitom součástí kontrolního plánu právě zpracování osobních údajů ve vnitrostátní části Schengenského informačního systému (SIS II). Rovněž byla provedena pravidelná kontrola zákonnosti zpracování v systému EURODAC, ve kterém jsou zpracovávány osobní údaje žadatelů o mezinárodní ochranu. Oba tyto systémy jsou z pohledu českého právního řádu informačním systémem kritické informační infrastruktury ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Dalším předmětem kontrol, realizovaných na základě kontrolního plánu, je zpracování osobních údajů, které jsou jako potenciálně problematické detekovány na úrovni členských států Evropské unie v rámci pracovní skupiny pro ochranu údajů WP29 nebo jejích podskupin. V roce 2017 byla projevem této aktivity zejména kontrola zpracování osobních údajů při využívání mobilních aplikací subjekty veřejné správy.

Kontrolní plán je při své tvorbě ovlivňován též předchozí kontrolní činností či šířeji dozorovou činností Úřadu. Právě při výkonu dozorové činnosti se totiž Úřad často setkává s jevy, které vyvolávají podezření, že neoprávněným zpracováním mohou být ohroženy osobní údaje v rámci celého sektoru apod. Příkladem takové kontroly zařazené do kontrolního plánu pro rok 2017 byly kontroly u telefonních operátorů zaměřené na zabezpečení osobních údajů zákazníků. Provést takovéto kontroly se ukázalo jako vhodné na základě zjištěného úniku zákaznických dat společnosti T-Mobile Czech Republic a.s., ke kterému došlo v roce 2016. Dalším příkladem byla kontrola zpracování osobních údajů u personální agentury, což byl výsledek kontrol provedených na základě podnětů, které byly Úřadu doručeny též v roce 2016, ze kterých vyplynuly pochybnosti o dodržování povinností při zpracování osobních údajů agenturních zaměstnanců.

Další skupinu podkladů, ze které vzniká kontrolní plán, pak tvoří podněty doručené Úřadu, které samy o sobě sice nejsou dostatečným podkladem pro zahájení kontroly, ale např. z jejich celkového počtu je zjevné, že se jedná o oblast zpracování, kterou je třeba podrobit podrobnějšímu zkoumání anebo je veřejností vnímána jako problematická. V roce 2017 tak byly na základě kontrolního plánu provedeny například kontroly subjektu, který žádal podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, o poskytnutí údajů o platech a odměnách jeho zaměstnanců. Kontrola byla zaměřena na další nakládání s takto získanými osobními údaji. Do kontrolního plánu byla také zařazena kontrola provozovatele dlužnického registru, která se měla mimo jiné zaměřit na předávání dat do tohoto registru a na využívání rodných čísel při jeho provozování.

I v roce 2017 byl v pololetí kontrolní plán doplněn o další plánované kontroly, čímž Úřad reagoval na aktuální podezření nebo pochybnosti týkající se zpracování osobních údajů, která se začínají realizovat i na základě nových právních předpisů. Příkladem bylo v roce 2017 zejména zpracování osobních údajů, jež probíhá na základě zákona č. 112/2016 Sb., o evidenci tržeb, a to včetně samostatné kontroly zaměřené na účtenkovou loterii pořádanou podle § 35 uvedeného zákona.

V následující části této výroční zprávy je možné se dozvědět více k některým případům, které byly předmětem kontroly na základě kontrolního plánu.

• POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

Inspektor František Bartoš

Shromažďování osobních údajů prostřednictvím kamerových systémů Policií ČR

Na základě podnětu a plánu kontrol uskutečnil Úřad kontrolu Policie ČR ve věci dodržování povinností správce a zpracovatele osobních údajů, zpracovávaných v rámci využívání informací shromažďovaných prostřednictvím automatizovaných kamerových systémů – měření úsekové rychlosti vozidel (MÚR), měření okamžité rychlosti vozidel (MOR), Systém LOOK Policie ČR, Strategické dopravní detektory (SDD), Vysokorychlostní vážení vozidel (WIM), Detekce jízdy na červenou (DTJ), Kontrolní mýtné stanice (brány) firmy Kapsch – dále jen „úsekové měření".

Kontrola byla provedena na třech krajských ředitelstvích Policie ČR. V rámci předmětu prováděné kontroly bylo prověřeno nejen oprávnění Policie ČR ke shromažďování osobních údajů prostřednictvím kamerového systému v souvislosti s úsekovým měřením, ale i jejich následné zpracování.

Kontrolou bylo zjištěno, že jednotlivá krajská ředitelství Policie ČR uzavírají s provozovateli automatizovaných kamerových systémů, tedy s příslušnými obcemi a městy a Ředitelstvím silnic a dálnic, smlouvy, na základě kterých jsou automatizovaně přenášeny informace provozovateli jednotlivých technických zařízení a současně Policii ČR. Tyto informace se týkají všech vozidel bez ohledu na skutečnost, zda záznam byl pořízen.

Základem těchto automatických systémů, které zaznamenávají dfc. všechna projíždějící vozidla, a to bez ohledu na skutečnost, zda dochází nebo nedochází k porušování právní povinnosti (rychlá jízda, jízda na červenou, přetížení vozidla apod.), jsou pořizovány fotografie přední části vozidla a jeho registrační značky. Současně kamerový systém registrační značku vozidla „přečte" a porovná s databází vozidel. Pořízené fotografie a záznamy jsou uloženy v systémech Policie ČR po dobu 6–12 měsíců.

V rámci oprávnění kontrolujících byla provedena kontrola využívání těchto informací vzhledem k činnosti policie i včetně kontroly oprávněnosti přístupu k pořízeným datům. Byly prověřeny interní kontrolní mechanismy Policie ČR nastavené k zabránění zneužití zpracovávaných informací, včetně kontroly jejich zabezpečení.

Kontrolou bylo konstatováno, že základním právním předpisem, podle kterého Policie ČR postupuje při úsekovém měření kamerovým systémem se záznamovým zařízením, je zákon č. 273/2008 Sb., o Policii České republiky, zejména jeho ustanovení § 2, § 60, § 62 a § 85. Zpracování osobních údajů v souvislosti s úsekovým měřením je obsaženo v § 79a zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, které upravuje, že „za účelem zvýšení bezpečnosti provozu na pozemních komunikacích je policie a obecní policie oprávněna měřit rychlost vozidel". Obecné ustanovení § 2 zákona č. 273/2008 Sb. ukládá Policii ČR sloužit veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku a veřejný pořádek, předcházet trestné činnosti, plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku

a bezpečnosti svěřené jí zákony. Dále bylo konstatováno, že dle *§ 60 odst. 1 zákona č. 273/2008 Sb.* je Policie ČR oprávněna zpracovávat v souladu s tímto zákonem a jinými právními předpisy informace včetně osobních údajů v rozsahu nezbytném pro plnění svých úkolů, přičemž dle odst. 2 výše uvedeného ustanovení musí Policie ČR zpracovávané informace zabezpečit před neoprávněným přístupem, změnou, zničením, ztrátou nebo odcizením, zneužitím nebo jiným neoprávněným zpracováním.

Kontrolou bylo zjištěno a konstatováno, že zásadním ustanovením, které Policii ČR umožňuje pořizování záznamů, je *§ 62 zákona č. 273/2008 Sb.* Podle odst. 1 uvedeného ustanovení může policie, je-li to nezbytné pro plnění jejích úkolů, pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných a zvukové, obrazové nebo jiné záznamy o průběhu úkonu. Podle odst. 2, jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, policie informace o zřízení takových systémů vhodným způsobem uveřejní. Uvedené zákonné zmocnění Policie ČR představuje tzv. úřední licenci, která je nezbytná k zásahu do osobnostních práv fyzických osob, přičemž dle ustanovení § 85 odst. 1 zákona *č. 273/2008 Sb.* může Policie ČR při plnění svých úkolů v souvislosti se zpracováváním osobních údajů při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů a zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti: *a*) zpracovávat nepřesné nebo neověřené osobní údaje; pokud je to možné, policie osobní údaje takto označí, *b*) zpracovávat osobní údaje i k jinému účelu, než ke kterému byly shromážděny, *c*) shromažďovat osobní údaje otevřeně i utajeným způsobem nebo pod záminkou jiného účelu anebo jiné činnosti, *d*) sdružovat osobní údaje, které byly získány k rozdílným účelům, za účelem předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů, zajištění vnitřního pořádku a bezpečnosti včetně pátrání po osobách a věcech a zajištění bezpečnosti České republiky. Dle odst. 2 výše uvedeného ustanovení zpracovává Policie ČR osobní údaje podle odstavce 1 odděleně od osobních údajů zpracovávaných při plnění jiných úkolů policie. Úsekové měření upravuje Policie ČR také interními předpisy a dohodami se subjekty mimo Policii ČR, což kontrolující řádně prověřili.

Kontrola společnosti Partners Financial Services, a.s., v souvislosti se zprostředkováním životního pojištění

Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů fyzických osob, klientů, při uzavírání smluv a při zprostředkování uzavírání smluv v oblasti pojišťovnictví.

Stěžovatel uvedl, že v souvislosti se zprostředkováním uzavření životního pojištění udělil a podepsal v rámci úvodního jednání společnosti Partners Financial Services, a.s. (dále jen „Partners“) souhlas se zpracováním osobních a citlivých údajů, a to nejen pojišťovně, ale i zprostředkovatelské společnosti. V průběhu projednávání smlouvy předal pro pojišťovnu dokumenty, které vyplnil jeho ošetřující lékař (zdravotní dotazník, laboratorní výsledky, výpis ze zdravotnické dokumentace), vypovídající o jeho zdravotním stavu. Následně došlo ze strany pojišťovny k rozhodnutí o ukončení jednání. Tím nedošlo k uzavření smlouvy. Stěžovatel proto písemně odvolal svůj souhlas se zpracováním osobních a citlivých údajů a požádal zprostředkovatelskou společnost Partners o vrácení dokumentů obsahujících informace o jeho zdravotním stavu a likvidaci všech citlivých údajů. Tento požadavek kontrolovaná společnost Partners odmítla.

Kontrolou bylo konstatováno, že smlouva nebyla uzavřena a tím pominul účel zpracování a uchovávání citlivých údajů. V daném případě byl účastník řízení povinen zpracování a uchovávání zdravotní dokumentace s citlivými údaji stěžovatele ukončit a zdravotní dokumentaci prokazatelně zlikvidovat ve smyslu § 20 odst. 1 zákona č. 101/2000 Sb., resp. je stěžovateli vrátit. V rámci kontroly zástupci společnosti Partners argumentovali, že v dané věci postupují ve smyslu pokynů Národní banky pro účely kontroly v oblasti dohledu nad činností pojišťovacích zprostředkovatelů, dále že dokumenty je společnost povinna uchovávat ve smyslu zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, dle které má povinnost veškeré údaje (tedy i citlivé) získané v rámci identifikace a kontroly klienta uchovávat, a to po dobu deset let od ukončení spolupráce.

Kontrolou bylo konstatováno, že účastník řízení v souvislosti s neoprávněným uchováváním citlivých údajů o zdravotním stavu stěžovatele porušil ustanovení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb., ve kterém je správci osobních údajů stanovena povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Odvoláním souhlasu se zpracováním citlivých údajů, a neuzavřením smlouvy došlo k tomu, že odpadl účel zpracování citlivých údajů, tj. plnění ze smlouvy o životním pojištění. Účastník řízení citlivé údaje stěžovatele uchovával bez konkrétně vymezeného účelu a bez vědomí správce osobních a citlivých údajů, tj. příslušné pojišťovny, a současně kontrolovaná zprostředkovatelská společnost nebyla ve smyslu § 9 písm. a) zákona č. 101/2000 Sb. schopna po odvolání souhlasu stěžovatele se zpracováním jeho osobních a citlivých údajů prokazatelně doložit existenci souhlasu subjektu údajů se zpracováním osobních a citlivých údajů.

Proti protokolu o kontrole podala kontrolovaná společnost námitky, které byly v plném rozsahu zamítnuty. V následném správním řízení jí bylo uloženo osobní a citlivé údaje stěžovatele zlikvidovat a vrátit mu požadované dokumenty. Tuto povinnost kontrolovaná společnost splnila. Ve věci bude vedeno řízení o přestupku.

Inspektorka Jiřina Rippelová

Kontrola v souvislosti se zpracováním osobních údajů zákazníků Hornbach Baumarkt CS, s.r.o.

Předmětem této kontroly, zahájené na základě podnětu doručeného Úřadu, bylo dodržování povinností stanovených zákonem č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů zákazníků, a to zejména zákazníků podezřelých z krádeže či poškození zboží v prodejnách hobby marketu. Prostředkem ke zpracování těchto osobních údajů byl jednak kamerový systém a dále software určený k evidování zboží, které se zadržené osoby pokusily odcizit.

Ve vztahu ke kamerovému systému bylo kontrolou zjištěno, že kontrolovaná osoba provozuje v prodejně, která byla zvolena pro účely kontroly, kamerový systém tvořený několika typy kamer (tubusové, pevné i otočné), přičemž všechny kamery umožňují přiblížení obrazu (zoom). Konkrétní zaměření kamer lze libovolně měnit, a to tak, aby vyhovovalo aktuálním potřebám kontrolované osoby. Kamery monitorují vnitřní prostor prodejny a dále venkovní prostor vjezdu a výjezdu u terminálu pro výdej zboží. Kamerový systém byl instalován za účelem ochrany majetku kontrolované osoby a je ovládán a spravován zaměstnanci společnosti, která zajišťuje ostrahu prodejny. Vzhledem k tomu, že kontrolující posoudili na základě konkrétních okolností předmětný kamerový systém tak, že do práv chráněných zákonem č. 101/2000 Sb. zasahuje pouze v míře přiměřené významu práv a zájmů kontrolované osoby, dospěli k závěru, že v tomto

případě lze aplikovat právní titul pro zpracování osobních údajů dle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Současně bylo posouzeno i plnění dalších povinností kontrolované osoby, konkrétně informování o provozu kamerového systému ve smyslu § 11 zákona č. 101/2000 Sb. a zajištění bezpečnosti zpracovávaných osobních údajů dle § 13 tohoto zákona. V obou těchto aspektech bylo shledáno, že kontrolovaná osoba postupuje v souladu s požadavky citovaných ustanovení. Ve vztahu k softwaru určenému k evidování zboží, které se pokusily odcizit zadržené osoby, bylo kontrolou zjištěno, že tento software na základě smluvních ujednání je povinna využívat společnost zajišťující ostrahu prodejny. Předmětný software má mimo jiné sloužit k evidenci zboží, které se pokusily odcizit (popř. poškodily) zadržené osoby, a to včetně evidence osobních údajů těchto osob. Kontrolou bylo nicméně zjištěno, že v praxi nejsou osobní údaje zadržených osob evidovány a předmětný software je využíván pouze k evidenci zboží, jehož odcizení bylo zabráněno, společně s uvedením identity zaměstnance ostrahy, který zákrok provedl. Vzhledem k tomuto zjištění nebylo zpracování osobních údajů zadržených osob (kontrolou byl zjištěn jeden konkrétní případ) hodnoceno jako porušení § 5 odst. 2 zákona č. 101/2000 Sb., ale jako porušení povinnosti stanovené v § 13 odst. 1 tohoto zákona, neboť kontrolovaná osoba nepřijala jasně definovaná opatření směřující k tomu, aby nemohlo dojít k neoprávněnému či nahodilému zpracování osobních údajů.

V návaznosti na tuto kontrolu přijala kontrolovaná osoba opatření směřující k nápravě zjištěných pochybení. Zejména s ohledem na tuto skutečnost (a současně s přihlédnutím k tomu, že kontrolou byl zjištěn pouze jeden případ) bylo od uložení sankce upuštěno.

Město Černošice – kontrola v souvislosti se zpracováním osobních údajů prostřednictvím kamerového systému provozovaného v učebnách

Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených v zákoně č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů prostřednictvím kamerového systému provozovaného v učebnách, v nichž probíhají zkoušky odborné způsobilosti žadatelů o řidičské oprávnění. Kontrolující konstatovali, že monitorování průběhu těchto zkoušek prostřednictvím kamerového systému se záznamem není zákonnou povinností kontrolované osoby a že mu nelze přiznat ani jiný právní titul dle § 5 odst. 2 zákona č. 101/2000 Sb. V daném případě není dán žádný zákonný ani jiný důvod hodnotit zkoušky vykonávané kontrolovaným jinak, než jakékoli jiné zkoušky odborné způsobilosti nebo zkoušky na akademické půdě (maturitní, vysokoškolské). Kontrolovaný tedy porušil povinnost stanovenou v § 5 odst. 2 zákona č. 101/2000 Sb.

V návaznosti na provedenou kontrolu byla kontrolované osobě uložena opatření k nápravě zjištěného stavu (tj. ukončení nezákonného zpracování osobních údajů). Sankce za uvedené jednání uložena nebyla, neboť s ohledem na informace, které měl Úřad k dispozici před registrací oznámení o tomto zpracování, bylo provedením registrace založeno legitimní očekávání města, že zpracování je v souladu s právem.

EURODAC – kontrola provedená na základě plánu kontrol Úřadu

Kontrola byla provedena na základě plánu kontrol Úřadu a povinnosti, která mu vyplývá z nařízení Evropského parlamentu a Rady č. 603/2013 ze dne 26. června 2013 o zřízení systému EURODAC.

Česká republika je členským státem systému EURODAC od roku 2004, přičemž zpracování osobních údajů v tomto systému příslušnými orgány se přímo řídí nařízením č. 603/2013. Architektura systému EURODAC je popsána v čl. 3 nařízení č. 603/2013, podle kterého se tento

systém skládá z ústřední databáze údajů o otiscích prstů a komunikační infrastruktury mezi ústředním systémem a členskými státy (v podobě šifrované virtuální sítě vyhrazené pro údaje systému EURODAC). Další součástí tohoto systému jsou národní přístupové body v jednotlivých členských státech. V systému EURODAC jsou zpracovávány osobní údaje žadatelů o mezinárodní ochranu (tj. státních příslušníků třetích zemí nebo osob bez státní příslušnosti, kteří podali žádost o mezinárodní ochranu) a dále státních příslušníků třetích zemí nebo osob bez státní příslušnosti zadržených příslušnými orgány v souvislosti s neoprávněným překročením hranice členského státu. U obou kategorií je dále podmínkou pro zpracování osobních údajů věk – musí se jednat o osoby starší 14 let. K otiskům prstů jsou dále přiřazeny informace o členském státu, který otisky do systému vložil, datu sejmutí otisků prstů, místu a datu podání žádosti o mezinárodní ochranu, pohlaví žadatele a případně další informace ohledně jeho příjezdu či odjezdu na a z území členských států, anebo datum rozhodnutí o podané žádosti. Osobní údaje žadatele o mezinárodní ochranu jsou v ústředním systému EURODAC uchovávány po dobu deseti let od data sejmutí otisků prstů a poté jsou automaticky vymazány, u osob zadržených při neoprávněném překročení vnější hranice členských států je tato lhůta 18 měsíců. Otisky prstů vložené do systému EURODAC lze v souladu s nařízením č. 603/2013 využít pouze k porovnání s otisky prstů státních příslušníků třetích zemí nebo osob bez státní příslušnosti, kteří se neoprávněně zdržují na území některého členského státu, a to za účelem ověření, zda tato osoba již dříve nepodala žádost o mezinárodní ochranu v jiném členském státě. Správcem osobních údajů zpracovávaných příslušnými orgány České republiky v systému EURODAC je Odbor azylové a migrační politiky Ministerstva vnitra ČR (OAMP). Úkoly OAMP spočívají především v koordinaci činností a metodickém vedení a dále v komunikaci s dalšími členskými státy při posuzování konkrétních případů. K osobním údajům zpracovávaným v systému EURODAC mají dále přístup útvary Policie ČR (zejména Ředitelství služby cizinecké policie, odbory cizinecké policie jednotlivých krajských ředitelství Policie a Kriminalistický ústav Praha). Role Kriminalistického ústavu Praha ve vztahu k systému EURODAC spočívá zejména ve vkládání údajů do tohoto systému v případě, kdy nebyly otisky prstů pořízeny v elektronické formě, ale daktyloskopickou černí, a dále provádí verifikaci shody při ověřování otisků údajů vůči systému EURODAC. Cizinecká policie je při zpracování osobních údajů v systému EURODAC v postavení vkladatelského pracoviště, nemá tedy oprávnění vložené údaje měnit či doplňovat.

Kontrolou byl prověřen postup OAMP, Kriminalistického ústavu Praha a cizinecké policie v Přijímacím středisku cizinců Zastávka, a to včetně posouzení opatření přijatých k zajištění bezpečnosti osobních údajů zpracovávaných v systému EURODAC, přičemž nebylo zjištěno žádné porušení povinností vyplývajících z nařízení č. 603/213 a subsidiárně ze zákona č. 101/2000 Sb.

Inspektorka Jana Rybínová

Kontrola informačního systému společnosti Falck Emergency, a.s.

Stěžovatel Úřadu oznámil, že i tři měsíce po ukončení pracovního poměru u společnosti Falck Emergency a.s. (dále jen „Společnost"), která poskytuje dopravní zdravotní služby, má stále ze svého mobilního telefonu elektronický přístup do informačního systému (dále také „FOS") Společnosti, jmenovitě do plánu rozvozu pacientů.

Kontrolou bylo zjištěno, že v průběhu roku 2017 u Společnosti skončil pracovní poměr šest zaměstnancům na pozici řidiče, přičemž pěti pracovníkům byl odebrán přístup do FOS ke dni, ke kterému byl jejich pracovní poměr ukončen, jednomu z pracovníků byl přístup zablokován až

po více než 4 měsících po ukončení pracovního poměru a bylo zjištěno, že mu byly i nadále zpřístupňovány osobní a citlivé údaje převážených pacientů. Dle Společnosti byla tato skutečnost zapříčiněna technickým nedostatkem právě používané verze 5.1.1 operačního systému Android informačního systému FOS, který umožňoval změnit heslo uživatele bez znalosti původního hesla. Zaměstnanec využil znalosti svého uživatelského jména pro přímý přístup do FOS a díky uvedené chybě si změnil heslo, čímž mu byl umožněn přístup do FOS z vlastního technického zařízení (mobilní telefon) bez nutnosti využít chráněný tablet Společnosti. Zaměstnavatele o této skutečnosti zaměstnanec neinformoval. Zároveň bylo zjištěno, že FOS umožňuje provádět kontrolu aktivit na poštovním účtu Společnosti, ze kterého vyplývá, jaký byl použit typ přístupu, z jaké IP adresy a v jakém datu, resp. čase. Z předloženého přehledu vyplývalo, že dne 18. července 2017 bylo do systému FOS přistoupeno prostřednictvím mobilního zařízení z IP adresy, která není adresou používanou Společností.

Společnost tím, že neoprávněně zpřístupnila osobní a citlivé údaje pacientů zpracovávané ve FOS v období od 5. dubna do 10. srpna 2017 osobě, která již ukončila pracovní poměr u Společnosti, neměla nastaveny dostatečné kontrolní mechanismy tak, aby zabránila neoprávněnému přístupu k osobním, resp. citlivým údajům, tedy dostatečně neposoudila rizika ve smyslu § 13 odst. 3 písm. c) zákona č. 101/2000 Sb., čímž porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. Společnost v rámci kontroly sdělila, že může odpovědně prohlásit, že šlo o zcela výjimečný případ a opakovanou kontrolou všech přístupových práv nebylo zjištěno žádné další obdobné selhání.

V rámci kontroly Společnost uvedené porušení napravila tím, že zablokovala přístup bývalému zaměstnanci, dále zavedla automatickou notifikaci pro IT specialistu o každé změně hesla i o každém přístupu do FOS z cizího zařízení, aktuální přístupová jména a hesla zná vždy jen IT specialista a operační manažer, který je přiděluje a jejich aktuálnost kontroluje na čtvrtletní bázi.

Správní řízení o uložení opatření k odstranění zjištěných nedostatků ve smyslu § 40 zákona č. 101/2000 Sb. nebylo se Společností vedeno, neboť tato odstranila protiprávní stav v průběhu kontroly. V navazujícím správním řízení byla Společnosti uložena pokuta za správní delikt ve výši 8000 Kč.

Systém správy identit na Jihočeské univerzitě v Českých Budějovicích

Kontrola Jihočeské univerzity v Českých Budějovicích (dále jen „Univerzita“) byla zahájena na základě kontrolního plánu Úřadu pro rok 2017 a oprávnění vyplývajícího z § 33 odst. 3 zákona č. 101/2000 Sb., Kontrola byla zaměřena na rozsah zpracovávaných údajů, jejich zabezpečení v rozsahu požadovaném dle § 13 zákona č. 101/2000 Sb., plnění informační povinnosti vůči subjektům údajů a dobu uchování v systémech správy identit univerzit, předávání údajů třetím stranám a plnění povinnosti ve smyslu § 6 zákona č. 101/2000 Sb.

Kontrolou bylo zjištěno, že Univerzita provozuje Systém správy identit (Identity Management – dále také „IdM“), který je založen na centrálním úložišti, v němž je uchovávána identita uživatele, tedy jednoznačná identifikace fyzické osoby a dále jí přiřazené uživatelské role. V univerzitním prostředí se tak jedná o studenty, pedagogy a další pracovníky Univerzity. Uživatelská role pak kromě oprávnění k vlastnímu přístupu do informačních systémů (dále také „IS“) přesně vymezuje rozsah přístupových oprávnění (autorizace) v daném IS.

Do daného IS jsou z centrálního úložiště přenášeny pouze ty údaje o uživateli, které jsou pro využití funkcionalit IS nezbytné. Z jednoho místa pak oprávněný uživatel-administrátor přiděluje a modifikuje oprávnění „běžných" uživatelů, např. při změně pracovního zařazení, přechodu pedagoga na jinou fakultu, změnu studijního oboru studenta apod. Navazující IS jsou synchronizovány se stavem v centrálním úložišti. Systémy správy identit mohou dále ovládat i další technické prostředky, např. řízení vstupu do určitých budov/prostor. Systém správy identit slouží na Univerzitě ke správě životního cyklu identit a předávání údajů o identitách do dalších komponent informačního systému Univerzity.

V systému IdM bylo ke dni 2. června 2017 uchováváno 71 094 identit, z toho jich bylo aktivních 12 292. Doba uchování neaktivních identit byla u zaměstnanců (resp. osobních spisů vedoucích a ostatních zaměstnanců) i studentů (resp. osobních spisů studentů) stanovena na 45 let.

V průběhu kontroly Univerzita provedla analýzu oživování identit z důvodů opětovného zápisu ke studiu a zaměstnanců. Na základě provedené analýzy Univerzita sdělila, že ze statistik stanoví lhůtu pro uchování neaktivních identit na sedm let. Identity budou smazány sedm let po ukončení právního vztahu k Univerzitě, u neaktivních identit, které budou uchovávány v IdM, budou uchovávány jen nezbytné údaje (jméno, příjmení, uživatelské jméno, id Number, osobní čísla zdrojových agend, e-mail), které budou pseudonymizovány. Dále Univerzita uvedla, že pokud od ní bude subjekt údajů vyžadovat poskytování služeb i po ukončení právního vztahu, budou jeho osobní údaje v IdM uchovávány po poskytnutí souhlasu žádajícího subjektu údajů.

Univerzita jako správce osobních údajů studentů, zaměstnanců a účastníků celoživotního vzdělávání zpracovávaných v Systému správy identit porušila ustanovení § 5 odst. 1 písm. e) zákona č. 101/2000 Sb., neboť stanovila dobu uchování osobních údajů studentů, zaměstnanců a účastníků celoživotního vzdělávání v systému IdM, resp. dobu uchování jejich tzv. neaktivních identit na 45 let, takto stanovená doba uchování není nezbytná k účelu jejich zpracování, kterým je správa životního cyklu identit a předávání údajů o identitách do dalších komponent informačního systému Univerzity.

Úřad, aniž zahájil řízení, věc ve smyslu § 40a zákona č. 101/2000 Sb. odložil, protože ze strany Univerzity došlo k nápravě protiprávního stavu bezprostředně poté, kdy se zjistilo porušení povinnosti. Navíc vzhledem k tomu, že nebyla při zpracování osobních údajů subjektů údajů v systému IdM v plném rozsahu využita doba uchování původně Univerzitou stanovena na 45 let, a upustil od uložení pokuty dle § 40a zákona č. 101/2000 Sb.

Právo být zapomenut – společnost Google Czech Republic, s.r.o.

Inspektorka Úřadu na základě podnětu subjektu údajů, jehož údaje byly zpracovávány prostřednictvím odkazů na internetu a který žádal o jejich odstranění, čímž uplatnil „právo být zapomenut", provedla šetření stížnosti, a ve smyslu § 3 zákona o kontrole č. 255/2012 Sb. vyzvala k zablokování přístupu na specifikované URL adresy prostřednictvím vyhledávače Google, a to společnost Google Czech Republic, s.r.o. Výzvu k zablokování doložila inspektorka Úřadu i sdělením, že stěžovatel disponuje soudním rozhodnutím, jehož kopie je součástí spisového materiálu vedeného ve věci, na základě něhož se tištěná média omluvila za nepravdivé informace o jeho soukromém životě, zveřejněné v článcích v těchto médiích a které jsou rovněž obsahem některých článků, zveřejňovaných prostřednictvím uvedených URL adres.

Následně obdržela inspektorka Úřadu odpověď od společnosti Google Czech Republic, s.r.o. s informací, že požadavek na zablokování přístupu byl postoupen společnosti Google Inc., se

sídlem 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA s tím, aby Úřad zaslal požadavek přímo společnosti Google Inc., která je vlastníkem, provozovatelem a poskytovatelem vyhledávače Google.

Shodnou výzvu k zablokování přístupu ke specifikovaným URL adresám inspektorka Úřadu zaslala společnosti Google Inc. Od společnosti Google Inc. následně Úřad obdržel informaci o tom, že ve vyhledávači Google bylo zablokováno vyhledávání a zobrazení uvedených webových stránek. Při ověřování provedených opatření bylo kontrolujícími zjištěno, že na URL, které ve výčtu v původní žádosti nebylo specifikováno, dochází taktéž ke zveřejňování osobních údajů stěžovatele, z toho důvodu byla zaslána dodatečně Google Inc. výzva k zablokování uvedené URL adresy.

Inspektorka Božena Čajková

Kontrola monitorování a následného zpracování záznamů pořízených během výkonu služby u Městské policie Hradec Králové

Kontrola byla zahájena na základě plánu kontrol Úřadu na rok 2017 a jejím předmětem bylo plnění povinností stanovených zákonem č. 101/2000 Sb., v souvislosti s monitorováním a následným zpracováním záznamů pořízených během výkonu služby strážníky městské policie. Strážníci městské policie pořizují videozáznamy o průběhu některých svých zákroků na základě § 24b odst. 1 zákona č. 553/1991 Sb., o obecní policii. Tyto záznamy následně ukládají na datová úložiště městské policie. Některé z těchto záznamů následně také předávají orgánům činným v trestním řízení k dalšímu využití, případně dalším příslušným orgánům ke správnímu řízení. Některé videozáznamy ze zásahů městské policie také zpřístupňují občanům prostřednictvím médií. Videozáznamy určené médiím před předáním upravuje (anonymizuje) městská policie tak, aby osoby na nich zachycené nebyly rozpoznatelné. V kontrole byly posuzovány dva konkrétní záznamy pořízené během úkonů strážníků městské policie a zveřejněné na internetu, u nichž bylo nutno v důsledku nedostatečné anonymizace, resp. poskytnutí dodatečných informací (osobních údajů), dospět k závěru, že i v podobě, v jaké byly zveřejněny na internetu, obsahovaly osobní údaje subjektů údajů, vůči kterým byl zákrok strážníků směřován. V případě těchto videozáznamů tak nebyly dodrženy postupy přijaté pro anonymizaci videozáznamů, čímž došlo k zásahu do práv osob na těchto záznamech zachycených. Městská policie tedy postupovala v rozporu s požadavky § 13 odst. 1 zákona č. 101/2000 Sb. Kontrolou bylo dále zjištěno, že městská policie nevede přehled o tom, jaké záznamy byly zveřejněny nebo zpřístupněny a jakému okruhu adresátů. Po předání či zpřístupnění záznamů tak ztrácí možnost zpětně ověřit, zda zveřejněný záznam byl skutečně pořízen strážníky městské policie, nebyl dále neautorizovaně upraven či doplněn o informace z jiných zdrojů. Tento postup byl vyhodnocen jako porušení § 13 odst. 3 písm. d) zákona č. 101/2000 Sb.

V návaznosti na tuto kontrolu provedla městská policie opatření směřující k nápravě zjištěných nedostatků. Za uvedené jednání byla následně uložena sankce ve výši 30 000 Kč.

Zpracování osobních údajů na webových stránkách společnosti FORDESK, s.r.o.

Předmětem kontroly, která byla zahájena na základě podnětu, bylo zpracování osobních údajů v souvislosti se službou, kterou kontrolovaná osoba poskytuje prostřednictvím webových stránek www.firmo.cz, a která spočívá v poskytování přehledných a kompletních informací o právnických i fyzických osobách – podnikatelích.

Při poskytování výše popsané služby kontrolovaná osoba shromažďuje z veřejných rejstříků volně dostupné informace (open data) o podnikatelích, tyto sdružuje a dále zpřístupňuje na www.firmo.cz. Postup kontrolované osoby je tak obecně v souladu s § 5 odst. 2 písm. d) zákona č. 101/2000 Sb. V případě informací přebíraných z živnostenského rejstříku je však nutno zohlednit, že dle § 60 odst. 3 písm. b) zákona o živnostenském podnikání č. 455/1991 Sb. dochází po uplynutí 4 let ode dne zániku posledního živnostenského oprávnění podnikatele k převedení informací o podnikateli z veřejné části tohoto rejstříku do části neveřejné. Po tomto převedení se dané osobní údaje již z povahy věci nedají považovat za údaje oprávněně zveřejněné a aplikace § 5 odst. 2 písm. d) zákona č. 101/2000 Sb. již není možná. Ve vztahu k těmto osobním údajům tak kontrolovaná osoba nedisponuje žádným právním titulem. Kontrolou bylo dále prověřeno, zda kontrolovaná osoba přijala opatření navazující na zákonné omezení veřejnosti údajů vyplývající z § 60 odst. 3 písm. b) zákona č. 455/1991 Sb. a došli k závěru, že opatření přijatá kontrolovanou osobou nevedou k zajištění žádoucího stavu, tj. skutečné aktualizaci zpracovávaných osobních údajů a výmazu těch, které již nejsou veřejně dostupné. Kontrolovaná osoba tím porušila povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb. Kontrolovaná osoba dále porušila povinnost vyplývající z § 21 odst. 2 zákona č. 101/2000 Sb., neboť nevymazala osobní údaje stěžovatelky na základě její žádosti, ačkoli v době žádosti nebyly osobní údaje stěžovatelky již veřejně dostupné.

V návaznosti na tuto kontrolu byla kontrolované osobě uložena opatření směřující k nápravě zjištěných nedostatků. Společnosti byla následně uložena pokuta ve výši 30 000 Kč.

Kontrola zabezpečení a přístupů k záznamům z kamerového systému provozovaného v domě bytového družstva Ohradní

Kontrola byla zahájena na základě podnětu, jehož předmětem byla manipulace se záznamy z kamerového systému provozovaného v bytovém domě.

Kontrolou bylo zjištěno, že kontrolovaná osoba provozuje v bytovém domě, který je v jejím vlastnictví, kamerový systém se záznamem (kamery monitorují hlavní i zadní vchody do domu, vstupní halu se schránkami, prostor před výtahy a kabinu výtahu). Kamery umístěné u hlavního vchodu monitorují současně i veřejné prostranství před domem (parkoviště). S ohledem na rozsah a zaměření kamerového systému, resp. jednotlivých kamer, a s přihlédnutím k účelu jeho provozu, dospěli kontrolující k závěru, že s výjimkou kamer monitorujících parkoviště lze aplikovat právní titul vyjádřený v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Ve vztahu ke kamerám monitorujícím parkoviště bylo konstatováno porušení povinnosti uvedené v § 5 odst. 2 zákona č. 101/2000 Sb., neboť pro posuzované zpracování osobních údajů nebyl shledán zákonem předvídaný právní titul. Jiné porušení povinností stanovených zákonem č. 101/2000 Sb. kontrolou zjištěno nebylo, a to ani ve vztahu k předmětu podnětu stěžovatele (nezákonná manipulace se záznamy).

Kontrolovaná osoba provedla v návaznosti na tuto kontrolu opatření směřující k nápravě zjištěného stavu. Za uvedené jednání byla bytovému družstvu uložena sankce ve výši 5000 Kč.

Inspektor Petr Krejčí

Kontrola společnosti Čedok, a.s. na základě kontrolního plánu Úřadu

Úřad pro ochranu osobních údajů provedl a ukončil kontrolu společnosti Čedok a.s., se sídlem Na Příkopě 857/18, Nové Město, 110 00 Praha 1, IČ: 60192755 (dále jen „kontrolovaná osoba").

Tato kontrola byla provedena na základě kontrolního plánu Úřadu na rok 2017. Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v souvislosti se zpracováním osobních údajů klientů kontrolované osoby získaných na základě s nimi uzavřené Smlouvy o zájezdu nebo Smlouvy o poskytnutí jednotlivé služby, včetně souvisejícího vyřizování žádostí o vízum a předávání osobních údajů pověřenému zpracovateli, průvodci, delegátovi či další osobě oprávněné poskytovat služby cestovního ruchu do vybraných konkrétních třetích zemí, které nejsou členskými státy Evropské unie, tedy mimo hranice schengenského prostoru. Cílem kontroly bylo především prověřit dodržování povinností stanovených správci a zpracovateli zákonem č. 101/2000 Sb., při předávání osobních údajů subjektů údajů do těch třetích zemí, které nejsou členskými státy Evropské unie, a nevztahuje se na ně zákaz omezování volného pohybu osobních údajů vyplývající z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas a kterou je Česká republika vázána, a do těch třetích zemí, do kterých nejsou osobní údaje předány na základě rozhodnutí orgánu Evropské unie, tedy do třetích zemí, do nichž mohou být osobní údaje dle ustanovení § 27 odst. 4 zákona č. 101/2000 Sb. předány, ale pouze když k tomuto předání vydá ÚOOÚ povolení. Z těchto třetích zemí byly vytipovány Rusko a Turecko. Jelikož šlo o kontrolu prováděnou dle ustanovení § 31 zákona č. 101/2000 Sb., na základě kontrolního plánu, bylo jí prověřeno dodržování kontrolovanou osobou s ohledem na uvedený předmět kontroly všech ustanovení zákona č. 101/2000 Sb., v nichž jsou stanoveny povinnosti správci/zpracovateli.

Kontrolovaná osoba stanovila účely, k nimž mají být osobní údaje zpracovány, jimiž jsou zpracování osobních údajů zákazníků za účelem uzavření a plnění Smlouvy o zájezdu, Smlouvy o poskytování jednotlivých služeb, Smlouvy o členství v Clubu Čedok týkající se věrnostního systému za účelem realizace věrnostních slev a poskytování nabídek služeb Čedok věrným zákazníkům, účastníků zájezdu nebo účastníků poskytnutých jím jednotlivých služeb a třetích osob, ve prospěch nichž je zákazníkem některá z těchto smluv s kontrolovanou osobou uzavřena, a za účelem nabízení obchodu nebo služeb subjektu údajů, jimiž jsou dle ustanovení § 4 písm. d) zákona č. 101/2000 Sb. fyzické osoby, k nimž se osobní údaje vztahují, které má uvedeny ve Všeobecných smluvních podmínkách cestovní kanceláře Čedok a.s., které jsou nedílnou součástí těchto smluv, jsou kontrolovanou osobou zveřejněny na jejích internetových stránkách a obsahují je také katalogy zájezdů kontrolované osoby. Do vytipovaných třetích zemí jsou osobní údaje předávány kontrolovanou osobou dle jí vydaných povolení k jejich předání do těchto zemí Úřadem pro ochranu osobních údajů.

Provedenou kontrolou bylo zjištěno, že kontrolovaná osoba při zpracování osobních údajů subjektů údajů za předmětnými účely dodržuje povinnosti jí stanovené, jakožto správci ve smyslu ustanovení § 4 písm. j) zákona č. 101/2000 Sb., a tudíž nebylo zjištěno porušení zákona o ochraně osobních údajů.

Kontrola dodržování povinností správce/zpracovatele osobních údajů ve společnosti INDEX NOSLUŠ, s.r.o.

Úřad pro ochranu osobních údajů provedl a ukončil kontrolu společnosti INDEX NOSLUŠ s.r.o., se sídlem Hornokrčská 583/30, Krč, 140 00 Praha 4, IČ: 25131419 (dále jen „kontrolovaná osoba").

Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, v souvislosti

se zpracováním osobních údajů subjektů údajů, které nebyly v souladu s účelem jejich shromažďování ve smyslu ustanovení § 4 písm. i) a § 20 zákona č. 101/2000 Sb. řádně zlikvidovány, přičemž písemnosti obsahující tyto osobní údaje byly nalezeny Městskou policií Města Slaný na veřejně přístupném místě.

Součástí předání věci Úřadu Městskou policií města Slaný bylo i větší množství listin, zejména pracovněprávní a daňové dokumenty, resp. registrační smlouvy, dohody o provedení práce, potvrzení o návštěvě školy a prohlášení poplatníka daně z příjmu fyzických osob ze závislé činnosti a z funkčních požitků, obsahující osobní údaje agenturních zaměstnanců kontrolované osoby z let 1999–2003, v souvislosti s činností kontrolované osoby jako agentury práce vykonávané na základě povolení uděleného ministerstvem práce a sociálních věcí. Kontrolou bylo zjištěno, že se jedná celkem o 177 souborů dokumentů obsahujících v jednotlivých průsvitných igelitových deskách (eurofólie formát A4) vždy odděleně pro jeden subjekt údajů za dané časové období několik dokumentů obsahujících v souhrnu osobní údaje v rozsahu jméno, příjmení, datum narození, rodné číslo, číslo občanského průkazu, státní příslušnost, adresa trvalého bydliště, adresa přechodného bydliště, telefonní kontakt, e-mailová adresa, název a adresa zdravotní pojišťovny, zdravotní stav, zdravotní omezení, zdravotní průkaz, název školy, název fakulty, ročník, adresa školy, potvrzení o studiu, znalosti/zkušenosti/schopnosti povolení. V těchto souborech dokumentů byly uvedeny osobní údaje některých subjektů údajů i opakovaně, ale s vyplněnými osobními údaji za jiné časové období zprostředkovaného zaměstnání, tedy se jednalo o listiny s osobními údaji celkem 136 subjektů údajů. Kontrolujícími bylo zjištěno, že se jednalo o důvodné shromažďování osobních údajů kontrolovanou osobou i z hlediska jejich rozsahu v souladu s účelem jejich zpracování.

Vzhledem k tomu, že kontrolovaná osoba řádně nezabezpečila zpracovávané osobní údaje svých agenturních zaměstnanců před jejich neoprávněným zpřístupněním, a tím, že byly nalezeny na veřejně přístupném místě, nezajistila jejich řádnou likvidaci, čímž porušila ustanovení § 13 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů, které stanoví správci a zpracovateli 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. Tato povinnost platí i po ukončení zpracování osobních údajů. Dále porušila ustanovení § 20 odst. 1 tohoto zákona, v němž je stanovena povinnost správci nebo na základě jeho pokynu zpracovateli provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, za což byla kontrolované osobě ve správním řízení uložena pokuta ve výši 30 000 Kč.

Kontrola na základě nesouhlasu instalace kamerového systému v prostoru šaten ve společnosti Novoměstské služby, s.r.o.

Úřad pro ochranu osobních údajů provedl a ukončil na základě podnětu kontrolu společnosti Novoměstské služby s.r.o., se sídlem Soškova 1346, 592 31 Nové Město na Moravě, IČ: 03022641, (dále jen „kontrolovaná osoba"), která je provozovatelem Městských lázní v Novém Městě na Moravě, jejichž vlastníkem je město Nové Město na Moravě. Podstatou podnětu návštěvníka Městských lázní byl nesouhlas s instalací většího množství kamer, kterými mají být sledovány prostřednictvím kamerového systému se záznamem prostory šaten určených k převlékání, včetně šatních skříněk, chodbiček, laviček apod., přičemž tyto prostory nejsou označeny informačními cedulkami, a není tedy zřejmé, které prostory šaten jsou a které nejsou monitorovány kamerami,

a proto se oznamovatel domníval, že těmito kamerami, které zachycují mimo jiné i převlékající se osoby, včetně nahých nezletilých dětí, dochází k porušování zákona o ochraně osobních údajů.

Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v souvislosti se zpracováním osobních údajů subjektů údajů získaných z instalovaného kamerového systému se záznamem prostřednictvím kamer umístěných zejména v prostorách šaten a místech určených k převlékání návštěvníků Městských lázní v Novém Městě na Moravě.

Kontrolou bylo zjištěno, že kontrolovaná osoba provozuje kamerový systém s obrazovým záznamem v prostorách Městských lázní Nové Město na Moravě za účelem, jímž je ochrana života, zdraví a majetku návštěvníků a zaměstnanců těchto lázní a rovněž i majetku kontrolované osoby. Převlékací kabinky a šatní skříňky jsou barevně odlišeny také proto, aby bylo zřejmé dle instalovaných cedulek, jaké prostory jsou kamerami monitorovány, tedy kamery kamerového systému s obrazovým záznamem provozovaného kontrolovanou osobou nemonitorují, resp. nezabírají, prostor převlékacích kabinek, určených k převlékání návštěvníků Městských lázní Nové Město na Moravě. Kamery tohoto kamerového systému s obrazovým záznamem monitorují, a tedy zabírají pouze prostory určené pro ukládání a odkládání věcí, tj. šatny a šatní skříňky určené pro uložení osobních věcí návštěvníků Městských lázní Nové Město na Moravě. Na převlékacích kabinkách jsou vylepeny cedulky obsahující text „Převlékací kabinka" s pokyny pro návštěvníky. V „Návštěvním řádu Městských lázní", umístěném na nástěnce určené pro návštěvníky Městských lázní Nové Město na Moravě, je stanovena povinnost návštěvníků převlékat se v převlékacích kabinkách, v šatně do jím vybrané šatní skříňky uložit všechny své osobní věci, pomocí čipového náramku mu při vstupu do těchto lázní vydaného, tuto šatní skříňku uzamknout a tento čipový náramek po celou dobu návštěvy areálu Městských lázní Nové Město na Moravě nosit na viditelném místě, například na ruce. Pokud by se tedy návštěvník Městských lázní Nové Město na Moravě převlékal v dosahu kamer kamerového systému s obrazovým záznamem, ač má k tomu vyhrazený kamerami nemonitorovaný prostor v převlékacích kabinkách, porušoval by tím „Návštěvní řád Městských lázní", v němž je stanoveno místo určené k převlékání a kontrolované osobě toto nelze přičítat k její tíži, resp. považovat za porušení zákona, jestliže by došlo k monitorování převlékajících se osob v místech, která k tomu nejsou vyhrazená. Jelikož k záznamu z kamerového systému jen v mimořádných událostech mají přístup pouze oprávněné osoby, je tak vyloučené jakékoliv sledování návštěvníků lázní. V daném případě nebylo zjištěno porušení zákona o ochraně osobních údajů.

Inspektor Daniel Rovan

Kontrola brokerské společnosti 4LifeFinance, s.r.o. zprostředkovávající finanční služby

Úřad provedl a ukončil kontrolu na základě podnětu stěžovatele, který ve své stížnosti uvedl, že se zúčastnil v sídle kontrolované společnosti schůzky za účelem revize jeho pojistných smluv. Během schůzky mělo vyjít najevo, že účastníci schůzky za kontrolovanou společnost měli k dispozici jeho jméno, telefonní číslo, údaje o tom, že je pojištěn a u koho, a rovněž údaje o době, kdy má jeho pojištění skončit, a to aniž by byl jejich klientem. Stejné údaje pak měla mít společnost k dispozici i o jeho manželce. Stěžovatel požádal na místě schůzky o uvedení zdroje těchto osobních údajů, což mu mělo být přislíbeno.

V rámci kontroly kontrolovaný předložil Smlouvu o spolupráci, uzavřenou s brokerskou společností, jejímž předmětem je zplnomocnění finančního poradce, aby v jeho zastoupení vyvíjel činnost směřující k vyřizování jeho záležitostí podle pokynů objednatele. Touto činností se rozumí především zprostředkování prodeje finančních produktů institucí smluvně vázaných s objednatelem. K této činnosti je poradce oprávněn využívat know-how objednatele i jeho interní informační systém.

Ve smlouvě je uveden závazek finančního poradce, že bude pro společnost vykonávat v roli zpracovatele zpracování osobních údajů subjektů údajů se smluvním vztahem ke společnosti, nebo subjektů údajů se zájmem o finanční produkty finančních institucí smluvně vázaných se společností. Dále je zde uvedeno, že finanční poradce se zavazuje, že klientu, který o to požádá, poskytne informaci o osobních údajích, jež o něm společnost zpracovává v interním informačním systému, a to ve smyslu § 12 zákona č. 101/2000 Sb., o ochraně osobních údajů (tj. zejména o účelu zpracování, o osobních údajích o klientu zpracovávaných, o příjemcích osobních údajů) a že Smlouva splňuje náležitosti smlouvy o zpracování osobních údajů ve smyslu ustanovení § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů.

Dále z vnitřních předpisů vyplynulo, že poradce nesmí shromažďovat osobní údaje klienta předtím, než získá od klienta nebo potenciálního klienta souhlas s jejich zpracováním elektronicky nebo písemně.

Kontrolou byly prověřovány povinnosti vyplývající ze znění § 6, neboť z kontrolních zjištění vyplynulo, že kontrolovaná společnost je zpracovatelem na základě smlouvy uzavřené se správcem osobních údajů stěžovatele, a dále povinnosti vyplývající ze znění § 12 odst. 1–4.

Kontrolou bylo zjištěno porušení § 12 odst. 2 písm. b) zákona č. 101/2000 Sb., neboť jak z uvedeného paragrafu, tak z uzavřené smlouvy o spolupráci mezi kontrolovaným a partnerskou společností působící v roli správce osobních údajů vyplývá povinnost poskytnout klientovi informaci o osobních údajích, které o něm společnost zpracovává v IIS (interním informačním systému), což kontrolovaný neučinil dostatečně.

Vzhledem k tomu, že kontrolovaný závadný stav napravil bezprostředně po ukončení kontroly, nebylo zahájeno správní řízení o nápravných opatřeních. Rovněž bylo upuštěno od uložení pokuty, neboť se jednalo o zcela ojedinělý případ.

Ze zkušeností Úřadu v dané oblasti vyplývá, že se jedná o velice častou praxi poskytovatelů tohoto druhu služeb a že se výše uvedenému správci podařilo vybudovat poměrně rozsáhlou síť zpracovatelských partnerských společností. Z tohoto důvodu byla do plánu kontrol na rok 2018 zařazena i kontrola této brokerské společnosti.

Kontrola základní školy v Trutnově v souvislosti se zřízením elektronické adresy ve formátu, který obsahoval osobní údaje žáků umožňující jejich identifikaci

Úřad na základě stížnosti provedl a ukončil kontrolu jedné z trutnovských základních škol. Stěžovatelka ve své stížnosti uvedla, že žákům čtvrté třídy měly být bez souhlasu či informování zákonných zástupců zřízeny e-mailové schránky pomocí služby Google Suite. E-mailové adresy byly vytvořeny ve formátu jmeno.prijmeni@doména školy. Při založení těchto e-mailů měly být podle stížnosti společnosti Google předány osobní údaje žáka minimálně v rozsahu jméno, příjmení a škola, kterou žák navštěvuje.

V rámci kontroly bylo zjištěno, že po upozornění kontrolovaného stěžovatelkou, škola informovala i ostatní zákonné zástupce žáků o svém postupu při zpracování osobních údajů. Škola

dále uvedla, že zřízení internetových adres žáků je nutné pro splnění požadavků Rámcového vzdělávacího programu. Z vyjádření ministerstva školství, mládeže a tělovýchovy ke stížnosti vyplynulo, že cílem Rámcového vzdělávacího programu (RVP ZV) je, aby byli žáci schopni bezpečně pracovat v prostředí elektronické pošty a rozeznat možná rizika tak, aby sami sebe a ostatní neohrozili. Pokud by zřízení schránek mělo vyžadovat využití osobních dat žáků, je nutné postupovat v souladu s právními předpisy o ochraně osobních údajů. Rámcový plán ani ministerstvo tedy nenutí školy ke konkrétní podobě e-mailových adres, naopak upozorňuje na nutnost dodržení povinností k ochraně osobních údajů.

Škola předložila interní dokument *Směrnice na ochranu osobních údajů*, upravující pravidla pro ochranu osobních dat zaměstnanců, žáků školy, také osob, které jsou ke škole v jiném pracovněprávním vztahu. V něm je mimo jiné uvedeno, že ke zpracování osobních údajů a citlivých údajů nad rozsah daný právními předpisy je nezbytný souhlas osoby, jejíž osobní údaje jsou zpracovávány. Organizace před zahájením zpracování osobních dat musí prokazatelně zajistit plnou informovanost těchto osob v rozsahu daném zákonem č. 101/2000 Sb., o ochraně osobních údajů, v platném znění, a poučení o jejich právech. Zajistí poučení o povinnosti zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení zaměstnání nebo příslušných prací. Za žáky podepisují souhlas se zpracováním jejich zákonní zástupci. Používaný tzv. „generální souhlas" ale mezi účely zpracování neuváděl službu G Suite pro vzdělání.

Dále kontrolovaný uvedl, že má se společností Google Inc. uzavřenu on-line smlouvu, a to pouze a výhradně na službu G Suite pro vzdělání. Žáci k jiným službám, u kterých jsou vyžadovány jejich osobní údaje, přístup nemají, a pokud se o to pokusí, je jejich účet automaticky zablokován. V rámci G Suite pro vzdělání měl kontrolovaný nastaveno omezení přístupu ke službám sociální sítě G+. Při zřizování účtů se v administraci Google Suite importuje tabulka csv, ve které jsou tři sloupce: jméno, příjmení, defaultní heslo. Při prvním přihlášení žáka účet vyžaduje heslo o min. délce osm znaků, které si určí žák. Zároveň je systémem žák informován o podmínkách zřízení e-mailového účtu, které musí přijmout. K administraci mají přístup pouze správci sítě, kteří jsou zaměstnanci školy. Mají pravomoc zablokovat jednotlivé účty, měnit hesla, nebo účty smazat. Při ukončení docházky žáka na škole dojde ke zrušení jeho e-mailového účtu.

Ze smlouvy s Google Inc. vyplývá standardní záruka ochrany pro uživatele před neoprávněným přístupem. Odpovědnost společnosti Google se nevztahuje na vnitřní správu nebo administraci služeb poskytovaných zákazníkovi, společnost Google je pouze zpracovatelem dat. V bodě Prohlášení, záruky a právní omezení je mimo jiné uvedeno, že zákazník souhlasí s tím, že je zodpovědný za získání rodičovského souhlasu se shromažďováním osobních údajů žáků, které budou použity ve spojitosti s poskytováním nebo používáním služeb zákazníkem a koncovými uživateli; koncoví uživatelé jsou definování jako jednotlivci, kterým zákazník umožní používání služeb. Ani z předloženého textu nevyplynula nutnost nastavit adresy pomocí jmen žáků.

Kontrolou byly prověřovány zejména povinnosti vyplývající ze znění § 5 odst. 1 písm. d), § 5 odst. 2, § 6 a § 11 odst. 1 a 2 zákona č. 101/2000 Sb. Z kontrolních zjištění vyplynulo, že kontrolovaná škola využívá k identifikaci koncového uživatele (žáka) v rámci služby G Suite pro vzdělávání jeho jméno a příjmení. Pomocí nich vytváří účet koncového uživatele (žáka). Protože není nezbytné používat jméno a příjmení žáka a jeho identifikaci lze provést méně invazivním zásahem do jeho soukromí, porušila tím § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. Dále bylo

zjištěno, že škola nedisponovala souhlasy zákonných zástupců žáků se zpracováním jejich osobních údajů k tomuto účelu, čímž porušila § 5 odst. 2 zákona č. 101/2000 Sb. Z kontrolních zjištění také vyplynulo, že kontrolovaný, jakožto správce osobních údajů, neinformoval zákonné zástupce subjektů údajů 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, čímž porušil § 11 odst. 1 zákona č. 101/2000 Sb. Z dalších kontrolních zjištění bylo patrné, že škola využívala tzv. „generální souhlas", který je zákonným zástupcům dětí předkládán k podpisu, rodič svým podpisem uděluje souhlas s rozsáhlým zpracováním osobních údajů dítěte a je po něm vyžadován souhlas i v případech, kde je toto zpracování osobních údajů uloženo zákonem. Dotčený rodič, kterému kontrolovaný tvrdí, že zpracování osobních údajů jeho dítěte probíhá na základě souhlasu, má tak o zpracování osobních údajů dítěte nesprávné informace a z pohledu kontrolovaného se jedná o nepravdivé a tím nedostatečné plnění informační povinnosti při shromažďování osobních údajů žáků. Tím dochází k porušení § 11 odst. 2 zákona č. 101/2000 Sb.

Vzhledem k tomu, že kontrolovaný projevil mimořádnou snahu napravit závadný stav bezprostředně po ukončení kontroly, nebylo zahájeno správní řízení o nápravných opatřeních.

Kontrola zpracování osobních údajů společnosti vytvářející databáze a obchodující s nimi ve společnosti SOLIDIS, s.r.o.

Na základě opakujících se stížností Úřad provedl a ukončil kontrolu společnosti obchodující s databázemi, SOLIDIS, s.r.o., zaměřenou na dodržování povinností stanovených zákonem č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů v databázích a jejich nabízení třetím osobám a dodržování povinností vyplývajících ze zákona č. 480/2004 Sb., o některých službách informační společnosti v souvislosti s rozesíláním obchodních sdělení pomocí elektronických prostředků.

Stěžovatelé opakovaně poukazovali na to, že byli telefonicky kontaktováni operátory, kteří nabízeli různé zboží nebo služby. Na dotazy oslovených, odkud mají jejich osobní údaje, obvykle přišla standardně připravená odpověď, ze které bylo patrné, že jejich osobní údaje byly nakoupeny od neurčitě specifikovaného správce osobních údajů, přičemž se tento správce zaručil, že data nabyl v souladu se zákonem. Nejčastěji uvedeným zdrojem byla společnost SOLIDIS.

Úřad provedl poslední kontrolu ve společnosti SOLIDIS, s.r.o., v roce 2013. Kontrola byla zaměřena na dodržování povinností stanovených zákonem č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů v databázích a jejich nabízení třetím osobám a dodržování povinností vyplývajících ze zákona č. 480/2004 Sb., o některých službách informační společnosti v souvislosti s rozesíláním obchodních sdělení pomocí elektronických prostředků. Kontrolou bylo zjištěno porušení povinností vyplývajících z § 7 odst. 2 a odst. 4 písm. c) zákona č. 480/2004 Sb.

Společnost SOLIDIS patří k jednomu z nejčastěji zmiňovaných správců, kteří dodávají zákazníkům databáze „na míru". Kontrola byla zaměřena zejména na přenositelnost souhlasu subjektu údajů se zpracováním jeho osobních údajů a informování subjektu o jejich předání třetím osobám.

Z kontrolních zjištění vyplynulo, že kontrolovaný osobní údaje získává v převážné míře z veřejně dostupných zdrojů, případně k nim získá přístup na základě pověření správce. V omezené míře jsou údaje získávány na základě licenčních smluv, ve kterých poskytovatel prohlašuje, že se jedná o zpracování v souladu se zákonem o ochraně osobních údajů a lze je zpracovávat

k účelu deklarovanému ve smlouvě. Kontrolovaný předložil kopie tří licenčních smluv podle § 90 a násl. zákona č. 121/2000 Sb., autorského zákona.

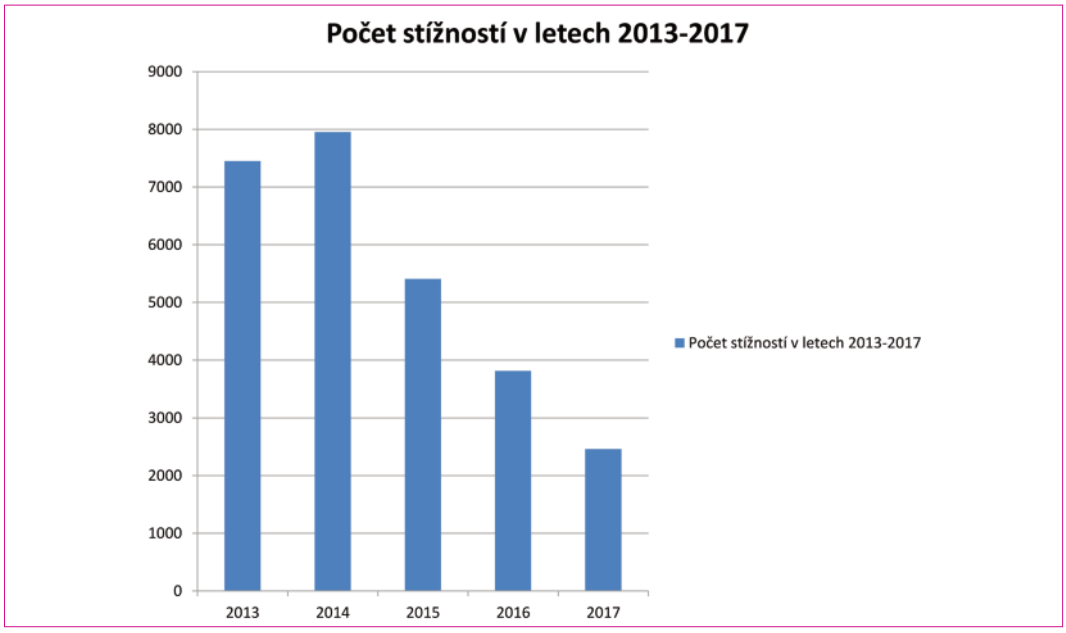
Dále kontrolovaný předložil bianko formulář objednávky, ve kterém bylo mimo jiné uvedeno, že kontrolovaný poskytne služby spočívající ve zpracování osobních údajů dle specifikace objednávky. Účel a rozsah osobních údajů je uveden ve specifikaci objednávky. Pokud je sjednán výstup, je tento dodán elektronicky ve formátu xls. Objednatel prohlašuje, že je seznámen se Všeobecnými obchodními podmínkami Poskytovatele, které jsou uvedeny na zadní straně této objednávky, a souhlasí s ujednáními zde uvedenými. Ty specifikují pojem služby jako *zejména marketingové průzkumy, tvorba speciálních databází, …, přičemž služby mohou zahrnovat zpracování osobních údajů*. Součástí služeb může být zpracování osobních údajů. Společnost provádí zpracování osobních údajů vlastními zaměstnanci.

Kontrolou byly prověřovány zejména povinnosti vyplývající ze znění § 5 odst. 1 písm. a) a b), § 5 odst. 2, odst. 5, odst. 7 a § 12 odst. 1–4 zákona č. 101/2000 Sb. Z kontrolních zjištění vyplynulo, že kontrolovaný koupil databázi subjektů údajů od jiného správce včetně deklarovaných souhlasů s jejich zpracováním. Vzhledem k tomu, že souhlasy subjektů údajů vedených v databázi jednoho správce a poskytnuté druhému správci nelze považovat za automatické souhlasy se zpracováním osobních údajů, došlo k porušení § 5 odst. 2. Jelikož kontrolovaný tyto osobní údaje využíval k oslovování a zasílání obchodních sdělení a navíc je dále poskytl dalším správcům bez souhlasu subjektů údajů, porušil § 5 odst. 5 a 7 zákona č. 101/2000 Sb. Dále z kontrolních zjištění vyplynulo, že kontrolovaný ani na opakovanou žádost subjektu údajů (stěžovateli) nepodal úplnou informaci o rozsahu zpracování a o zdroji osobních údajů, čímž nesplnil svoji povinnost vyplývající z § 12 odst. 2 písm. b) zákona č. 101/2000 Sb.

Kontrolovanému byla správním příkazem uložena nápravná opatření. Tato nápravná opatření společnost SOLIDIS ve stanoveném termínu splnila. Ve věci je na základě kontrolních zjištění se společností vedeno řízení o přestupku.

Inspektor Josef Vacula

NEVYŽÁDANÁ OBCHODNÍ SDĚLENÍ



Z výše uvedeného grafu je patrné, že počet doručených stížností na nevyžádaná obchodní sdělení dosáhl svého maxima v roce 2014, kdy bylo Úřadu doručeno téměř osm tisíc stížností. Od tohoto roku je však možné pozorovat sestupný trend v počtu přijatých podnětů. Tento trend je, dle názoru ÚOOÚ, možné vysvětlit především dvěma vlivy.

Prvním z těchto vlivů je zmenšení propagace slevových portálů. Fenomén slevových portálů u nás prožíval boom především okolo roku 2010. V následujících letech však zájem o slevové portály uvadal. Za tímto poklesem je možné hledat jak skutečnost, že slevové akce s nabízením zboží a služeb přestaly být tolik atraktivní, tak medializované kauzy některých slevových portálů, které sice vybraly peníze od svých zákazníků, ale protiplnění již neposkytly.

Druhým důvodem, který Úřad spatřuje jako rozhodující pro zmenšující se počet doručených podnětů, je skutečnost, že provozovatelé freemailových služeb začali své klienty před hromadnou a obtěžující poštou lépe chránit tím, že tento typ doručených zpráv automaticky končí ve složkách „hromadné" a „spam", aniž by uživatel e-mailového účtu musel pro tuto selekci učinit jediný krok.

V neposlední řadě je také třeba zmínit, že se též výrazně změnila edukace osob ve vztahu k elektronickým komunikacím a také jejich přístup k podání stížností. V předchozích letech ÚOOÚ často obdržel stížnosti, které již na první pohled nebylo možné hodnotit jako obchodní sdělení ve smyslu § 2 písm. f) zákona č. 480/2004 Sb. V roce 2017 pak bylo možné zaznamenat výrazný pokles stížností, které bylo při následné analýze možné označit jako SPAM (v roce 2017 se jednalo o 57 stížností, v roce 2016 o 167 stížností a v roce 2015 o 165 stížností), tedy jako takovou zprávu, která není obchodním sdělením, ale je zprávou pouze obtěžující.

Ačkoli dle výše uvedeného grafu je patrné, že stížností výrazně ubylo, není na místě hovořit o úbytku práce pro inspektorát zabývající se nevyžádanými obchodními sděleními, neboť tato problematika se stala náročnější, a to především z hlediska odhalování pachatelů přestupků. Často také dochází k provázanosti mezi jednotlivými subjekty, které v rámci kontroly figurují. Pracovníci inspektorátu také musí pracovat s větším množstvím povinných osob a často též s řetězením subdodavatelů (faktických šiřitelů). Všechny tyto aspekty vzhledem k zákonným lhůtám řízení prodlužují. Cenou za delší dobu řízení však zpravidla bývá odhalení jak šiřitele obchodních sdělení, tak osob, které se na šíření obchodních sdělení podílejí a jejich následné potrestání ve správním řízení.

Společnost anji s.r.o.

Od ledna 2017 byly Úřadu doručovány stížnosti na zasílání nevyžádaných obchodních sdělení směřující vůči společnosti anji s.r.o. Vzhledem k přijatému počtu stížností byla dne 2. března 2017 s výše uvedeným subjektem zahájena kontrola dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), jejímž cílem bylo vyhodnotit dodržování zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů v souvislosti se zasíláním nevyžádaných obchodních sdělení.

V rámci kontrolních úkonů bylo kontrolujícími zjištěno, že kontrolovaná osoba zakoupila databázi e-mailových kontaktů a k rozesílce obchodních sdělení na tyto kontakty využila dvou společností, a to společnosti Effective online s.r.o. a společnosti Clever Monitor s.r.o.

Prvním problémem, který zcela očividně zavdal příčinu celému kontrolnímu řízení, je nákup databáze. Jak již ÚOOÚ několikrát uvedl, je vysoce nepravděpodobné, že bude existovat taková databáze, která by splňovala kritérium vědomého souhlasu, které je z hlediska šíření

obchodních sdělení nejdůležitější. Pro úplnost je třeba dodat, že souhlas musí být 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. Souhlas se zasíláním obchodních sdělení nemůže být dán generálně, tj. neurčitému okruhu subjektů (šiřitelů obchodních sdělení) k neurčitým nabídkám. Při zakoupení databáze pak platí povinnost validního právního titulu pro zasílání obchodních sdělení obdobně. Úřad tak opakovaně konstatuje, že je vysoce nepravděpodobné, že bude existovat taková databáze, jejímž obsahem budou elektronické adresy, jejichž uživatelé udělili k zasílání obchodních sdělení souhlas, a to právě z toho důvodu, že souhlas musí být dán konkrétnímu šiřiteli před odesláním obchodního sdělení, respektive, souhlas musí být udělen tomu subjektu, v jehož prospěch jsou obchodní sdělení zasílána. K tomu je potřeba říci, že kontrolovaná osoba informovala společnost prodávající databázi (Imper CZ s.r.o.) o účelu koupě databázového produktu. Přesto však Imper CZ s.r.o. tento databázový produkt prodal a po dohodě s nabyvatelem (kontrolovanou osobou) došlo k úpravě smlouvy. Nicméně i přes úpravu smlouvy o poskytnutí licence k databázi nebylo tuto databázi možné použít v souladu se zákonem č. 480/2004 Sb.

K předešlému odstavci Úřad konstatuje, že mezi zákonným zpracováním osobních údajů správcem osobních údajů (§ 4 písm. j) zákona č. 101/2000 Sb.) a zasíláním obchodních sdělení druhým subjektem, ať již ve svůj prospěch, či ve prospěch třetí strany, neexistuje žádné propojení. Jinými slovy, jestliže dojde k legálnímu zpracování osobních údajů resp. e-mailových adres subjektem A, neznamená to, že jejich využití prováděné subjektem B, byť by probíhalo za shodným účelem (nabídka zboží či služeb), je též legální, neboť je třeba získat souhlas s takovým obchodním oslovením uživatele elektronické adresy (viz výše k otázce souhlasu se zasíláním obchodních sdělení).

Dalším problémovým bodem celého případu bylo využití dalších dvou společností (Effective online s.r.o. a Clever Monitor s.r.o.) k faktickému šíření obchodních sdělení. K této problematice Úřad konstatuje, že odpovědný za rozesílku je nejen ten, kdo k takové rozesílce dá pokyn, uzavře za tím účelem smlouvu, nebo nabídne jiné protiplnění, ale rovněž ten, kdo ji realizuje, aniž by projevil spravedlivě požadovatelnou míru obezřetnosti a prověřil, zda příjemci obchodních sdělení skutečně svůj souhlas s takovou elektronickou poštou vyjádřili. V návaznosti na novou právní úpravu přestupkového zákona (zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich), je třeba k odpovědnosti právnické osoby za přestupek dodat to, že dle § 20 cit. zákona je nutné, aby došlo k jednání fyzické osoby, které se následně přičítá osobě právnické. Skupina fyzických osob, jejichž jednání se právnické osobě přičítá, je taxativně vymezena § 20 odst. 2 zákona č. 250/2016 Sb.

V popisovaném případě však Úřad nepostupoval podle nové právní úpravy, ale vzhledem k přechodným ustanovením v zákoně č. 250/2016 Sb. a vzhledem ke skutečnosti, že došlo ke kumulaci správních deliktů kontrolované osoby (kromě nedoložení souhlasu, a tedy zasílání obchodních sdělení bez souhlasu, kontrolovaná osoba rovněž pochybila z hlediska formálních stránek obchodních sdělení), vedl ÚOOÚ společné řízení se společnostmi anji s.r.o., Effective online s.r.o. a Clever Monitor s.r.o. podle „staré" právní úpravy.

Společné řízení bylo zahájeno doručením Oznámení o zahájení řízení, které bylo zasláno a doručeno všem zúčastněným společnostem. Úřad poskytl všem účastníkům řízení prostor pro

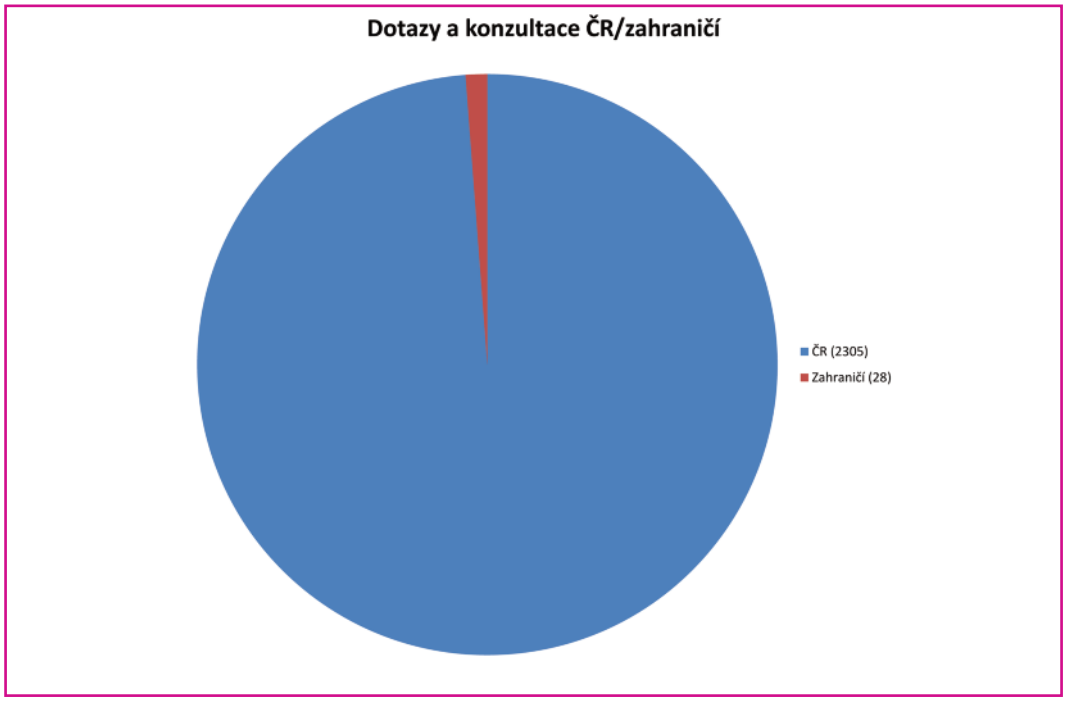
vyjádření se k celému řízení a následně vydal své rozhodnutí. V tomto rozhodnutí Úřad akcentoval především shora popsanou problematiku databázových systémů. Dále se Úřad zabýval problematikou pojmu šiřitel obchodních sdělení, kde v rozhodnutí zopakoval svůj dříve uveřejněný názor (viz https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=23490&n=za-sireni-obchodnich-sdeleni-je-odpovedny-nejen-rozesilatel-ale-i-objednatel). K tomuto pojmu ÚOOÚ dodává, že je třeba na něj hledět především z jazykového hlediska, kdy dle Slovníku spisovného jazyka českého, je možné šiřitele chápat jako „toho, kdo něco šíří, uvádí ve známost".[1] Proto je třeba za šiřitele obchodních sdělení považovat jak ten subjekt, který obchodní sdělení fakticky odesílá, tak také toho, kdo k takovému odeslání dá pokyn, uzavře za účelem takového odesílání smlouvu, či učiní k uvedení obchodního sdělení ve známost jiný krok, v jehož důsledku dojde k faktickému odeslání obchodního sdělení.

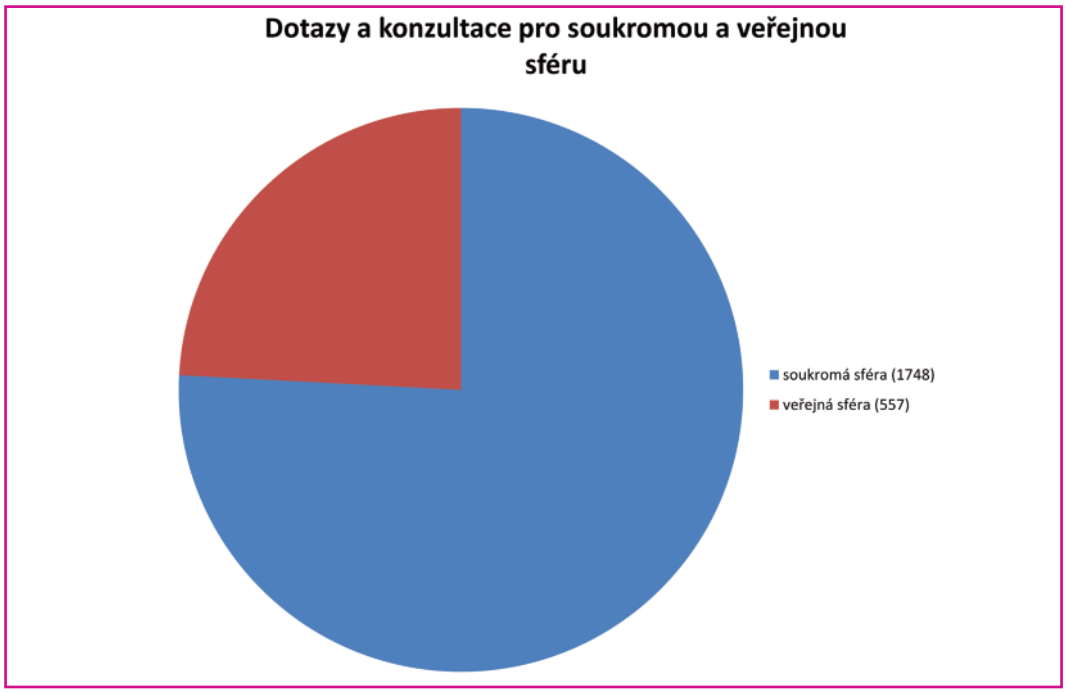
Z hlediska správního trestání Úřad zohlednil několik skutečností, které o sankcích pro jednotlivé účastníky rozhodly. Na straně kontrolované osoby to byl především fakt, že ihned po zahájení kontrolního řízení došlo k zastavení e-mailové kampaně a kontrolovaná osoba s kontrolujícími po celou dobu jak kontrolního, tak navazujícího správního řízení, aktivně spolupracovala. Dalším neopomenutelným faktem byl, dle počtu ÚOOÚ doručených stížností, relativně malý dopad na soukromí jednotlivých stěžovatelů. V případě společností, které rozesílku obchodních sdělení provedly, pak Úřad jako rozhodující vyhodnotil skutečnost, že obě společnosti jsou profesionály ve svém oboru, obě se zabývají marketingovou činností. Oběma společnostem nadto byla známa smlouva mezi kontrolovanou osobou a společností Imper CZ s. r. o. o poskytnutí oprávnění k užití databáze. Z této smlouvy měly obě společnosti, jakožto profesionálové v oboru, ve smyslu § 5 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, seznat, že takto nastavená smlouva neopravňuje ani jednu ze společností k šíření obchodních sdělení.

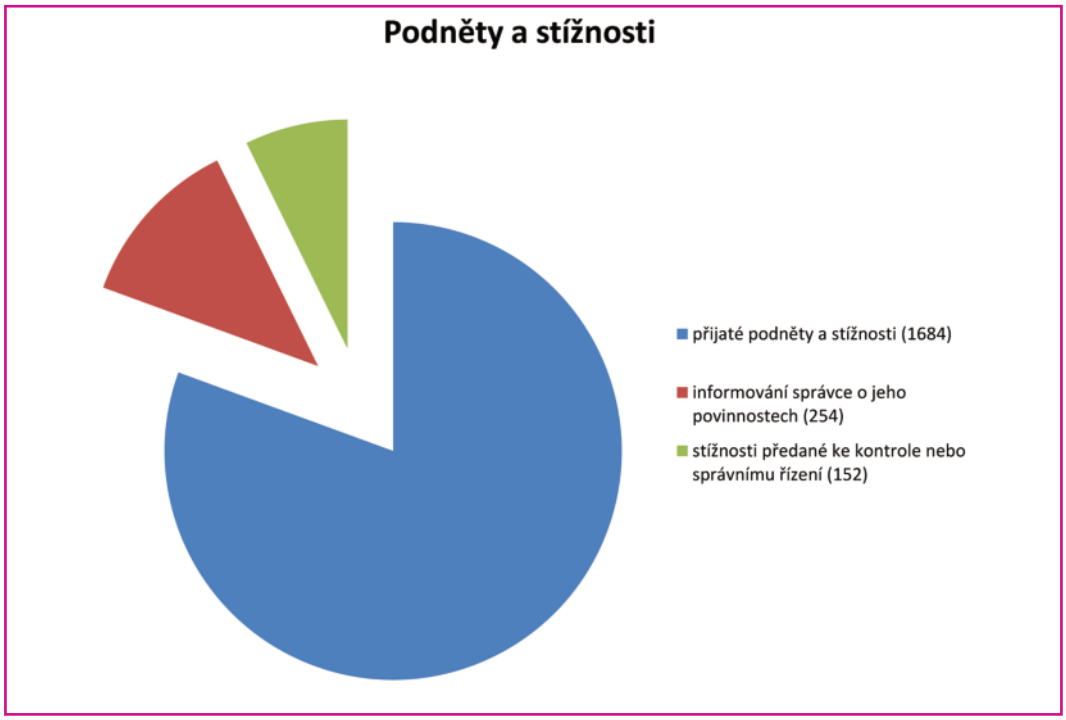
K celému případu je třeba doplnit, že společnost Clever Monitor s. r. o. podala proti rozhodnutí ÚOOÚ rozklad, který předsedkyně Úřadu zamítla.

[1] http://ssjc.ujc.cas.cz/search.php?hledej=Hledat&heslo=%C5%A1i%C5%99itel&sti=EMPTY&where=hesla&hsubstr=no

Ostatní dozorová činnost







• STÍŽNOSTNÍ A KONZULTAČNÍ AGENDA

Výkon stížnostní agendy v roce 2017 probíhal standardním způsobem, bez vážnější ingerence nových či novelizovaných právních předpisů v porovnání s předchozím rokem.

Zhruba pětinovou část stížnostní agendy tvořily v roce 2017 stížnosti na kamerové systémy provozované různými subjekty, ať už v pozici správců osobních údajů či soukromými fyzickými osobami, které jednaly v rámci občanskoprávní odpovědnosti. Další oblastí, kterou lze zmínit, bylo zpracování osobních údajů pro účely přímého marketingu a dalších marketingových aktivit. Rezonance tohoto tématu ve stížnostní agendě vyústila v navržení této oblasti ze strany odboru pro styk s veřejností do plánu kontrol pro rok 2018. Nelze opominout ani stížnosti na zpracování osobních údajů finančními institucemi, a to zejména ve vztahu k souvisejícímu zpracování osobních údajů v informačních databázích o bonitě a důvěryhodnosti spotřebitele. Velká část stížností se týkala i zpracování osobních údajů zaměstnavateli či samosprávou, ale např. i školskými zařízeními. Další obdržené stížnosti se týkaly ostatních aspektů oblastí života, ve kterých dochází ke zpracování osobních údajů.

Oproti předchozímu roku došlo v roce 2017 v rámci výkonu stížnostní agendy k častějšímu využívání informativních dopisů, jejichž účelem je informovat správce o jeho povinnostech zejména v případech, kdy ze stížnosti vyplývá bagatelní porušení povinností, které lze napravit, aniž by byl zároveň nutný i veřejnoprávní zásah ve formě správního řízení či kontroly nebo kdy nevyplývá působnost. Ty byly zasílány nejčastěji správcům osobních údajů, ale i jiným osobám, které Úřad informoval o jejich zákonných povinnostech a doporučeních, jak postupovat, aby bylo dostáno především zákonu č. 101/2000 Sb. Tak tomu bylo učiněno v 254 případech, zejména u:

- zveřejňování identifikačních údajů žadatelů o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím,
- některých povinných subjektů,
- nesprávně formulovaných informací pro subjekty údajů,
- u nadbytečného vyžadování souhlasu se zpracováním osobních údajů.

Velmi často byly informativní dopisy uplatňovány i v oblasti kamerových systémů provozovaných správci. Soukromým fyzickým osobám v oblasti jimi využívaných kamer byly zasílány informace mající vztah k ochraně soukromí ostatních fyzických osob a nemožnosti překračovat meze nastavené zákonem č. 89/2012 Sb., občanský zákoník. Lze konstatovat, že tato forma informativních dopisů se velmi osvědčila a ve většině případů došlo k okamžité nápravě.

Náplň konzultační agendy ÚOOÚ doznala po obsahové stránce v roce 2017 oproti minulým rokům podstatné změny v souvislosti s blížícím se nabytím účinnosti obecného nařízení o ochraně osobních údajů.[2] Od prvního čtvrtletí roku 2017 narůstal trend z konce minulého roku, kdy začaly přibývat jak písemné dotazy, tak i telefonické žádosti o konzultace k budoucí právní úpravě ochrany osobních údajů. Narůstající mediální kampaň k této problematice bohužel navíc přinesla mnoho nesprávných názorů a dezinterpretací. Příkladem může být i údajné rozšíření pojmu osobní údaj o další údaje či údajné uložení nových povinností, které již zákon o ochraně osobních údajů dávno ukládá. Tyto dezinterpretace tak bylo třeba vysvětlovat a uvádět na pravou míru. Na druhou stranu bylo pozitivní stránkou této kampaně, že k problematice ochrany osobních údajů připoutala pozornost většiny správců a i těch, kteří se jí předtím dostatečně nevěnovali. To se projevilo i v enormním nárůstu telefonických dotazů, které pracovníci odboru pro styk s veřejností odbavili. Koncem roku 2017 již v konzultační agendě převažovalo téma obecného nařízení.

K nejčastějším dotazům k obsahu GDPR patřily otázky k pověřenci pro ochranu osobních údajů, hlavně pak které subjekty ho budou muset jmenovat, kdo bude moci tuto funkci zastávat i jakým způsobem lze kvalifikaci k výkonu této funkce získat. K dalším frekventovaným tématům patřily dotazy k posouzení vlivu na ochranu osobních údajů: v jakých případech ho bude nutné provádět, zejména kdy bude zveřejněn seznam operací, které budou tomuto posouzení podléhat, a kdy bude nutné provést předchozí konzultaci s Úřadem. Vysvětlovat bylo třeba i podmínky pro aplikaci nového práva na přenositelnost osobních údajů, případné výjimky z povinnosti vést záznamy o činnostech zpracování či kdo je příslušný pro vypracování kodexů chování. Dotazy směřovaly i k upřesnění některých vágních pojmů, např. jaké zpracování lze považovat za rozsáhlé, nebo pojmu vysoké riziko. V některých případech se tazatelé zajímali, zda se za účinnosti obecného nařízení změní dosavadní přístupy, např. k systémům založeným na biometrické identifikaci subjektu údajů. Opomenout nelze ani mnoho obecných dotazů na dopad GDPR na jednotlivé správce.

K zodpovězení dotazů byl využíván nejen samotný text obecného nařízení, ale i pokyny skupiny WP29 vydávané k jeho aplikaci. Ty jsou veřejnosti k dispozici na webových stránkách Úřadu. Na některé konkrétně formulované dotazy bylo přesto obtížné odpovídat, protože až aplikační

[2] Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

praxe může přinést ustálený výklad některých obecně formulovaných pojmů. K usnadnění zodpovídání četných dotazů slouží na webových stránkách Úřadu rubrika častých otázek k obecnému nařízení a základní příručka.

Významnější osobní konzultace k GDPR byly prováděny i za účasti pracovníků jiných útvarů ÚOOÚ. Ty byly poskytnuty např. různým sektorovým zástupcům, jako např. České bankovní asociaci, Sdružení pro internetový rozvoj, Asociaci inovativního farmaceutického průmyslu i reprezentacím budoucích pověřenců pro ochranu osobních údajů.

Z dotazů k zákonu o ochraně osobních údajů opět dominovaly žádosti o vysvětlení podmínek pro provozování kamerových systémů. Časté byly i otázky k možnosti pořizování obrazových a zvukových záznamů jiným, neautomatizovaným způsobem. Naši experti se taktéž hodně věnovali dotazům na téma zpracování osobních údajů v činnosti obce včetně možností zveřejňování osobních údajů na základě zákona, možností jejich zpřístupňování na základě zákona o svobodném přístupu k informacím, aniž by byl porušen zákon o ochraně osobních údajů či způsobu zápisu osobních údajů do obecních kronik. Možnosti případné změny platné právní úpravy s ohledem na posílení ochrany osobních údajů se týkaly dotazy na masivní šíření rodných čísel podnikatelů jako součásti daňového identifikačního čísla v účtenkách na základě zákona o elektronické evidenci tržeb a povinnosti lékařů vydávat elektronické recepty ukládané do centrálního úložiště Státního ústavu pro kontrolu léčiv podle zákona o léčivech.

• POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

Úřad uložil v roce 2017 pokuty za správní delikty a přestupky v souhrnné výši 6 097 000 Kč, z toho za nevyžádaná obchodní sdělení 4 618 000 Kč. Shrnutí statistických informací o řízeních, která ÚOOÚ v roce 2017 vedl, lze nalézt v části této výroční zprávy nazvané Úřad v číslech.

Hlavní výzvou v oblasti vedení správních řízení v roce 2017 byla pro Úřad nová právní úprava tzv. správního trestání obsažená v zákoně č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, která nabyla účinnosti dne 1. července 2017. Uvedený zákon zpřesňuje a unifikuje některá pravidla pro správní řízení o sankcích. Porušení zákona zakládající správně trestní odpovědnost nazývá přestupkem, a to bez ohledu na skutečnost, zda jej páchá fyzická osoba na jedné straně (tedy stejně jako dosud) nebo právnická osoba či fyzická osoba podnikající na straně druhé.[3]

Z hlediska přestupků projednávaných Úřadem lze za významnou změnu považovat stanovení a sjednocení promlčecí doby přestupků. S ohledem na výši pokuty, kterou lze za jejich spáchání uložit, se jedná o dobu maximálně pět let od spáchání přestupku. Nově je i možnost ukládat právnickým osobám a fyzickým osobám podnikajícím za přestupky, které spáchají, pouze napomenutí, případně za podmínek stanovených zákonem[4] lze od uložení správního trestu upustit. Možnost uložit napomenutí využil ÚOOÚ v roce 2017 v pěti případech. Jednalo se například o případ obce, která jako součást informací poskytnutých na základě žádosti podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, poskytla žadateli též osobní údaje, a to

[3] Tedy ty subjekty, které se doposud dopouštěly tzv. jiných správních deliktů.
[4] Jestliže vzhledem k závažnosti přestupku, okolnostem jeho spáchání a osobě pachatele lze důvodně očekávat, že již samotné projednání věci před správním orgánem postačí k jeho nápravě.

v rozsahu počtu stížností, žádostí a podnětů, které u ní podala konkrétní osoba v předchozích letech. K tomu je třeba uvést, že účelem zpracování osobních údajů osob, které se na obec (či jakýkoli jiný povinný subjekt podle zákona č. 106/1999 Sb.) obracejí se svými stížnostmi, žádostmi a podněty, k němuž byly tyto údaje shromážděny, je jejich přijetí, zaevidování a vyřízení. Následným zpřístupněním osobních údajů žadatelů v souvislosti s poskytováním informací podle zákona č. 106/1999 Sb. byl tento účel zjevně překročen. Nemožnost poskytnutí uvedených osobních údajů lze také vyvodit z § 8a zákona č. 106/1999 Sb., podle kterého osobní údaje poskytne povinný subjekt jen v souladu s právními předpisy upravujícími jejich ochranu, tj. v souladu se zákonem č. 101/2000 Sb., který, jak výše uvedeno, podobný postup neumožňuje.

Pro Úřad a jeho činnost je dále významná část zákona č. 250/2016 Sb., týkající se určení druhu a výměry správního trestu, zejména pak kritéria, která se posuzují při určování povahy a závažnosti přestupku. Patří mezi ně i demonstrativní výčet polehčujících a přitěžujících okolností, který v oblasti trestání přestupků a jiných správních deliktů doposud zcela chyběl. Mezi polehčující okolnosti, které mohou být z hlediska činnosti Úřadu relevantní, lze zařadit například to, že pachatel napomáhal k odstranění škodlivého následku nebo oznámil přestupek správnímu orgánu a při jeho objasňování účinně napomáhal. Naopak z přitěžujících okolností v některých případech může ÚOOÚ přihlížet k tomu, že pachatel spáchal přestupek na dítěti, osobě těhotné, nemocné, zdravotně postižené, vysokého věku nebo nemohoucí. Jinak řečeno, protiprávní zpracování osobních údajů, za které je postihován, se týkalo právě této skupiny osob.

Obecně z hlediska zpracování osobních údajů zákon č. 250/2016 Sb. umožňuje uložit jako správní trest tzv. zveřejnění rozhodnutí o přestupku (ve veřejném sdělovacím prostředku a vyvěšením na úřední desce). Tento druh správního trestu však nelze uložit fyzické osobě nepodnikající a možnost jej uložit musí výslovně stanovit zákon. Příkladem takového zákona je zákon č. 257/2016 Sb., o spotřebitelském úvěru, který v § 159 ukládá České národní bance uveřejnit bez zbytečného odkladu pravomocné rozhodnutí o udělené pokutě způsobem umožňujícím dálkový přístup, a to po dobu pěti let. Pokud by uveřejnění bylo na základě předchozího posouzení shledáno vůči dotčené fyzické osobě jako zjevně nepřiměřené, Česká národní banka uveřejní rozhodnutí bez uvedení identifikačních údajů o pokutované osobě. Samozřejmostí, která je také upravena v zákoně č. 250/2016 Sb., je, že obsahem zveřejněného rozhodnutí o přestupku nesmějí být údaje umožňující identifikaci jiné osoby než pachatele. *A contrario* lze z předchozího textu vyvodit, že v případě, že by došlo ke zveřejnění rozhodnutí o přestupku, aniž by tato skutečnost byla zvláštním právním předpisem umožněna, nebo by jako součást zveřejněného rozhodnutí o přestupku byly zveřejněny i osobní údaje jiné osoby, než je pachatel přestupku, jednalo by se o postup protiprávní.

Závěrem lze konstatovat, že v roce 2018 dojde, stejně jako u mnoha dalších postupů Úřadu, ke změnám v ukládání sankcí v souvislosti s účinností obecného nařízení o ochraně osobních údajů. Přesnou podobu správního trestání přitom bude Úřad i veřejnost znát až po přijetí nového zákona o zpracování osobních údajů. Už dnes je však možno říci, že například při určení druhu a výměry sankce se bude postupovat podle čl. 83 nařízení, které mimo jiné stanoví nezávisle na zákonu č. 250/2016 Sb. okolnosti, které je třeba při ukládání správní pokuty zohlednit.[5]

[5] Např. kroky podniknuté ke zmírnění škod způsobených subjektům údajů, míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích následků nebo též způsob, jakým se dozorový úřad dozvěděl o porušení. Zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře.

• POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

Soudnímu přezkumu byla v roce 2017 předložena některá rozhodnutí a bylo vyhlášeno několik rozsudků. Zároveň však řada rozhodnutí ÚOOÚ na soudní přezkum stále čeká. Za rok 2017 lze z konkrétních poznatků z předmětné soudní praxe poukázat na následující rozsudky, týkající se zejména zveřejňování záznamů Policie ČR, zveřejňování záznamů soukromými subjekty, sledování zaměstnanců a provozování kamerových systémů:

1. Zveřejnění zkráceného audiovizuálního záznamu, který byl původně vyhotovený dne 12. června 2013 Policií ČR při zatčení Mgr. Jany Nečasové, dříve Nagyové, v pořadu České televize s názvem „Otázky Václava Moravce". Toto jednání sledovalo veřejný zájem v souladu s ustanovením § 8d odst. 1 trestního řádu.

Plk. Mgr. Robert Šlachta, ředitel Útvaru pro odhalování organizovaného zločinu Služby kriminální policie a vyšetřování, poskytl dne 22. prosince 2013 k odvysílání v pořadu České televize s názvem „Otázky Václava Moravce", kterého se účastnil jako host, zkrácený audiovizuální záznam, jenž byl původně vyhotovený dne 12. června 2013 Policií ČR při zatčení Mgr. Jany Nečasové, dříve Nagyové. V tomto záznamu byly technickými prostředky rozostřeny tváře osob, které jsou na záznamu zachyceny. Uvedené jednání ovšem Úřad kvalifikoval jako porušení povinností uložených v § 13 odst. 1 zákona č. 101/2000 Sb. spočívající v nepřijetí opatření zabraňujících neoprávněnému předání předmětného záznamu, a tedy jako spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., za což uložil pokutu ve výši 60 000 Kč. Rozhodnutí správního orgánu prvního stupně č.j. UOOU-01670/14-11 ze dne 18. dubna 2014 pak potvrdilo rozhodnutí předsedy Úřadu č.j. UOOU-01670/14-17 ze dne 23. června 2014, které ovšem bylo posléze napadeno správní žalobou.

V rozsudku č.j. 5A 138/2014 ze dne 2. listopadu 2017 Městský soud v Praze předmětné žalobě vyhověl. Soud především připomněl, že ustanovení § 8d odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), umožňuje zveřejnění informace, odůvodňuje-li to veřejný zájem. Zároveň je však nutné, aby tento zájem převažoval nad právem na ochranu soukromí dotčené osoby. Toto ustanovení trestního řádu zároveň představuje výjimku ze zákazu zveřejňovat informace. To je zakotveno v ustanovení § 8a trestního řádu. V dané věci pak soud shledal, že na zveřejnění informace byl vzhledem ke kontextu situace silný veřejný zájem, a to s ohledem na potřebu uchovat důvěru v Policii ČR. K tomu, aby zveřejnění konkrétní informace bylo ustanovením § 8d odst. 1 trestního řádu ospravedlněno, bylo ovšem třeba posoudit i to, zda tento veřejný zájem převažoval nad právem na ochranu soukromí dotčené osoby, zde Jany Nagyové. Soud přitom neměl žádných pochyb o tom, že zveřejnění videa do soukromého života Jany Nagyové skutečně zasáhlo. K tomu dále uvedl, že zveřejnění policejního videozáznamu ze zadržení osoby není standardním postupem. Tato skutečnost však nemá vliv na posouzení splnění kroku vhodnosti, ale jde až o otázku proporcionality v užším smyslu.

Městský soud v Praze vyslovil souhlas s názorem ÚOOÚ, že zveřejnění videozáznamu je citelnějším zásahem do soukromí než slovní či písemná informace. Rozsah informací a intenzita vjemu bývá při obrazovém záznamu vyšší než při jeho slovním popisu. Na druhou stranu však neshledal rozsah těchto vedlejších informací jako velký. Soud měl dále za zásadní, že záznam neukazoval Janu Nagyovu v žádné choulostivé či nedůstojné situaci. Nebyl tak způsobilý

negativně ovlivnit její čest a důstojnost, tedy kromě samotné informace, že byla zadržena ve svém bytě ve večerních hodinách. To je však opět informace, která již byla známa, a nebyla tedy zveřejněna předmětným videozáznamem. Z rozsudku tudíž vyplynulo, že zásah do soukromí Jany Nagyové nebyl velký, zatímco sledovaný legitimní cíl měl velký význam.

Stejně tak by, podle názoru soudu, nemohlo být dosaženo sledovaného účelu cestou přezkumu jinými orgány. Soud také odmítl názor, že by zveřejnění videozáznamu mělo nějaký negativní dopad na trestní řízení proti Janě Nagyové.

2. Zpracování osobních údajů zaměstnanců České pošty, s.p. na základě aplikace technologie GPS lokalizace, jejímž prostřednictvím byly shromažďovány informace o zaměstnancích v pozici listovního doručovatele v rozsahu: *délka trasy, čas strávený na trase, vyhodnocení, zda se doručovatel pohyboval pouze ve svém okrsku, evidence a zobrazení sledovaných událostí označených doručovatelem v průběhu pochůzky, procentuální vyjádření obslužnosti doručovacího okrsku (poměr navštívených doručovacích míst vůči celkovému počtu doručovacích míst), doručovací místa s největším počtem návštěv a kompletní rozpis navštívených/nenavštívených doručovacích míst*. Dělo se tak pro účely kontroly a optimalizace listovních doručovacích okrsků, případně úpravu databáze dodacích míst, což postrádalo zákonný podklad.

Kontrolou provedenou u České pošty, s.p. ukončenou protokolem o kontrole zn. INSP1-3568/12-12/BYT ze dne 4. října 2012 bylo zjištěno provozování technologie GPS lokalizace, jejímž prostřednictvím dochází v rozporu s § 5 odst. 2 zákona č.101/2000 Sb. ke shromažďování osobních údajů zaměstnanců a z uvedených důvodů bylo uloženo opatření k nápravě spočívající v likvidaci shromážděných osobních údajů a zákazu dalšího zpracování osobních údajů ve stanoveném rozsahu. Na základě podaných námitek sice byla nápravná opatření částečně změněna, nicméně i přesto bylo předmětné rozhodnutí předsedy Úřadu č.j. INSP1-3568/12-16 ze dne 3. ledna 2013 napadeno správní žalobou.

Tuto žalobu však Městský soud v Praze ve svém rozsudku č.j. 6A 42/2013 ze dne 5. května 2017 zamítl. Soud v odůvodnění rozsudku především uvedl, že je třeba rozlišovat získávání informací zaměstnavatelem o výkonu práce zaměstnanci a shromažďování osobních údajů zaměstnanců. Kontrola výkonu práce prováděná zaměstnavatelem je oprávněná tehdy, jestliže nenarušuje soukromí zaměstnance na pracovišti. Výjimku mohou představovat závažné důvody spočívající ve zvláštní povaze činnosti zaměstnavatele.

V daném případě zaměstnavatel údaje shromažďoval systematicky po dobu jednoho roku. Povahu jeho činnosti pak nelze dle názoru soudu považovat za tak zvláštní, že by bylo možno pochůzkami na trase v doručovacím okrsku odůvodňovat narušení soukromí doručovatelů na pracovišti. Využití předmětné technologie ani nemohlo zabránit případnému nedoručení zásilek adresátům či jinému nesprávnému jednání. Samotná povinnost plnit podmínky licence a zákona nedělá z činnosti zaměstnavatele nic, co by odůvodňovalo nerespektování soukromí zaměstnanců na pracovišti.

K tomu, aby zpracování osobních údajů bylo legální, by bylo třeba, aby zaměstnavatel posoudil různé možnosti zpracování a zvolil tu, která do soukromí doručovatelů zasáhne v nejmenší míře. To však nebylo splněno v případě, kdy zaměstnavatel zpracovával každý den informace ve výše uvedeném rozsahu.

Soud zároveň uvedl, že Úřad zohlednil zájem zaměstnavatele na plnění jeho povinností podle zákona o poštovních službách.[6] ÚOOÚ zdůraznil, že zpracovávání osobních údajů prostřednictvím předmětné technologie v rozsahu údajů ohledně místa a času vypovídajících o navštívených doručovacích místech za účelem zajištění kvality poskytované poštovní služby a vyřízení reklamací nebylo v rozporu se zákonem č. 101/2000 Sb., proto příslušným způsobem upravil uložená opatření k nápravě. Ačkoliv zaměstnavateli náleží právo kontrolovat dodržování pracovněprávních povinností zaměstnanců,[7] musí tak učinit v mezích právním řádem stanovených možností. Zpracovávání osobních údajů zaměstnanců předmětnou technologií však nebylo přiměřeným způsobem zvolené kontroly či získávání statistických dat. S ohledem na výše uvedené nelze učinit závěr, že by předmětnou technologií zpracovávané údaje zaměstnanců žalobce spadaly pod výjimku § 5 odst. 2 písm. a) a písm. e) zákona č. 101/2000 Sb., neboť zpracování osobních údajů v takovém rozsahu nebylo nezbytné pro dodržení právní povinnosti žalobce. Vzhledem k rozsahu získaných údajů se v tomto případě dělo v rozporu s právem doručovatelů na ochranu jejich soukromí na pracovišti.

3. 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 je již překročením vymezené hranice. Důležitá není na tomto místě ani skutečnost, zda by tento postup posléze vedl k odhalení pachatele či nikoli.

Nejvyšší správní soud svým rozsudkem č.j. 3 As 118/2015 ze dne 8. června 2016 na základě kasační stížnosti podané Úřadem zrušil předchozí rozsudek Městského soudu v Praze, jímž bylo zrušeno rozhodnutí Úřadu, kterým byla provozovateli kamerového systému uložena pokuta v celkové výši 5000 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.

Podanou ústavní stížnost v této věci pak Ústavní soud svým usnesením III. ÚS 3565/16 ze dne 5. září 2017 zamítl a potvrdil názor dříve vyjádřený především výše uvedeným rozsudkem Nejvyššího správního soudu.[8] K tomu také Ústavní soud konstatoval, že v průběhu předchozího řízení stěžovatel zjevně relevantně nezpochybnil závěr o absenci „nezbytnosti" zveřejnění fotografie samotným stěžovatelem na sociální síti. Ostatně stěžovatel sám v ústavní stížnosti uvedl, že danou fotografii by zřejmě zveřejnila i Policie ČR, což Policie ČR nezpochybnila. To nepodporuje názor stěžovatele, podle něhož by zveřejnění jím bylo nezbytné, jediné přístupné a efektivní řešení k ochraně jeho majetkových práv.

Z celého řízení ani z ústavní stížnosti navíc nevyplynulo, že by Policie ČR při předání záznamu odmítla plnit své zákonné povinnosti. Stěžovatel v průběhu řízení proti postupu Policie ČR nic

[6] Zabezpečení a řádné doručení zásilek, zejména v souvislosti s vyřizováním reklamací apod.
[7] Viz § 316 odst. 2 zákoníku práce
[8] Viz Výroční zpráva 2016

nenamítal. Jednání stěžovatele pak nelze ospravedlnit ani ustanovením § 89 odst. 2 trestního řádu umožňujícím souběžně s orgány činnými v trestním řízení vyhledávat důkazy proti pachateli, jelikož by toto porušovalo zákonem regulovanou ochranu osobních údajů.

Ústavní soud tedy neshledal, že by závěry orgánů veřejné moci představovaly libovůli nebo jiné vybočení z ústavních mezí.

Tímto případem se však Úřad znovu podrobně zabýval a po obsáhlé diskusi vydal dne 3. října 2017 stanovisko, které pro hodnocení obdobných případů znamená v jeho rozhodování určitý posun:

"Za současného vedení Úřadu by k uložení pokuty společnosti ekolo.cz nedošlo. Jeho předsedkyně Ivana Janů je přesvědčena, že žádná interpretace jakéhokoli zákona nemůže být odtržena od vnímání spravedlnosti ve společnosti.

Je třeba ctít také zásadu, že se každý může přiměřeným způsobem domoci svého práva, pokud bylo zasaženo do jeho zákonem chráněných zájmů. Důležité přitom je, aby to bylo přiměřeně a za podmínky, že je jasné, že zásah veřejné moci nepřijde včas. A to byl právě tento případ," vysvětlila předsedkyně Ivana Janů.

Zároveň je důležité připomenout, že posledním aktivním krokem Úřadu v této kauze bylo podání kasační stížnosti 1. června 2015 k Nejvyššímu správnímu soudu, což se stalo tři měsíce před nástupem předsedkyně Ivany Janů do čela instituce.

„Doufala jsem, že v rámci řízení před Ústavním soudem bude vzata v úvahu specifičnost případu ekolo.cz a že bude zvážen i praktický dopad rozhodnutí soudu," prohlásila předsedkyně Úřadu.

Současně upozorňuje na zavádějící tvrzení týkající se případu, která se objevila v médiích a která nejsou založena na úplném výkladu platného práva. Argument, že k pořizování, resp. zveřejnění záznamu byl údajně nutný souhlas osoby podezřelé z krádeže, není správný. V této věci totiž není pro konání okradeného nutný souhlas nahrávané osoby. Důležitá pro posouzení případu je skutečnost, zda jednal v zájmu ochrany osob či majetku, na což pamatuje zákon o ochraně osobních údajů.

Úřad chce veřejnost ujistit, že v jeho rozhodovací praxi dochází k postupnému vývoji (viz Stanovisko č. 1/2016 – Umístění kamerových systémů v bytových domech). Takovéto změny však nemohou mít charakter jednorázové, rychlé kampaně, ale musí se naopak jednat o promyšlený proces, který je založen vždy na důkladném posuzování každé individuální kauzy tak, aby byla respektována zásada proporcionality při výkladu zákona o ochraně osobních údajů a ochrana práv a právem chráněných zájmů při zpracování osobních údajů správcem či dalšími osobami.

4. Provozování kamerového systému pořizujícího také záznam z prostoru cizích sousedních nemovitostí, a to bez souhlasu zaznamenávaných osob, nelze legalizovat obecným tvrzením, že se jedná o nutnou obranu před poškozováním vlastního majetku.

Úřad rozhodnutím č.j. UOOU-08116/14-14 ze dne 20. listopadu 2014 kvalifikoval zpracování osobních údajů prostřednictvím kamerového systému instalovaného a provozovaného na

obytném domě, který pořizoval záznam z prostoru sousedních nemovitostí ve vlastnictvích jiných osob, a to bez souhlasu zaznamenávaných osob, jako spáchání přestupku podle § 44 odst. 2 písm. e) zákona č. 101/2000 Sb., za což provozovateli uložil pokutu ve výši 5000 Kč. Na základě rozkladu bylo rozhodnutím předsedy Úřadu č.j. UOOU-08116/14-22 ze dne 22. ledna 2015 rozhodnutí správního orgánu prvního stupně změněno především tak, že pokuta byla snížena na částku 2000 Kč. Nicméně ve zbytku byl rozklad v zásadě zamítnut, a rozhodnutí předsedy proto bylo napadeno správní žalobou.

Nejvyšší správní soud v rozsudku č.j. 2 As 140/2017 ze dne 20. září 2017 potvrdil rozsudek Městského soudu v Praze č.j. 4A 21/2015 ze dne 30. března 2017 o zamítnutí žaloby proti rozhodnutí ÚOOÚ o uložení pokuty. Soud uvedl, že argumentace provozovatele kamerového systému o nutné a přiměřené obraně jeho majetku před trestnou činností zůstala v rovině ryze subjektivního tvrzení či spíše subjektivních pocitů. Ty nemají žádný objektivní základ ve spisovém materiálu a důkazech tam obsažených.

Vysoká četnost jeho stížností a opakované odkazy na úřední záznamy o podání vysvětlení samy o sobě nemají význam. Pokud nikdy nebylo vydáno správní či soudní rozhodnutí přisvědčující tvrzené skutkové verzi, bylo by nutno předložit alespoň věrohodný důkaz, který by objektivně předmětné tvrzení podpořil. To se však nestalo.

Navíc ani v kasační stížnosti nebylo nabídnuto vysvětlení o důvodech tohoto konání. Sousedka se měla neustále dopouštět protiprávního jednání. Provozované kamery (tzv. fotopasti) však žádné takové jednání nezachytily.

Zároveň bylo konstatováno, že výjimka dle ustanovení § 3 odst. 6 písm. d) zákona č. 101/2000 Sb. se týká pouze orgánů činných v trestním řízení.

• REGISTRACE

Oproti roku 2016 došlo v loňském roce k mírnému poklesu v počtu podaných oznámení o zpracování osobních údajů. Na Úřad bylo zasláno celkem 9241 oznámení o zpracování nebo změně zpracování osobních údajů (oproti 9708 podání v roce 2016). Z toho 513 oznámení (tedy více než 5,5 procenta) obsahovalo neúplné nebo nesprávné údaje nebo nebylo zřejmé, zda při oznámeném zpracování nemůže dojít k porušení zákona. Proto byla oznamovatelům zaslána výzva na doplnění oznámení o zpracování osobních údajů. Z celkového počtu obeslaných subjektů jen 31 zaslalo doplňující údaje, které potvrdily obavy z možného porušení zákona č. 101/2000 Sb., o ochraně osobních údajů, a bylo tudíž zahájeno řízení dle § 17 uvedeného zákona. Z celkového počtu podaných podnětů však pouze u jednoho oznámení nebylo zahájení zpracování osobních údajů povoleno. U ostatních zpracování došlo k úpravě parametrů zpracování osobních údajů nebo odstoupení od registrace.

Na základě žádostí správců rovněž ÚOOÚ provedl zrušení 156 zpracování osobních údajů.

Nejčastěji podávanými oznámeními o zpracování osobních údajů v roce 2017 byla zpracování osobních údajů kamerovými systémy se záznamem[9] a zpracování osobních údajů v rámci provozování internetových obchodů.

[9] Asi 40 procent ze všech oznámení.

Zpracování osobních údajů kamerovými systémy ohlásilo v roce 2017 celkem 3202 správců (odhad ke konci roku 3800), z toho bylo zapsáno do registru 2970 správců (ke konci roku odhad 3550). Zbytek tvořila zpracování, kdy správce odstoupil od pořizování kamerového záznamu, nebo šlo o osobní potřebu správce.

Od 25. května 2018 vstoupí v účinnost nová právní úprava oblasti ochrany osobních údajů, kterou je obecné nařízení o ochraně osobních údajů.[10] Jednou z řady významných změn, které nová právní úprava přináší, je zrušení oznamovací povinnosti, která byla správcům osobních údajů uložena zákonem č. 101/2000 Sb. Zároveň s tím bude v květnu 2018 uzavřen veřejný registr zpracování osobních údajů. Oznamovací povinnost a vedení veřejného registru zpracování osobních údajů bude nahrazeno jinými právními instituty.

Oznamovací povinnost umožňovala Úřadu zasáhnout do zpracování osobních údajů ještě ve stadiu před jeho započetím, takže registrační proces představoval jistou formou předběžné kontroly. GDPR převádí tuto funkci ve značné míře do oblasti samoregulace, kdy jsou správci osobních údajů povinni sami vést záznamy o činnostech zpracování (čl. 30), v případě vysoce rizikových zpracování provést posouzení vlivu na ochranu osobních údajů (čl. 35), a teprve v případě, že vysoká rizika nelze eliminovat, obrátit se na Úřad s žádostí o konzultaci (čl. 36).

Zveřejnění zaregistrovaných oznámení zároveň zprostředkovalo subjektům údajů základní informace o správci osobních údajů a jím prováděných zpracováních (pokud nebyly uplatněny výjimky z oznamovací povinnosti). Obecné nařízení nahrazuje tuto funkci prohloubením zásady transparentnosti zpracování (čl. 12), informační povinnosti správců vůči subjektům údajů (čl. 13 a 14) a zavedením institutu pověřence pro ochranu osobních údajů (čl. 37 až 39).

Tyto změny kladou celkově větší důraz na vlastní odpovědnost správců osobních údajů, kdy musí být sami schopni doložit, že zpracování provádějí v souladu s GDPR.

• PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

V roce 2017 přijal Úřad 31 nových a dořešil tři starší žádosti o povolení k předání osobních údajů do třetích zemí podle § 27 odst. 4 zákona č. 101/2000 Sb. ÚOOÚ se podařilo vyřešit všechny žádosti v rámci daného kalendářního roku, takže všech 34 řízení bylo ukončeno.

Jedno řízení bylo zastaveno, neboť žadatel nereagoval na výzvu k doplnění žádosti. Jedna žádost byla odložena, neboť žadatel nakonec zajistil předání osobních údajů do třetí země s nedostatečnou úrovní osobních údajů způsobem, který nevyžaduje povolení Úřadu.[11] Obecně však Úřad dlouhodobě doporučuje využití standardních smluvních doložek podle rozhodnutí Evropské komise.

V ostatních 32 případech ÚOOÚ předání osobních údajů do třetích zemí povolil, a to na základě následujících právních titulů.

[10] Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů).
[11] V tomto konkrétním případě prostřednictvím účasti amerického příjemce údajů v programu štít soukromí.

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 21 případech.

V pěti případech 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. Ve čtyřech případech bylo právním titulem povolení ustanovení § 27 odst. 3 písm. a), tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů. V jednom případě vydal Úřad povolení pro předání nezbytné k naplnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou podle ustanovení § 27 odst. 3 písm. d) zákona č. 101/2000 Sb. V jednom případě povolil Úřad České národní bance předání nezbytné pro uplatnění důležitého veřejného zájmu podle ustanovení § 27 odst. 3 písm. d) zákona č. 101/2000 Sb.

Co se týče cílových zemí, ve většině případů šlo o předání osobních údajů do více zemí všech světadílů. Dělo se tak typicky v případech, kdy jsou osobní údaje sdíleny s ostatními pobočkami nadnárodní skupiny, přičemž zpracování a předání osobních údajů se řídí závaznými vnitropodnikovými pravidly dané nadnárodní skupiny.

Nad předáním do jedné konkrétní země geograficky výrazně převažovala předání do více zemí či do velkého počtu poboček v mnoha zemích, ve kterých typicky působí skupina, do níž jako pobočka nadnárodní skupiny patří i český správce osobních údajů. Tato skupina zajišťuje ochranu osobních údajů sdílenou v rámci skupiny právě výše uvedenými závaznými vnitropodnikovými pravidly. V případě povolených předání do jedné či dvou konkrétních třetích zemí byly cílovou destinací osobních údajů v osmi případech Spojené státy americké, ve čtyřech případech Indie a po jednom případě Austrálie, Kanada, Kolumbie. V jednom případě šlo o předání osobních údajů účastníků olympijské výpravy do Jižní Koreje.

ÚOOÚ se v několika případech zapojil do schvalovací kooperační procedury BCR určité nadnárodní skupiny, a to v roli tzv. co-reviewera. Tato schvalovací procedura v současné době probíhá podle pracovního dokumentu WP107 přijatého dne 14. dubna 2005 Pracovní skupinou WP29. V rámci nepsané gentlemanské mutual recognition dohody většiny dozorových orgánů jednotlivých členských zemí Evropské unie pomáhají vedoucímu dozorovému úřadu realizujícímu schvalovací proceduru konkrétních BCR (tzv. lead authority) jeden až dva dozorové úřady. Ty provádějí připomínkování konsolidovaného návrhu BCR a zhodnocení, zda návrh BCR odpovídá zásadám definovaným ve stanovisku WP153, resp. WP195. Tato schvalovací procedura bude evidentně uplatňována i v režimu obecného nařízení,[12] ačkoliv není ještě zcela jasné, jakým způsobem bude upravena a navázána na mechanismus jednotnosti definovaný novým nařízením.

Řešením právě uvedené otázky a mnoha dalších problémů vyvstávajících v souvislosti s blížící se účinností obecného nařízení o ochraně osobních údajů se Úřad zabývá v součinnosti s ostatními dozorovými orgány jednotlivých členských zemí Evropské unie v rámci práce podskupiny International Transfers Pracovní skupiny WP29. Výsledkem práce této podskupiny je příprava doposud tří materiálů.

---

[12] Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Dva z nich shrnují nezbytné náležitosti závazných vnitropodnikových pravidel v souladu s čl. 47 obecného nařízení: revidované zásady, které musejí naplňovat BCR pro správce (WP256, původně WP153) a revidované zásady, které musejí naplňovat BCR pro zpracovatele (WP257, původně WP195). Oba tyto dokumenty byly koncem roku 2017 předloženy k veřejné konzultaci.

Třetím dokončeným materiálem připraveným pro předložení k veřejné konzultaci jsou revidované zásady pro hodnocení adekvátnosti úrovně ochrany osobních údajů ve třetí zemi (původně WP12). Tímto dokumentem dává Pracovní skupina WP29 Evropské komisi návod, jakým způsobem má postupovat při hodnocení odpovídající úrovně ochrany podle čl. 45 obecného nařízení.

Mezi další dokumenty, které mají přispět k výkladu ustanovení GDPR v oblasti předávání osobních údajů do třetích zemí a na jejichž přípravě se Úřad podílí, patří především pokyny pro upřesnění kritérií, na jejichž základě lze pro předání osobních údajů použít výjimky dané čl. 49 obecného nařízení.

Nezbytné náležitosti správních ujednání, zahrnující vymahatelná práva subjektů údajů podle čl. 46(3b) obecného nařízení, přinese stanovisko k předávání osobních údajů v rámci administrativní spolupráce mezi veřejnými subjekty.

A konečně materiál věnovaný certifikaci jako nástroji předávání osobních údajů do třetích zemí by měl především osvětlit povahu článkem 46(2f) GDPR vyžadovaných závazných a vymahatelných závazků správce nebo zpracovatele ve třetí zemi. Ta tak bude mít při zpracování předaných osobních údajů povinnost dodržovat evropské zásady ochrany osobních údajů.

Specifické téma posledních let představuje program štítu soukromí (Privacy Shield). Více k tématu v rubrice Styky se zahraničím a mezinárodní spolupráce.

• SCHENGENSKÁ SPOLUPRÁCE

Na ochranu osobních údajů zpracovávaných rozsáhlými evropskými informačními systémy, mezi něž patří Schengenský informační systém druhé generace (SIS II), Vízový informační systém (VIS), Eurodac a Celní informační systém (CIS), je kladen v jejich právní úpravě velký důraz. Úřad plní v oblasti schengenské spolupráce úlohu dozorového orgánu, který vykonává dohled nad dodržováním příslušných předpisů, a tak přispívá k ochraně základních práv osob, jejichž osobní údaje jsou předmětem zpracování v rámci schengenského prostoru. Pověřený zástupce ÚOOÚ se navíc pravidelně účastní jednání koordinačních skupin, které jsou k jednotlivým systémům na evropské úrovni sestaveny.

Kromě dohledu a kontroly související s plněním požadavků na zákonné zpracování osobních údajů ze strany správce v rámci výše zmíněných informačních systémů se Úřad zabýval také vznikem nových informačních systémů a právních předpisů. Ty budou upravovat stávající podobu těchto systémů. Příkladem nově vznikajícího systému je ETIAS *(European Travel Information and Authorization System*), v rámci kterého budou zpracovávány osobní údaje osob ze třetích zemí, které nemají ve vztahu k Evropské unii vízovou povinnost. ÚOOÚ dále připomínkoval nově vznikající návrhy právních úprav vztahující se k systémům SIS II a Eurodac.

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

Společným jmenovatelem koordinačních skupin pro jednotlivé informační systémy v roce 2017 byla příprava webových stránek, včetně jejich obsahu. Odkazy na tyto skupiny byly vloženy i na webové stránky Úřadu. Další společnou činností byla finalizace společných modelů inspekcí systémů Eurodac, SIS II a CIS. Tyto dotazníky mají za účel sjednotit kontrolní postupy v rámci povinných auditů.

Velkými tématy roku 2017 byl koncept interoperability informačních systémů a rozpočty jednotlivých orgánů pro ochranu osobních údajů. Dále se koordinační skupiny pro VIS a SIS II zabývaly aktualizací schengenských doporučení vztahujících se k pravidelnému hodnocení základních aspektů schengenské spolupráce jednotlivých členských států.

Aktuální problémy řešené v rámci koordinačních skupin

Koordinační skupina pro systém SIS II (SIS II SCG) zaslala v létě roku 2017 jménem všech svých členů dopis panu Antonio Tajanovi, předsedovi Evropského parlamentu. V něm vyjádřila některé pochybnosti týkající se nového „legislativního balíku" revidujícího SIS II sestávajícího z návrhů tří nařízení. Změny přicházející s novými návrhy reprezentují proměnu dosavadního systému a je třeba je důkladně analyzovat ve vztahu k základním principům ochrany osobních údajů. Mimo toto téma se skupina intenzivně zabývala problematikou logování ve vnitrostátních systémech jednotlivých členských států.

Koordinační skupina pro VIS (VIS SCG) dokončovala v průběhu prvního pololetí roku 2017 dokument zabývající se implementací článku 41 nařízení Rady (EU) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému a o výměně údajů o krátkodobých vízech mezi členskými státy. Tento materiál ukládá vnitrostátním orgánům dozoru povinnost provést nejméně jednou za čtyři roky audit zpracování údajů ve vnitrostátním VIS. Koordinační skupina dále pokračovala v přípravě studie týkající se subdodavatelů systémů a k nim se vztahujícím právním předpisům o ochraně osobních údajů.

Jednou z hlavních činností koordinační skupiny pro systém Eurodac (Eurodac SCG) bylo vytvoření dotazníku srovnávajícího práva subjektu údajů. Tento dotazník bude rozeslán členským státům k vyplnění na začátku roku 2018.

Koordinační skupina pro celní informační systém (CIS SCG) dokončila na začátku roku 2017 jednotný dokument upravující obecná pravidla zpracování osobních údajů v CIS. Dokument byl uveřejněn na webových stránkách Úřadu. Jako zpravodaj na dokončení společného inspekčního plánu pro CIS se na něm také aktivně podílí Česká republika.

Počty podnětů, stížností, dotazů a jejich vyřízení

Jednou z povinností Úřadu je i vyřizování zaslaných podnětů subjektů údajů tykajících se zpracování osobních údajů v SIS II. Úřad v roce 2017 obdržel deset podnětů, přičemž osm z nich se týkalo realizace práva na informace či uplatnění práva na výmaz údajů ze systému. Tyto žádosti byly dále postoupeny k vyřízení správci osobních údajů na národní úrovni, kterým je Policie České republiky. Dvě stížnosti na postup správce při zpracování osobních údajů byly zařazeny jako součást pravidelného auditu národní součásti SIS II, který ÚOOÚ vykonává na základě povinností vyplývajících z evropské legislativy.

Úřad dále obdržel celkem 26 podání, v rámci kterých se žadatelé dotazovali na vízovou politiku České republiky či na průběh vyřizování svých vízových žádostí. Vzhledem k tomu, že tato problematika nespadá do zákonem stanovených kompetencí ÚOOÚ, 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 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, jsou v každém státě schengenského prostoru pravidelně prováděny evaluace základních aspektů schengenské spolupráce. Mezi ty patří ochrana vnitřních a vnějších hranic, policejní spolupráce a úroveň ochrany osobních údajů při využívání SIS II.

Hodnotící týmy jsou vždy vytvářeny ad hoc k jednotlivým evaluacím. Ty jsou složeny ze zástupců Evropské komise a expertů ze členských států. Hodnotící tým na základě předložených dokumentů a kontroly na místě připraví zprávu shrnující jeho poznatky o souladu praxe v daném členském státě s požadavky schengenského acquis. Tato kontrola obvykle zahrnuje návštěvu policejního útvaru, jež zajišťuje provoz národní součásti schengenské databáze, orgánu pro ochranu osobních údajů a dalších dotčených orgánů.[13]

V roce 2017 se zaměstnankyně Úřadu účastnila jako národní expertka evaluační mise ve Španělsku (říjen 2017).

[13] Ministerstvo zahraničních věcí pro oblast vydávání schengenských víz, azylový úřad, ministerstvo vnitra jako gesční orgán pro schengenskou spolupráci.

Analytická činnost

1. Analýza shromažďování osobních údajů prostřednictvím úsekového měření

Analytické oddělení (ANA) se v souvislosti s problematikou shromažďování osobních údajů fyzických osob při tzv. úsekovém měření[14] zabývalo modelovou situací, která se týkala oprávněnosti plošného uchovávání osobních údajů Policií ČR po určitou (různou) dobu bez vazby na spáchání protiprávního jednání dotčenými osobami. Na shodný problém upozorňovaly opakovaně zprávy o stavu lidských práv v České republice, poprvé v roce 2006: „*Pochybnosti z hlediska ochrany soukromí vzbuzuje zavedení kamerových systémů k tzv. úsekovému měření rychlosti vozidel. Dochází k plošnému zaznamenávání konkrétních údajů o pohybu osob (vozidel) bez toho, že by impulzem pro záznam bylo zjištěné porušení předpisů… Je tak porušena zásada, že represivní složky smějí být činné jen na základě zjištěných faktů o porušení pravidel.*" Rovněž podle zprávy zveřejněné nevládní organizací Iuridicum Remedium[15] policie plošně zaznamenává pohyb aut, fotí řidiče a automatizovaně rozeznává SPZ, přičemž rozdílná doba uchovávání záznamů v jednotlivých krajích je těžko obhajitelná.

Uvedené shromažďování dat se uskutečňuje za účelem ochrany veřejného pořádku, což je výjimka ve vztahu k zákonu o ochraně osobních údajů. Platí totiž speciální právní úprava zákona o Policii ČR; to ovšem neznamená vyloučení obecných principů ochrany osobních údajů a dozorové role Úřadu. Titulem pro zpracování osobních údajů je v tomto případě institut úsekového měření upravený v § 79a zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, podle kterého je policie a obecní policie oprávněna měřit rychlost vozidel za účelem zvýšení bezpečnosti provozu na pozemních komunikacích.[16]

[14] Při tzv. úsekovém měření vozidel se zaznamenává registrační značka vozidla na počátku i konci úseku.

[15] Viz: Dostupné z http://www.iure.org/15/1210/policie-plosne-zaznamenava-pohyb-aut-foti-ridice-automa-tizovane-rozeznava-spz-udaje-o-kazdem, obdobně http://www.autoforum.cz/zivot-ridice/policie-uchovava-fotky-vsech-co-projedou-kolem-jejich-radaru-i-kdyz-nic-neprovedli/.
U zveřejněné zprávy není uvedeno její datum.

[16] Například § 17b zákona č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů.

Relevantní právní úpravou, která umožňuje Policii ČR pořizování záznamů, je ustanovení § 62 zákona č. 273/2008 Sb., o Policii ČR. Policie podle něj může, je-li to nezbytné pro plnění jejích úkolů, pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných, stejně jako zvukové, obrazové nebo jiné záznamy o průběhu úkonu. Dále se předpokládá uveřejnění informace o zřízení napevno instalovaných kamerových systémů užívaných policií např. k monitorování právě dopravní situace.

Ve většině případů záznamy shromážděné při úsekovém měření obsahují osobní údaje, na které se vztahují obecná pravidla upravená v § 79 a následujících zákona o Policii ČR. Pokud jde o dobu uchovávání osobních údajů, podle § 87 odst. 1 policie uchovává osobní údaje pro účely podle § 85 po dobu, která je nezbytná k účelu jejich zpracování. Pomine-li tento účel, osobní údaje zlikviduje s výjimkou případů výslovně stanovených v zákoně. Pokud jde o výraz „doba nezbytná pro účely zpracování", ačkoliv je tato formulace obecná, nepochybně neznamená libovůli, ale prokazatelně nezbytnou dobu. Tak jako při jakémkoliv výkonu pravomoci je třeba i při pořizování záznamů respektovat zásadu přiměřenosti (§ 11 zákona o Policii ČR), a to z hlediska míry zásahu do práv osob, jichž se záznamy týkají, a závažnosti konkrétního úkolu, který tím policie plní. Pro účely interpretace doby nezbytné pro zpracování se rovněž uplatní obecné principy platné pro ochranu osobních údajů, především tzv. princip minimalizace uchovávání osobních údajů. Z analýzy ANA vyplynulo, že za slabé místo shromažďování údajů v oblasti úsekového měření by bylo třeba považovat, pokud by byla prokázána různá doba uchovávání záznamů osob v jednotlivých krajích. To by totiž svědčilo o tom, že údaje lze zpracovat za kratší dobu a není nezbytné je uchovávat déle.

Provádění úsekového měření Policií ČR se tedy uskutečňuje na základě speciální právní úpravy při zachování dozorové role ÚOOÚ. Shromažďování záznamů v oblasti silniční dopravy za účelem veřejného pořádku je nutno po určitou přiměřenou dobu stanovenou jako „nezbytnou k účelu jejich zpracování", kterým je bezpečnost provozu na pozemních komunikacích, považovat za souladnou se zákonem i ve vztahu k bezúhonným osobám. Samotný Úřad již v minulosti k problematice úsekového měření uvedl, že tento způsob měření zpracovává i osobní údaje osob, které se nedopustily přestupku, a proto je nepřetržité sledování všech projíždějících vozidel silným zásahem do soukromí jednotlivce a jeho umístění musí být podloženo skutečnou nebezpečností daného úseku vyvolávající potřebu stálého dozoru.[17] Z pohledu ochrany osobních údajů to prakticky znamená, že kamery by měly být instalovány, pokud k tomu existují bezpečnostní důvody a neměly by být umisťovány a používány nadbytečně. Rovněž rakouský ústavní soud v minulosti k problematice úsekového měření rychlosti uvedl, že sběr osobních dat musí probíhat tak, aby byl pro řidiče místně a časově předvídatelný.[18] Informace o umístění kamer by měly být zveřejněny tak, aby ke shromažďování osobních údajů docházelo pro řidiče předvídatelným způsobem. Důvodem pro jejich umístění je totiž prevence nehod v oblasti provozu na dopravních komunikacích, tedy ochrana hodnot, jimiž je zdraví a život občanů,[19] nikoliv výběr pokut.

[17] https://www.uoou.cz/zpracovani-osobnich-udaju-v-souvislosti-s-merenim-rychlosti-vozidel/d-6230
[18] https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Dokumentnummer=JFT_09929385_06G00147_00
[19] Na českých silnicích zemřelo například v roce 2015 669 lidí. Policie vyšetřovala skoro 93 tisíc nehod. Nejtragičtějšími měsíci byly červenec a září, kdy si havárie vyžádaly 80 životů.

2. Analýza sledování soukromého obydlí kamerou souseda

Předmětem posouzení ANA byla modelová situace, kdy vlastník nemovitosti (fyzická osoba) namítal, že je zasahováno do jeho práva na soukromí, neboť vchod do jeho domu je soustavně monitorován kamerou z protějšího domu. Stěžovatel požadoval nápravu stavu Úřadem a veřejným ochráncem práv. Provozovatel kamery uvedené skutečnosti popíral a tvrdil, že soukromí jiné osoby nesleduje. Z právního hlediska bylo problematické, jakým způsobem by se stěžovatel měl domáhat nápravy závadného stavu. Je přitom nepochybné, že sledování fyzické osoby kamerami závažně zasahuje do soukromí fyzických osob a je třeba nastavit jeho hranice. Obzvlášť v situaci sledování rodinného domu bezpečnostní kamerou sousedem či jinou třetí osobou je závažně dotčeno právo na soukromí v prostoru vyhrazeném jeho osobnímu a intimnímu životu.[20] Pravidlem by mělo být, že vlastník kamery v zásadě může až na výjimky sledovat kamerou jen vlastní pozemek či nemovitost. Přípustná je pouze malá tolerance, jak vyplývá z rozhodovací činnosti ÚOOÚ.

Ačkoliv v ČR neexistuje speciální zákon o kamerách, není pochyb o tom, že v případě zpracování osobních údajů by se ve výše uvedeném případě uplatnila působnost zákona o ochraně osobních údajů. Podle současného výkladu může být za zpracování považováno provozování kamerového systému se záznamem i bez záznamu. Hlavní problém je ovšem v tomto případě v tom, že nelze ověřit skutečnosti tvrzené vlastníkem kamery a stěžovatelem. Úřad totiž nemá možnost vstupu na pozemek a do obydlí fyzické osoby, tedy i vlastníka kamery. Je proto sporné, zda se jedná o zpracování osobních údajů.

Pokud by se nejednalo o zpracování osobních údajů, přichází v úvahu ochrana osobnosti podle příslušných ustanovení v občanském zákoníku (dříve §§ 11–16 zákona č. 40/1964 Sb., nyní § 84–90 zákona č. 89/2012 Sb.). V právní teorii se hovoří o tzv. komplementaritě právní úpravy ochrany osobnosti fyzické osoby, která spočívá v zabezpečení účinné ochrany osobnosti fyzické osoby prostředky různých právních odvětví právního řádu.[21] Dlužno však doplnit, že toto pojetí komplementarity není dosud doprovázeno příslušnou judikaturou Nejvyššího soudu.

Při řešení zadané otázky je předmětem ochrany tedy právo na soukromí. Právo na soukromí,[23] případně právo na informační sebeurčení[24] jsou tzv. základní práva, která jsou v právním státě garantována prostřednictvím ústavního pořádku. Pokud jde o záruky výše uvedených základních práv, podle pracovního materiálu stanovícího podmínky pro zásah do práva na soukromí a na ochranu osobních údajů zpracovaného expertní pracovní skupinou WP29[25] by se obecně měla uplatnit následující pravidla:

- zpracování by mělo být založeno na jasných, přesných a dostupných pravidlech;
- musí být prokázána nezbytnost a proporcionalita zásahu s ohledem na legitimní účel;
- musí existovat nezávislý mechanismus dohledu;
- jednotlivec musí mít k dispozici dostupné efektivní opravné prostředky.[26]

---

[20] Metodický materiál Úřadu požaduje, aby zásahy do soukromí nebyly nadměrné.
[21] Knap, Švestka, Jehlička, Pavlík, Plecitý: Ochrana osobnosti podle občanského práva. Str. 25. Linde Praha, 2004.
[22] Rozhodnutí Úřadu č.j. UOOU-01297/16-48.
[23] Čl. 7 Listiny základních práv EU.
[24] Čl. 10 odst. 3 Listiny. Čl. 8 Listiny základních práv EU.
[25] Pracovní skupina byla ustavena podle **směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.**
[26] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

K upřesnění otázky hranic sledování kamerou také významně přispěl rozsudek Soudního dvora EU věci František Ryneš C 212/13 ze dne 11. prosince 2014, když posoudil položenou předběžnou otázku na základě směrnice 95/46/ES týkající se zpracování osobních údajů. Zabýval se zde výkladem pojmu „výkon výlučně osobních či domácích činností", z pohledu působnosti směrnice. Soudní dvůr uvedl, že článek 3 odst. 2 druhá odrážka směrnice Evropského parlamentu a Rady 95/46/ES musí být vykládán tak, že provozování kamerového systému, který zabírá též veřejné prostranství, nepředstavuje zpracování údajů pro výkon výlučně osobních či domácích činností ve smyslu uvedeného ustanovení.[27] Jinými slovy, obrazový záznam pořízený prostřednictvím kamerového systému nainstalovaného osobou na jejím rodinném domě a zabírajícího veřejné prostranství není výjimkou z působnosti směrnice o ochraně osobních údajů (a tedy ani pravidel upravených zákonem o ochraně osobních údajů).

Pokud jde o otázku, do jaké míry a jakými prostředky je chráněno soukromí fyzické osoby, na jejíž obydlí směřují kamery, je vždy nutné zohlednit konkrétní okolnosti případu, kterých může být celá řada, a mohou zakládat odlišné posouzení případu či různou intenzitu postihu. Půjde například o to, zda je sledováno veřejnosti přístupné místo či soukromý prostor, jaký druh kamery je používán (skutečná či atrapa, se záznamem nebo bez záznamu), jaký je dosah kamery mimo vlastní pozemek (malá či větší vzdálenost od hranice pozemku), kam je kamera namířena (nejvíce citlivý bude vchod nebo místa, kde se odehrává soukromý život), zda je možné ověřit skutečný stav věci, zda je správcem fyzická či právnická osoba, důvody, pro které je monitorován veřejný prostor a další.

V případě zpracování osobních údajů fyzické osoby (tzv. subjektu údajů) správcem platí zákon o ochraně osobních údajů, takže subjekt údajů se může domáhat práv, která mu dává zákon (např. právo na přístup k údajům a práv na shromážděné informace), případně může upozornit Úřad na závadné jednání, aby tento mohl využít administrativní postupy či sankce, které zákon obsahuje. V situacích, ve kterých se nejedná o zpracování údajů, může být soukromí předmětem ochrany pouze v civilním řízení na základě žaloby na ochranu osobnosti podle občanského zákoníku. V tomto ohledu je však nutné vyčkat na případná soudní rozhodnutí, zejména na rozhodnutí nejvyšších soudů (Nejvyšší správní soud či Nejvyšší soud).

O tom, jaká jsou pravidla pro zacházení s kamerami, informuje Úřad veřejnost v případě potřeby. Je však na místě upozornit, že k řešení sporných záležitostí není vždy nutné využívat soudní cestu. Například vlastník kamery, který z konkrétních závažných důvodů hodlá zvolit toto řešení k ochraně svého majetku, může předem požádat o souhlas dotčenou osobu, případně jí názorně kameru ukázat a rozptýlit její pochybnosti, že je monitorováno její obydlí. Potom nemůže dotčená osoba tvrdit, že je monitorována, nebo mít subjektivní pocit, že je sledována, pakliže ovšem podstata sporu není v něčem jiném (sousedský spor). Vlastníci kamer (či atrap) by měli být také poučeni o alternativních způsobech zabezpečení nemovitosti. V řadě případů je efektivnější spolehlivé mechanické zabezpečení, které může být zároveň levnější a účinnější. Měli by být také informováni, že za zásah do soukromí jiné osoby by mohly soudy

[27] Článek 3 odst. 2 druhá odrážka směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob musí být v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů vykládán v tom smyslu, že provozování kamerového systému nepředstavuje zpracování údajů pro výkon výlučně osobních či domácích činností ve smyslu uvedeného ustanovení. Obrazový záznam zachycující osoby však v takovém případě musí být ukládán formou nekonečné smyčky do takového nahrávacího zařízení umístěného fyzickou osobou na jejím rodinném domě za účelem ochrany majetku, zdraví a života majitelů domu, přičemž takový systém zabírá též veřejné prostranství. Může se například jednat o pevný disk.

potenciálně považovat i pocit dotčené osoby, že je předmětem systematického, trvajícího a identifikujícího sledování.

Ochraně soukromí fyzických osob je tedy třeba poskytnout ochranu, jejíž způsob a prostředky je určen konkrétními okolnostmi případu. ÚOOÚ nemůže ve všech případech kamerového sledování poskytnout ochranu dotčenému subjektu, může jednat jen v mezích své působnosti stanovené zákonem. Za situace, kdy ještě neexistuje dostatečná soudní judikatura vztahující se k ochraně soukromí, je vhodné, aby Úřad poskytoval v rámci osvětové činnosti veřejnosti poučení, jakým způsobem postupovat. Tyto závěry ÚOOÚ zaujal rovněž v rámci diskuse s veřejným ochráncem práv.

3. Analýza dat předávaných v rámci onkologického screeningu z pohledu ochrany osobních údajů

Onkologické screeningové programy představují ambiciózní projekt v oblasti ochrany veřejného zdraví, jehož realizace vychází z toho, že rakovina je klíčovým problémem ve všech členských státech Evropské unie (EU). To vedlo k podpoře přijetí národních onkologických programů a k zavedení onkologického screeningu u nejzávažnějších nádorových onemocnění. Jeho podstatou je veřejná podpora použití údajů o rakovině pro výzkum veřejného zdraví pro účely předcházení a léčby této nemoci. Onkologické screeningové programy (screening nádorů kolorekta, karcinomu prsu a děložního hrdla) byly v ČR systematicky zahájeny na základě doporučení Rady EU z roku 2003 o screeningu rakoviny a postupně realizovány. Jeho provádění je plně v kompetenci národních úřadů.

S implementací onkologických screeningových programů je úzce spojena otázka ochrany osobních údajů. V tomto ohledu se ve výše citovaném doporučení stanoví, že veškeré postupy sběru, uchovávání, převádění a analyzování údajů ve zdravotnických registrech musí být plně v souladu s úrovní ochrany, kterou stanoví jak směrnice 95/46/ES, tak relevantní právní úprava členských států o správě a zpracování zdravotnických údajů (zejména odkaz na čl. 8 směrnice 95/46/ES). Konečně podle čl. 3 doporučení musí monitorování vyhovět standardům definovaným evropskou sítí pro onkologické registry. Vznik a vedení screeningových databází tak musí být v plném souladu s relevantní právní úpravou na ochranu osobních údajů.

Úřad se již v minulosti (v letech 2011–2012) zabýval dodržováním povinností správce v souvislosti se shromažďováním a zpracováváním osobních údajů za účelem správy dat při monitoringu onkologických screeningových programů. Dospěl k závěru, že v těchto případech nejsou zpracovávány osobní údaje, ale anonymní údaje.[28] *V souvislosti s průběžným vývojem a upřesňováním právního rámce ochrany osobních údajů vznikla potřeba teoreticky přezkoumat výše uvedený závěr z hlediska souladu s novějšími teoretickými poznatky v oblasti ochrany osobních údajů*, např. se stanoviskem WP29 v otázce pojmů osobní údaj,[29] s nedávným rozsudkem Soudního dvora EU ve věci *Breyer vs. Bundesrepublik Deutschland*,[30] případně s připravovaným obecným nařízením o ochraně osobních údajů (účinným od 25. května 2018).

Obecně platí, že Úřad v souvislosti s přípravou na GDPR přezkoumává svá dřívější stanoviska v oblasti ochrany osobních údajů. To se potenciálně týkalo i otázky zpracování údajů

[28] Výroční zpráva Úřadu pro ochranu osobních údajů z roku 2012, str. 35–36.
[29] Zřejmě jde o Stanovisko Pracovní skupiny pro ochranu údajů zřízené podle čl. 29 č. 4/2007 k pojmu osobní údaje ze dne 20. června 2007.
[30] Věc C-582/14 Patrick Breyer proti Bundesrepublik Deutschland ze dne 19. října 2016.

o pacientech v rámci screeningu onkologických onemocnění, kterou se ANA zabývala jako modelovým případem, viz níže.

Základní otázkou ve výše uvedených souvislostech při novém posuzování bylo, zda jsou v rámci screeningu předávány osobní údaje a zda jde o zpracování osobních údajů, které podléhá režimu zákona o ochraně osobních údajů. Pokud by totiž správce dostával anonymní údaje a pracoval jen s nimi, nejednalo by se o zpracování osobních údajů. Další zásadní otázkou, kterou si bylo nutno položit z pohledu současného chápání definice osobních údajů v kontextu rozsudku Soudního dvora ve věci Breyer, byla otázka identifikace osobních údajů, tedy zda je možné data předávaná správci zasadit do takového kontextu, aby mohla vést k identifikaci subjektu údajů. Jinými slovy, zda se jedná o osobní údaje, které mohou být identifikovány nepřímo.

Tyto otázky ovšem nebylo možno řešit pouze teoreticky. K jejich posouzení bylo sice nutné vyjít z relevantní právní úpravy, stanovisek a judikatury, ale i ze znalosti toho, jakým konkrétním způsobem dochází k předávání osobních údajů ze zdravotnických zařízení přes screeningová centra správci. Aktuální zjištění z kontrolní činnosti v tuto chvíli Úřad nemá. Mohl proto pouze pomocně vyjít z dřívějších kontrolních zjištění. V souvislosti s výše popsaným posunem v oblasti osobních údajů by se v takové situaci ÚOOÚ klonil k závěru, že předávaná data o vyšetřeních by měla být posuzována jako osobní údaje.

Takový závěr by samozřejmě teoreticky znamenal, že na činnost správce osobních údajů získaných v rámci onkologických screeningových programů je třeba aplikovat právní úpravu ochrany osobních údajů. Subjektům údajů by tak bylo zaručeno vykonávat svá práva (přístup k údajům) a byla by zajištěna vyšší úroveň ochrany osobních údajů a soukromí subjektů údajů. Na správce údajů by totiž byly kladeny požadavky pro zajištění vyšší bezpečnosti těchto dat před náhodnými úniky a jejich možným zneužitím. Zároveň je z veřejně dostupných zdrojů zřejmé, že některá opatření zajišťující vyšší úroveň ochrany osobních údajů již byla v posuzované oblasti aplikována. Jedná se například o aplikaci principů *privacy by design*, které lze pozorovat v užití šifrování či v logickém dělení datového prostoru. Další možnosti ve vztahu k ochraně osobních údajů rozšíří implementace obecného nařízení.

Legislativní činnost

Obecně

V roce 2017 se ÚOOÚ věnoval především implementaci nového unijního regulačního rámce ochrany osobních údajů (GDPR, JHAD & PNRD), o čemž pojednává zvláštní kapitola výroční zprávy.

U návrhů ostatních právních předpisů je Úřad povinné připomínkové místo. Bohužel je některými resorty, jejichž návrhy mají značný dopad na ochranu soukromí, soustavně opomíjen.

ÚOOÚ již od 1. ledna 2013 sleduje vyhodnocování dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů (DPIA).[31] Bohužel ani po čtyřech letech praxe není podoba DPIA optimální. Některé resorty opakovaně nepravdivě uvádějí, že „zpracování osobních údajů nebude nijak zasahovat do ochrany soukromí".

Jedním z nejdůležitějších návrhů předpisů, ke kterému se Úřad v rámci legislativního procesu vyjadřoval, byl návrh věcného záměru zákona o sčítání lidu, domů a bytů v roce 2021. Věcný záměr počítá s maximálním využitím existujících administrativních zdrojů dat a minimální zátěží respondentů, neboť primárním způsobem sběru dat z terénního šetření bude on-line sčítání. ÚOOÚk návrhu uplatnil připomínky týkající se specifikace osobních údajů a jejich dalšího využívání.

Unijní právní řád

Vzhledem ke kvantitativní změně evropské regulace a jejího vlivu na českou normotvorbu se posílila důležitost unijního právního řádu. Úřad na to zareagoval tím, že do své působnosti zařadil od 20. března 2017 aktivní sledování přípravy unijních právních předpisů (směrnic a nařízení) v resortních koordinačních skupinách (RKS). Ty slouží k vypracování stanoviska ČR pro jednání pracovních skupin Rady EU, tj. Rady ministrů členských zemí. Výstupy jsou v chráněném režimu, a proto není možné o nich sdělovat většinu informací.

[31] Povinnost z legislativních pravidel vlády bude nyní právní povinností z článku 35 GDPR.

ÚOOÚ je k 1. lednu 2018 zapojen do RKS ministerstva financí, ministerstva průmyslu a obchodu, ministerstva spravedlnosti, ministerstva vnitra, ministerstva zdravotnictví, Národního úřadu pro kybernetickou a informační bezpečnost, Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví a Úřadu vlády. Kromě priorit popsaných dále se Úřad podrobněji věnoval oblasti justice a vnitra, zejména návrhu nařízení ECRIS-TCN, EURODAC, ETIAS či PNR.

Elektronické soukromí

Návrh nařízení o respektování soukromého života a ochrany osobních údajů v elektronických komunikacích (CELEX: 52017PC0010) má anglickou zkratku *ePrivacy* či *ePR* a má nahradit stávající směrnici 2002/58/ES. K tomuto návrhu má podpůrnou působnost obecné nařízení. V současné době již byla ePR schválena v Evropském parlamentu. V Radě EU projednání tak rychlé není; původní předpoklad, že ePrivacy nabyde účinnosti stejně s GDPR, tj. 25. května 2018, není technicky možné naplnit.

Gestorem je ministerstvo průmyslu a obchodu. Návrh je velice kontroverzní a je odbornou veřejností podrobně sledován. Jedná se zejména o *cookies*, nastavení prohlížečů, zadržení údajů a komunikaci mezi stroji. Úřad vychází ze stanovisek unijních ochránců dat: WP29 a evropského inspektora ochrany údajů. Zaměřil se zejména na problematiku přímého marketingu, obtěžujících spamů či volání, které se v praxi dozorového úřadu nejvíce řeší.

Zadržení údajů

Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, anglicky *data retention*, byla zrušena rozsudkem ESD *Digital Rights Ireland v. Irsko*, sp. zn. C-293/12. EU proto připravuje novou regulaci preventivního uchovávání, tj. zadržení, provozních a lokalizačních údajů v telekomunikacích, při respektování rozsudku ESD *Tele2 Sverige AB v. Post-och telestyrelsen*, sp. zn. C-203/15, o zákazu plošného zadržování údajů občanů EU. Řešením tedy je zadržení údajů v konkrétních a odůvodněných případech, zatímco v ostatních případech má policie využívat údaje, které mají telekomunikační operátoři pro své vlastní potřeby. Gestorem je ministerstvo vnitra.

Volný pohyb neosobních údajů

Návrh nařízení o volném pohybu neosobních údajů (CELEX: 52017PC0495) chce dosáhnout informační výměny, která by nebyla omezena hranicemi. Gestorem je Úřad vlády ČR. Obchodní společnosti ani členské státy by kromě bezpečnostních výjimek nesměly požadovat uchování neosobních údajů na území jednoho státu. Tím by měla být zaručena konkurenceschopnost evropské datové ekonomiky. ÚOOÚ zde upozornil na to, že v praxi bude obtížné rozlišit osobní a neosobní údaje a že datová sada, která obsahuje byť jediný osobní údaj, je již souborem osobních údajů.

Implementace nového unijního regulačního rámce ochrany osobních údajů (GDPR, JHAD a PNRD)

Ministerstvo vnitra jako gestor předložilo do meziresortního připomínkového řízení návrh zákona o zpracování osobních údajů (ZZOÚ). Jeho podstatou je adaptace českého právního řádu

na GDPR, transpozice JHAD[32] a promítnutí závazků z úmluvy Rady Evropy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat. ÚOOÚ je spolugestorem.

ZZOÚ má nahradit stávající zákon č. 101/2000 Sb., ochraně osobních údajů a o změně některých zákonů. Novelizace tohoto zákona vzhledem k nutnosti implementovat sekundární právní předpisy EU se vzhledem k velkému rozsahu změn ukázala být velice nepraktická. Ze zákona o ochraně osobních údajů jsou do ZZOÚ recipována ustanovení, která se vztahují k působnosti Úřadu. Mění se však jeho struktura; ZZOÚ nadále nepočítá s funkcí inspektorů.

Ministerstvo vnitra je rovněž gestorem návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů – doprovodného zákona k ZZOÚ. Spolugestorem je ministerstvo dopravy. Podstatou návrhu doprovodného zákona je transpozice PNRD[33] a sektorové změny vyvolané obecným nařízením či JHAD, zejména ve finančních a justičních předpisech. V rámci připomínkového řízení bylo navrženo změnit celkem 19 zákonů.

Navrhovanou právní úpravou dochází též ke změně zákona č. 341/2011 Sb., o Generální inspekci bezpečnostních sborů. Nově by měla GIBS disponovat některými pravomocemi obdobnými pravomocím policie. Jde o uveřejňování informací hromadnými sdělovacími prostředky, odnětí věci, ale i vstup do obydlí, jiného prostoru nebo na pozemek.

Úřad k návrhu zákona uplatnil 24 připomínek, z toho 19 zásadních a pět doporučujících, přičemž stěžejní byly připomínky týkající se rozsahu zpracovávaných osobních údajů Policií ČR a státními zastupitelstvími. ÚOOÚ například požadoval po předkladateli návrhu zdůvodnění, proč evidence Policie ČR, týkající se digitálních fotografií a vedená za účelem vyhledávání, odhalování nebo stíhání trestných činů, nemá být využívána pouze v souvislosti se zločiny. Dále Úřad požadoval, aby státní zastupitelství zpracovávala osobní údaje pouze v rozsahu odpovídajícím plněnému úkolu.

Vystoupení zaměstnanců oddělení legislativního

V prvním dubnovém týdnu roku 2017 se v Hradci Králové konal 20. ročník konference ISSS – Internet ve státní správě a samosprávě. Z pohledu ochrany osobních údajů se soustředil na téma GDPR (obecné nařízení o ochraně osobních údajů). Vedoucí oddělení Vít Zvánovec si ve svém vystoupení vytknul za cíl rozptýlit přílišné obavy z obecného nařízení o ochraně osobních údajů u laické i odborné veřejnosti a zdůraznit poselství Úřadu, že obecné nařízení znamená evoluci, nikoli revoluci.

Vedoucí oddělení legislativního se také na začátku července roku 2017 v rámci TAIEX zúčastnil semináře ochrany osobních údajů ve zdravotnictví v Ankaře. Vystoupil s příspěvkem o boji proti přenosným nemocem. Tato oblast je totiž podrobně regulována unijním právním řádem, takže se jí Turecko musí přizpůsobit.

Na konferenci České právo a informační technologie v Brně vystoupila Daniela Havlíková. Na akci prezentovala pohled Úřadu na návrh nařízení ePrivacy. Její vystoupení vzbudilo výrazný ohlas.

---

[32] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.
[33] Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016, o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

Příprava Úřadu na implementaci obecného nařízení o ochraně osobních údajů

Nadcházející účinnost obecného nařízení zásadním způsobem ovlivňuje činnost Úřadu a testuje jeho schopnost vypořádat se s novými úkoly. V roce 2017 začal ÚOOÚ s nařízením systematicky pracovat, odpovídat na dotazy veřejnosti, poskytovat informace na svých webových stránkách a v závislosti na svých personálních možnostech postupně zajišťovat širší okruh aktivit v procesu přípravy (činnost přednášková, konzultační a metodická). Výklad nového právního rámce se přitom s dalšími poznatky stále více strukturuje, jednak podle oblastí, ve kterých je ochrana osobních údajů zajišťována (např. bankovnictví, neziskový sektor), jednak podle charakteru povinných subjektů (veřejná správa, soukromý sektor). Od druhé poloviny roku 2017 lze mluvit o určitém cíleném přístupu či metodologii přípravy, pokud jde o aktivity vně Úřadu.

Seznámení se s obecným nařízením, nazývaným GDPR, je rovněž v nabídce velkého počtu školicích a vzdělávacích subjektů, zejména advokátních kanceláří a školicích agentur. Za předpokladu, že jsou splněny odborné nároky na zvládnutí problematiky osobních údajů, nelze proti tomuto způsobu osvěty nic namítat. Zpětná vazba, kterou ÚOOÚ má, ovšem ukazuje na určitá úskalí nabízených služeb. V některých případech, v reakci na nervozitu a nejistotu veřejnosti ohledně budoucích povinností plynoucích z obecného nařízení a hrozbu pokut, vycházejí uvedené vzdělávací subjekty vstříc aktuální poptávce a vzbuzují dojem, že jde o složitou problematiku, kterou si je nutné zajistit formou outsourcingu.[34] Také jim často chybí nezaujaté hodnocení nezbytné role ochrany soukromí a osobních údajů v digitálním věku, což problematiku ochrany osobních údajů odkazuje do role „dalšího evropského předpisu“, či není dostatečně vysvětlován způsob, jakým nařízení porozumět a aplikovat je na základě obecných principů.

Úřad v procesu přípravy na nařízení, kterou realizuje v rámci své osvětové a vzdělávací činnosti, volí vhodné koncepční přístupy a metody. Charakter samotného nařízení totiž předurčuje, jak s pravidly pro ochranu dat pracovat. Jde o to, že neexistuje a nebude existovat jediný univerzální manuál, metodika či vyčerpávající návod, jak implementovat či aplikovat GDPR. U každého subjektu musí být aplikována ochrana osobních údajů specifickým způsobem odpovídajícím charakteru zpracovávaných osobních údajů a vnitřnímu fungování organizace. K tomu je potřebná jak detailní znalost zkoumané oblasti, tak principů ochrany osobních údajů. Je třeba se rovněž orientovat v souvisejících oblastech jako IT technologie, kybernetická bezpečnost, archivní a spisová služba a další. Konečně je třeba přijmout fakt, že ochrana osobních údajů není neměnná, ale bude reagovat na rizika spojená s vývojem informačních technologií. Je tedy třeba počítat s tím, že ochraně osobních údajů bude potřebné věnovat kontinuální pozornost a sledovat její vývoj.

Kromě toho je třeba zdůraznit, že jedním z hlavních konstrukčních prvků nařízení je princip odpovědnosti správce či zpracovatele. Prakticky to znamená, že pokud ÚOOÚ poskytuje konzultační činnost budoucím správcům, požaduje, aby se tito aktivně spolupodíleli na přípravě konzultací. Jedině oni totiž detailně znají specifika oboru, v němž působí, povahu vnitřního fungování své organizace a vykonávaných činností a jsou schopni připravit přehledy a analýzy

[34] Outsourcing (dostupné z https://cs.wikipedia.org/wiki/Outsourcing "Angličtina" angl. out = vně, a source = zdroj) znamená, že zadávající subjekt vyčlení různé podpůrné a vedlejší činnosti a svěří je smluvně jiné (dostupné z https://cs.wikipedia.org/wiki/Společnost "Společnost (podnikání)" společnosti čili subkontraktorovi, specializovanému na příslušnou činnost. Je to tedy druh (dostupné z https://cs.wikipedia.org/wiki/Dělba_práce "Dělba práce") dělby práce, činnost však není zajišťována vlastními zaměstnanci firmy, nýbrž na základě smlouvy za finanční úplatu.

zpracovávaných osobních údajů a v návaznosti na to formulovat případné otázky. To vše již vyžaduje určitý stupeň porozumění problematice ochrany osobních údajů. Tento způsob přípravy požaduje Úřad za efektivní. Nadto preferuje, aby se do příprav na implementaci obecného nařízení v daném sektoru zapojila komora, asociace, sdružení či jiný subjekt, které zohlední právní i etické aspekty dané oblasti. Tato spolupráce zároveň do budoucna vytváří vhodnou platformu pro další činnosti (např. kodexy chování) či metodickou pomoc poskytovanou konkrétním subjektům při ochraně osobních údajů v dané oblasti.

Jak již bylo uvedeno, činnost ÚOOÚ v oblasti konkrétní přípravy na nařízení lze zhruba členit na činnost přednáškovou, konzultační a metodickou, přičemž pro každou z těchto aktivit jsou uplatňovány přístupy, které posilují aktivní participaci zainteresovaných subjektů na implementaci obecného nařízení. Např. u přednáškové činnosti je upřednostňováno, aby se na ní aktivně podílel příslušný ústřední orgán státní správy, pokud jde o veřejnou správu, či zástupce zájmové nebo profesní asociace, pokud jde o soukromý subjekt. Pokud jde o metodickou činnost v oblasti ochrany osobních údajů, Úřad za rozhodující považuje aktivní přístup orgánů, do jejichž působnosti náleží metodické řízení dané oblasti (např. metodický pokyn ministerstva školství v případě škol či metodický pokyn ministerstva zdravotnictví určený nemocnicím). ÚOOÚ se v těchto případech nebrání poskytnutí součinnosti ve formě konzultace, nemůže však nahrazovat koncepční a metodickou činnost uloženou jednotlivým státním orgánům.

Konkrétně v loňském roce pracovníci Úřadu zajistili či se podíleli na celkem 86 bezplatných přednáškách po celé republice. Zvláštní pozornost byla především věnována subjektům, jejichž činnost nějakým způsobem přispívá k prosazování veřejného zájmu, jako jsou např. obce, profesní sdružení, církve či neziskové organizace. Pozornost byla také věnována malým a středním podnikům. Jako konkrétní příklad dobře zvládnuté součinnosti lze uvést cyklus přednášek pro obce organizovaný Svazem měst a obcí, na němž se podílel ÚOOÚ i ministerstvo vnitra.[35] Předávání teoretických poznatků bylo v tomto případě doprovázeno postupným vytvářením srozumitelných metodických materiálů. Další příklad podnětné spolupráce představovaly interaktivní semináře pořádané Úřadem pro neziskové subjekty, např. pro Armádu spásy ČR. Podle zkušeností ÚOOÚ náležité vysvětlení problematiky obecného nařízení vede ke snížení či odstranění obav z nové právní úpravy, zvyšuje povědomí a zájem o problematiku ochrany osobních údajů a aktivizuje zahájení prací na implementaci GDPR.

Úřad také považuje za potřebné zdůraznit, že ochranu osobních údajů zejména ve veřejné správě by především měli zajišťovat vlastní pracovníci organizací, namísto využívání tzv. outsourcingu. Řešení pomocí vlastních pracovníků má pro organizaci více výhod. Jednou z nich je, že vlastní zaměstnanci zpravidla dobře znají vnitřní situaci v organizaci, jsou schopni podílet se na přípravě vnitřních předpisů a v případě potřeby budou dobře dostupní. Toto řešení je zpravidla také finančně úsporné oproti finančně náročnému outsourcingu.

Přípravu na implementaci obecného nařízení se nevyplatí podceňovat. Zejména v období předcházejícím účinnosti nařízení je vhodné považovat činnosti související s ochranou osobních údajů za prioritní.

---

[35] Akademie GDPR, dlouhodobého programu seminářů a výměny zkušeností organizovaného Svazem průmyslu a dopravy ČR s odbornou garancí Úřadu pro ochranu osobních údajů a expertů ze Svazu průmyslu a dopravy ČR, PRK Partners, IBM, KPMG a Masarykovy univerzity. Viz http://www.gdprakademie.cz/#o-akademii

Vyřizování stížností podle § 175 správního řádu

Ustanovení § 175 zákona č. 500/2004 Sb., správní řád, je institut, který slouží k ochraně práv dotčených osob pro případ, že jim zákon neposkytuje jiný prostředek ochrany, než kterým jsou odvolání nebo další řádné či mimořádné opravné prostředky.

V souladu s § 175 zákona č. 500/2004 Sb. mají dotčené osoby zákonem stanovené právo obrátit se na správní orgán se stížností, pokud se domnívají, že správní orgán postupoval nesprávně. Rovněž mají podle citovaného ustanovení právo obrátit se na správní orgán s podnětem na nevhodné chování úředních osob.

Stížnostmi podle § 175 zákona č. 500/2004 Sb. se Úřad zabýval i v roce 2017, kdy vyřídil celkem 34 stížností. Ve většině případů stěžovatelé vyslovili nesouhlas s vyřízením jejich předchozího podnětu, ve kterém bylo ze strany stěžovatelů vzneseno podezření z nezákonného zpracování osobních údajů. Z celkového počtu těchto stížností byly čtyři posouzeny jako důvodné a sedm stížností jako částečně důvodné. Zbylých 23 stížností bylo shledáno bezdůvodnými. Při porovnání celkového počtu stížností s předchozím rokem lze konstatovat, že celkový počet stížností zůstal prakticky nezměněn.

Dvacet tři stížností směřovalo proti postupu odboru pro styk s veřejností, jehož náplní je vyřizovat stížnosti a podněty, které jsou ÚOOÚ 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 bylo analytickým oddělením 14 stížností posouzeno jako bezdůvodné, čtyři stížnosti byly posouzeny jako důvodné a pět stížností jako částečně důvodné. V případě, že po přezkoumání podnětu stěžovatele bylo shledáno podezření z porušení zákona č. 101/2000 Sb., ná-

sledoval zákonem stanovený postup, kdy jsou tyto podněty postoupeny buď inspektorovi Úřadu k provedení kontroly, nebo oddělení správních činností k zahájení správního řízení pro podezření ze spáchání správního deliktu či přestupku.

V jedenácti případech se stěžovatelé obrátili na ÚOOÚ se stížností proti závěrům kontrolních postupů Úřadu nebo postupu při vedení kontroly inspektory Úřadu. Z tohoto celkového počtu byla jedna stížnost posouzena jako částečně důvodná a deset stížnosti jako bezdůvodné. Ve výše uvedených případech byl stěžovatel informován o výsledku šetření, příp. zjištěném pochybení a dalším postupu v dané konkrétní věci.

Ve všech případech byl příslušný útvar ÚOOÚ informován o vyřízení stížnosti. Pokud byl jeho postup shledán nesprávným nebo částečně nesprávným, byl vyzván k přijetí takových opatření, aby v obdobných případech již ke stejnému pochybení nedocházelo.

Z celkového počtu 34 podnětů, které Úřad obdržel od stěžovatelů, žádný nesměřoval proti nevhodnému chování úředních osob. Je proto 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 zodpovědně a v souladu s principy dobré správy.

Styky se zahraničím a mezinárodní spolupráce

Prioritou pro rok 2017 byla aktivní spolupráce v rámci Pracovní skupiny WP29. Kromě pravidelné účasti na plenárních zasedáních rozšířil Úřad své zastoupení do pracovních podskupin, kam vysílal své zástupce. Jednalo se o šest odborně zaměřených pracovních formací:

- Podskupina pro spolupráci mezi úřady,
- Podskupina pro technologii,
- Podskupina pro klíčová ustanovení směrnice 95/46,
- Podskupina pro hranice, cestování a vynucování práva,
- Podskupina pro mezinárodní předávání dat,
- Podskupina pro elektronickou státní správu (e-government).

Jednotliví delegáti se tak například podílejí na tvorbě pokynů a stanovisek, jež mají sloužit především správcům a zpracovatelům jako pomůcka pro přípravu na obecné nařízení o ochraně osobních údajů. K většině vydaných materiálů z této série pořídil ÚOOÚ ve vlastní režii české překlady, a to krátce po jejich oficiálním uveřejnění. Cílem bylo, aby se texty dostaly k co nejširšímu okruhu zájemců. Konkrétně jde o tyto materiály:

- Vodítka pro určení vedoucího dozorového úřadu správce nebo zpracovatele
- Vodítka týkající se pověřenců pro ochranu osobních údajů
- Vodítka týkající se práva na přenositelnost údajů
- Vodítka k uplatňování a stanovování správních pokut pro účely Nařízení 2016/679
- Vodítka k posouzení vlivu na ochranu osobních údajů a ke stanovení, zda zpracování bude „pravděpodobně mít za následek vysoké riziko“ pro účely Nařízení 2016/679
- Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679

- Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679
- Vodítka k souhlasu podle Nařízení 2016/679
- Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti

K většině uvedených dokumentů Evropská komise později vypracovala vlastní překlady do národních jazyků. Pro odlišení oficiálních verzí od překladů pořízených Úřadem byl u pracovních, neoficiálních verzí použit název „vodítka" v kontrastu k oficiálnímu výrazu „pokyny".

Koncem jara navštívila ÚOOÚ delegace srbských kolegů, kteří se zajímali především o otázky ochrany dat a soukromí v souvislosti s používáním moderních technologií (kamerové sledování, ochrana soukromí v prostředí internetu, provádění kontrol v této oblasti).

Krátce nato projevilo zájem o návštěvu Úřadu vedení japonské Komise ochrany dat. Schůzka se uskutečnila v červnu, přičemž hlavní pozornost japonských ochránců dat patřila obecnému nařízení o ochraně osobních údajů a jeho dopadům na činnost dozorových orgánů.

Jako každý rok vysílal ÚOOÚ své pracovníky na různé zahraniční konference a odborné semináře. Prioritou byly akce, které se konají pravidelně, jako např. jarní konference komisařů ochrany dat nebo setkání zástupců úřadů ze střední a východní Evropy. Obecně ve sledovaném roce došlo k omezení počtu cest na semináře a konference ve prospěch účasti na pracovních zasedáních v zahraničí. Vzhledem ke kompetencím Úřadu nebo v souvislosti s úsilím vyvíjet činnost v mezinárodních pracovních skupinách bývá jeho účast na těchto akcích vyžadována.

S obdobnou filozofií hodlá ÚOOÚ přistupovat k vysílání svých pracovníků na zahraniční cesty i v roce 2018.

Specifické téma posledních let představuje program štítu soukromí (Privacy Shield). Ten z rozhodnutí Evropské komise zajišťuje adekvátní ochranu osobních údajů předaných do Spojených států amerických společnostem, jež se zavázaly dodržovat zásady obsažené v Annexu II rozhodnutí o odpovídající úrovni ochrany osobních údajů zajištěné „euroamerickým štítem soukromí" z července 2016. Seznam společností, které se účastní uvedeného programu, vede ministerstvo obchodu Spojených států amerických (Department of Commerce) a je přístupný na webové stránce www.privacyshield.gov.

V září 2017 proběhlo první každoroční společné posouzení fungování štítu soukromí (annual review), kterého se za evropskou stranu zúčastnil tým složený ze zástupců Evropské komise a zástupců WP29. Právě ta vydala 28. listopadu, vedle zprávy Evropské komise, svou vlastní zprávu o výsledcích annual review. Tato zpráva konstatuje výrazné zlepšení, které Privacy Shield přinesl oproti zrušenému Safe Harboru, a to především v oblasti dohledu amerického ministerstva obchodu nad procesem certifikace jednotlivých účastníků programu. Zpráva WP29 zároveň vypočítává oblasti, kde je třeba pracovat na dalším vylepšení: návodnost pro firmy a transparentnost pro evropské subjekty údajů, nedostatky v dohledu nad plněním zásad ze strany firem, problém výkladu zvláštního režimu pro zaměstnanecká data, problém automatických rozhodnutí a profilování.

Co se týče oblasti přístupu amerických zpravodajských orgánů k osobním údajům předaným z Evropské unie do Spojených států, zpráva WP29 konstatuje, že tvrzení americké strany o tom, že nedochází k plošnému přístupu zpravodajských orgánů k předaným osobním údajům, nejsou podložena žádnými právně závaznými dokumenty. Nelze se přitom opřít ani o novou zprávu personálně poddimenzovaného Privacy and Civil Liberties Oversight Board (PCLOB).

Proto WP29 vyzývá Evropskou komisi i příslušné orgány Spojených států amerických, aby obnovily jednání v této věci. Zároveň vyzývá, aby byla americkou stranou urychleně obsazena jak pozice ombudsmana štítu soukromí, tak i neobsazené pozice PCLOB. Zároveň by měla být odtajněna interní procesní pravidla pro jednání ombudsmana se zpravodajskými orgány.

Úřad, sdělovací prostředky a komunikační nástroje

Uplynulý rok 2017 se z mediálního hlediska vyznačoval hned několika pomyslnými vrcholy a jedním ústředním tématem, které se prolínalo všemi dvanácti měsíci.

V prvním čtvrtletí se zájem médií soustředil na vyhlášení již tradiční soutěže „Moje soukromí! Nekoukat, nešťourat". Konkrétně se jednalo o její 11. ročník. Svou pozornost si v mediálním prostředí získaly také oslavy mezinárodního Dne ochrany osobních údajů, jehož součástí bylo diskusní setkání s předsedkyní Ivanou Janů a také prezentace pro krajské úřady s následnou diskusí na téma ochrany osobních údajů, které vzbudily mezi stovkami posluchačů značný zájem.

Zcela dominantním tématem však byla od počátku roku blížící se účinnost obecného nařízení o ochraně osobních údajů, známé také pod zkratkou GDPR.[36] Úřad mu proto od ledna věnoval výraznou pozornost. Na úrovni ústřední státní správy oslovila předsedkyně ÚOOÚ jednotlivé ministry s nabídkou pomoci při přípravě na obecné nařízení, přičemž upozorňovala zejména na povinnost ustanovit pověřence pro ochranu osobních údajů (DPO). Pro zástupce ministerstev uspořádal Úřad seminář, další odborné akce připravil pro ostatní ústřední úřady a jimi řízené či zřizované organizace. Zástupci ÚOOÚ navštívili s přednáškami také gymnázia.

Úřad se rovněž v roce 2017 připojil k oslavám Dne bezpečnějšího internetu. Cílem bylo podpořit bezpečnější a odpovědnější využívání internetu a on-line technologií, a to zejména dětmi a mladými lidmi.

Významnou akcí byla v první polovině roku z pohledu Úřadu i médií konference k obecnému nařízení s názvem GDPR 360°, která byla určena pro

[36] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

zástupce státní správy, podnikové právníky, odborníky na ochranu dat či majitele a jednatele společností. I tu osobně zahájila předsedkyně Ivana Janů.

Snaha o větší osvětu v oblasti ochrany osobních údajů a příprava na účinnost obecného nařízení stála rovněž v prvním pololetí za zahájením prací a uveřejňováním neoficiálních překladů materiálů skupiny WP29. Ty umožnily veřejnosti rychlejší a kvalitnější seznámení s jednotlivými částmi nařízení.

Média se v prvních šesti měsících intenzivně zajímala o témata, jakými bylo například využívání a zveřejňování policejních kamerových záznamů, odpovědnost za šíření obchodních sdělení či rekordní udělená pokuta za spam ve výši 4,25 milionu korun.

Na sklonku prvního pololetí ÚOOÚ slavnostně vyhlásil vítěze soutěže „Moje soukromí! Nekoukat, nešťourat", přičemž počet přijatých příspěvků byl rekordní a překonal dosavadní vrchol z roku 2009.

Ani v druhé polovině roku zájem celostátních i regionálních médií o téma GDPR nijak nepolevoval. Mediálním prostorem poměrně výrazně rezonovala i soudní prohra vydavatelství MAFRA, které podalo na Úřad žalobu kvůli udělené pokutě za zveřejnění soukromých telefonických hovorů bývalého premiéra Petra Nečase a jeho ženy Jany Nečasové (dříve Nagyové). Ještě výraznějšího zájmu médií se ÚOOÚ dočkal v případě kontroly systému elektronické evidence tržeb (EET), kterou zařadil do plánu kontrol. O stejném zájmu lze hovořit také v případě zahájení kontroly společnosti Internet Mall.cz, a.s. Ta přišla důsledkem hackerského útoku téměř o 750 tisíc údajů svých klientů.

Média se v závěru roku zajímala o téma zveřejňování platů úředníků, ke kterému se vyjadřoval také Ústavní soud. Konkrétně šlo o stanovisko Úřadu, který v něm zdůrazňoval nutnost velmi pečlivě zvažovat veškeré zásahy do soukromí.

ÚOOÚ také až do konce roku nadále zveřejňoval další vodítka v rámci dokumentů vydaných skupinou WP29 a kontinuálně pracoval na neoficiálních překladech jednotlivých textů.

MEDIÁLNÍ OBRAZ

Úřad se dlouhodobě netěšil přílišné mediální přízni. Důvody lze spatřovat v některých rozhodnutích o udělení pokuty, ke kterým se novináři díky dlouhotrvajícím soudním sporům neustále vraceli, ale i v samotné specializaci na ochranu osobních údajů. Odborná práce ÚOOÚ vyžaduje čas při řešení podnětů, což je v rozporu se současným mediálním trendem, který Úřadu veškeré zpravodajství přibližuje ke stále vyšší rychlosti a zkratkovitosti.

O výrazném posunu vztahu médií směrem k ÚOOÚ můžeme hovořit v souvislosti s vystoupením předsedkyně Ivany Janů k případu ekolo[37] a následnému vyjádření Úřadu ke kauze obce Kravaře. Nový přístup, v rámci kterého by patrně nebyla pokuta v případu ekolo, ani obci Kravaře vůbec udělena, byl výrazným signálem pro veřejnost, že dochází k postupnému vývoji v rozhodování ÚOOÚ, které se odlišuje od praxe za bývalého vedení.

Tato změna v přístupu pod současným vedením, které má snahu, aby byl ÚOOÚ více nápomocen veřejnosti a posuzoval jednotlivé případy individuálně, se setkala ze strany médií s velmi pozitivním ohlasem.

[37] Stanovisko Úřadu vydané dne 3. října 2017, strana 40

KNIHOVNA ÚŘADU

Knihovna Úřadu disponuje 2400 svazky, což činí meziroční nárůst o zhruba sto svazků ve srovnání s rokem 2016, z čehož jeden byl darem.

V prvním pololetí plnil prostor knihovny svou standardní funkci, kterou bylo zázemí pro zaměstnance, jimž byly k dispozici publikace potřebné pro jejich práci. Prezenčně však sloužil i odborné veřejnosti. Provoz v druhé polovině roku byl však silně ovlivněn plánovanou rekonstrukcí. Prostory totiž plnily zároveň funkci velké zasedací místnosti. Proto bylo rozhodnuto o přesunu knihovny do samostatných prostor, které budou lépe odpovídat jejímu účelu.

WEBOVÉ STRÁNKY ÚŘADU

Webové stránky patří i nadále mezi stěžejní komunikační nástroje Úřadu. Prostřednictvím své internetové prezentace ÚOOÚ informuje veřejnost především o své činnosti a legislativě z oblasti ochrany osobních údajů. Z výše uvedeného vyplývá, že jedním z hlavních témat pro Úřad byla v roce 2017 příprava na obecné nařízení, což se výrazně odrazilo na úpravách v uspořádání webu. Zásadním způsobem došlo ke změnám na titulní straně, kde byly vloženy zvýrazněné odkazy na jednotlivé části nové rubriky GDPR (obecné nařízení). Cílem bylo usnadnit orientaci návštěvníkům stránek, jejichž zájem o toto téma směrem ke konci roku neustále narůstal. Své vlastní odkazy z titulní strany webu tak má například základní příručka k GDPR, nejčastější otázky a odpovědi k obecnému nařízení či pokyny pracovní skupiny WP29.

Zmíněna byla nová rubrika GDPR (obecné nařízení), která vznikla přepracováním rubriky obecné nařízení EU, kde byly shromažďovány informace k obecnému nařízení o ochraně osobních údajů. Rubrika však získala v průběhu roku 2017 přehlednější členění a nové podrubriky. Odborníci Úřadu osobně vypracovali obsah většiny z nich. Konkrétně jde o upřesnění role ÚOOÚ v rámci GDPR, základní dvanáctibodovou příručku, ale také nejčastější otázky a odpovědi k obecnému nařízení nebo desatero omylů či zavádějících tvrzení. Úřad těmito změnami cílil na zjednodušení přístupu k důležitým informacím o GDPR široké odborné i laické veřejnosti.

ÚOOÚ i nadále věnoval na svém webu zvýšenou pozornost některým rubrikám. Judikatura obsahuje rozhodnutí českých i zahraničních soudů, která se týkají oblasti ochrany osobních údajů. Dozorová činnost je pak základním posláním Úřadu. Návštěvníci v ní naleznou přehled s podrobnými informacemi o kontrolách.

V roce 2017 doplnila webové stránky ÚOOÚ jejich mobilní verze, která zvýšila dostupnost jejich obsahu.

Informační systém ORG

Zákon č. 111/2009 Sb., o základních registrech, a jeho změna zákonem č. 100/2010 Sb., přinesl Úřadu nový úkol. Do 30. června 2012 vytvořit informační systém ORG jako součást systému základních registrů, která bude zajišťovat procesy spojené s identifikací fyzických osob a se zabezpečením jejich osobních údajů.

Smyslem začlenění Informačního systému ORG do systému základních registrů je ochrana identity občanů před zneužitím jejich osobních údajů. ORG je jedinou institucí, která dokáže překládat agendové identifikátory z jedné agendy do agendy druhé.

Od července 2012 tedy systém základních registrů shromažďuje a uchovává základní informace o fyzických osobách.

Informační systém ORG v systému základních registrů je realizován v rámci Integrovaného operačního programu, prioritní osa Modernizace veřejné správy – Cíl Konvergence, oblast podpory Rozvoj informační společnosti ve veřejné správě. Odbor strukturálních fondů MV ČR schválil na konci listopadu 2009 a letos skončí jeho pětiletá udržitelnost.

V roce 2014 byl přijat zákon č. 181/2014 Sb., o kybernetické bezpečnosti a prováděcí vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti. Zároveň vyšlo Nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury, doplněné Usnesením vlády č. 390/2015 ke 2. aktualizaci 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 e-governmentu.

Toto označení klade mimořádné nároky na technické vybavení a bezpečnostní 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.

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

K naplnění tohoto doporučení směřovala, v podstatné části letošního roku, činnost oddělení ORG. Byla ve znamení certifikace ISMS pro IS ORG.

Součástí certifikace byla například kontrola směrnic pro řízení přístupu do datových center, provozních řádů, bezpečnostní politiky, registru rizik a aktiv, plán obnovy apod.

Došlo k nastavení a doladění nástrojů pro sledování přístupů do systému. Tyto nástroje hlásí a registrují pravděpodobné a skutečné kybernetické útoky na IS ORG.

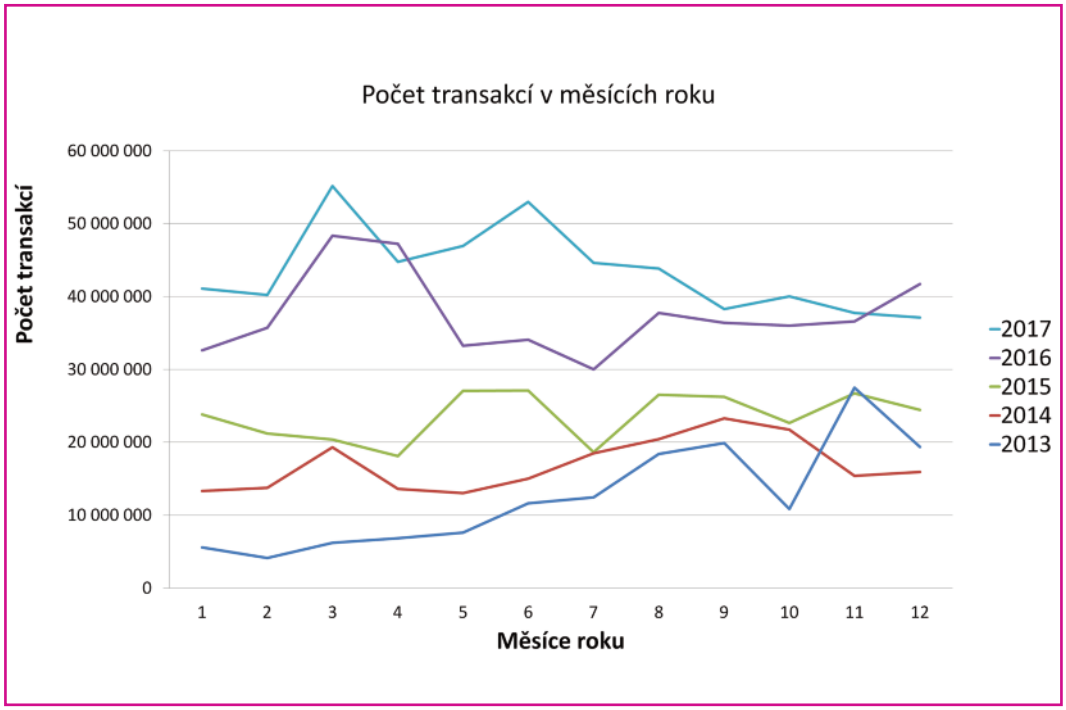
Na začátku listopadu 2017 se v sídle Úřadu uskutečnil bezpečnostní audit zaměřený na provoz IS ORG. Ten navazoval na předchozí audit z roku 2016, který přiznal ÚOOÚ pro IS ORG certifikát dle normy ČSN ISO/IEC 27001:2014.

Samotný provoz systému byl bez podstatných výpadků v komunikaci a dostupnosti dat.

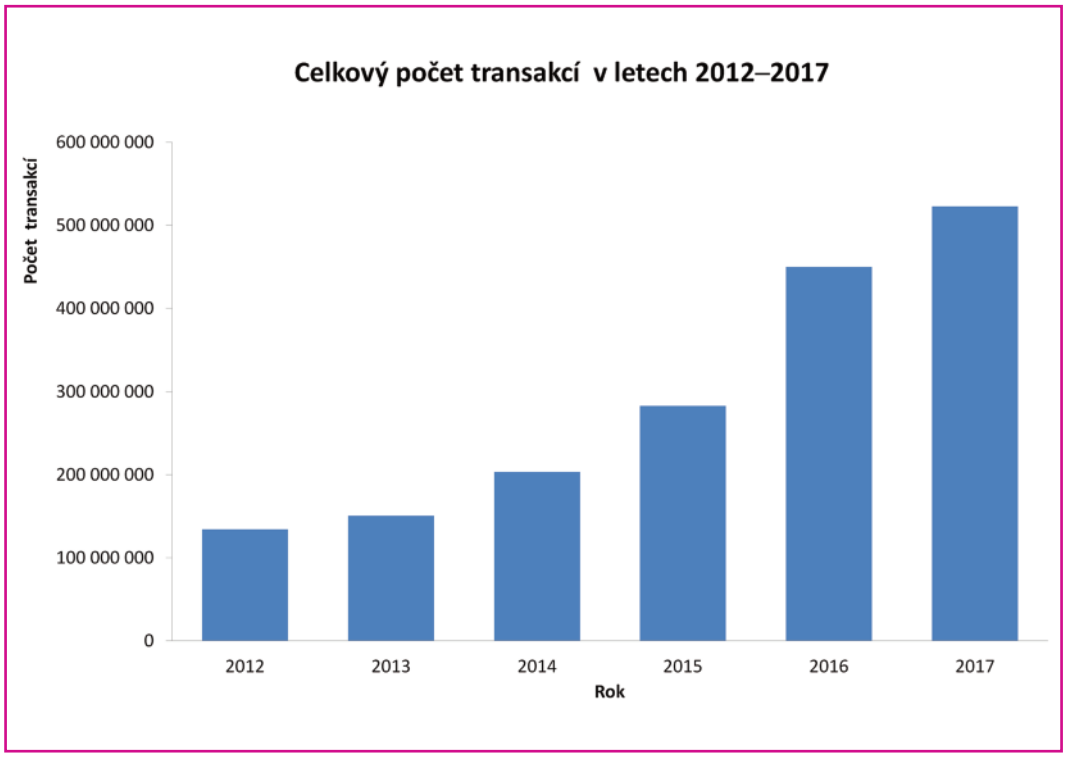
V systému je zaregistrováno 403 agend. Znamená to, že systém je využíván ve 403 oblastech, kde se s nimi obyvatel může každodenně setkat. Jsou zde obsaženy téměř všechny oblasti lidského zájmu. Od oblasti týkající se lidské tkáně a orgánů, autorského práva až po průběh služby vojáků v záloze.

Na rozdíl od předešlých let proběhl přechod z roku 2016 na rok 2017 plynule bez skokového nárůstu nebo poklesu počtu transakcí mezi měsíci prosincem a lednem.

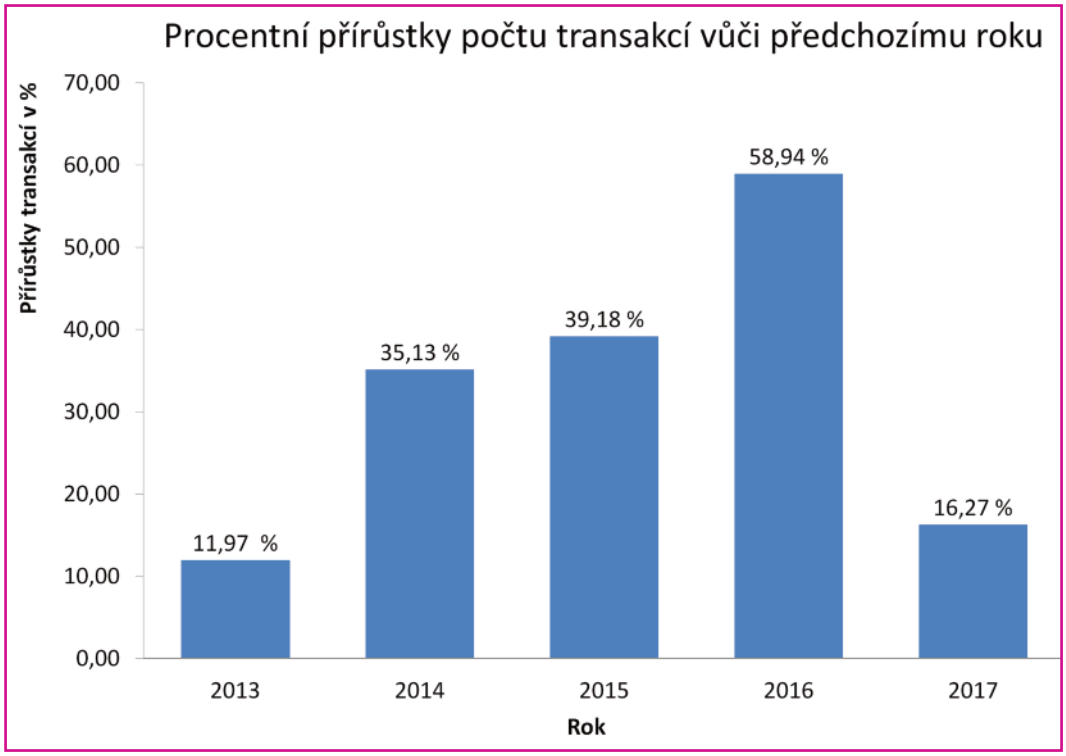
V grafu „Počet transakcí v měsících roku" je vidět skoro tradiční březnová špička, která je od roku 2016 mnohem patrnější než v letech 2013, 2014 a 2015.



Rozšiřování a využívání systému základních registrů je patrné z grafu „Celkový počet transakcí v letech 2012–2017". Nejvyšší roční přírůstek počtu transakcí byl v roce 2016, a to 166 779 679 transakcí.

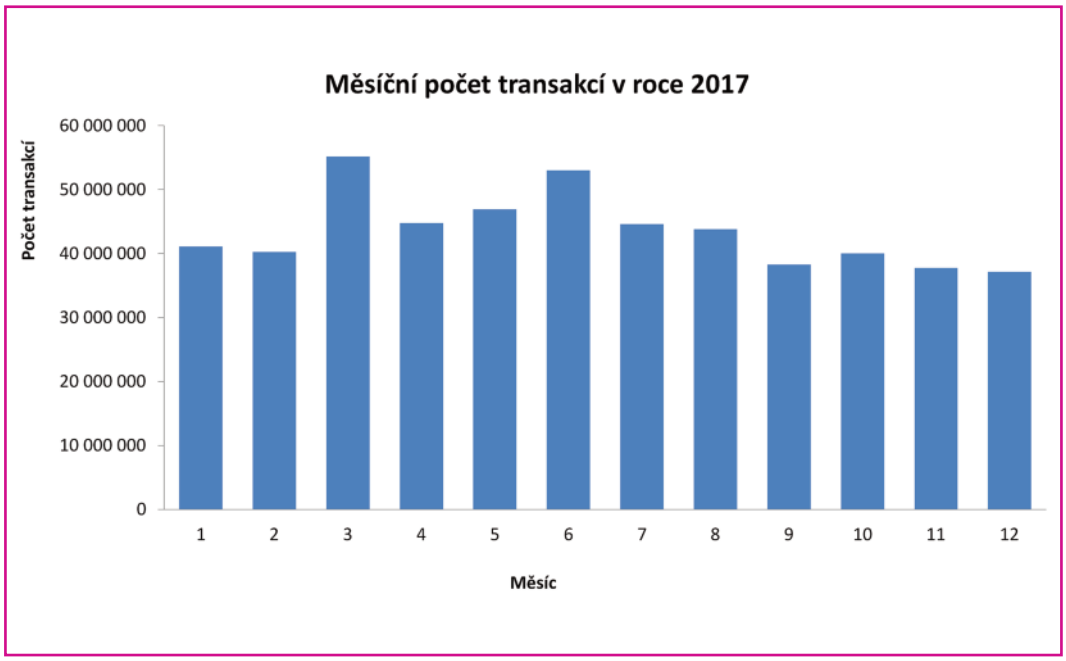


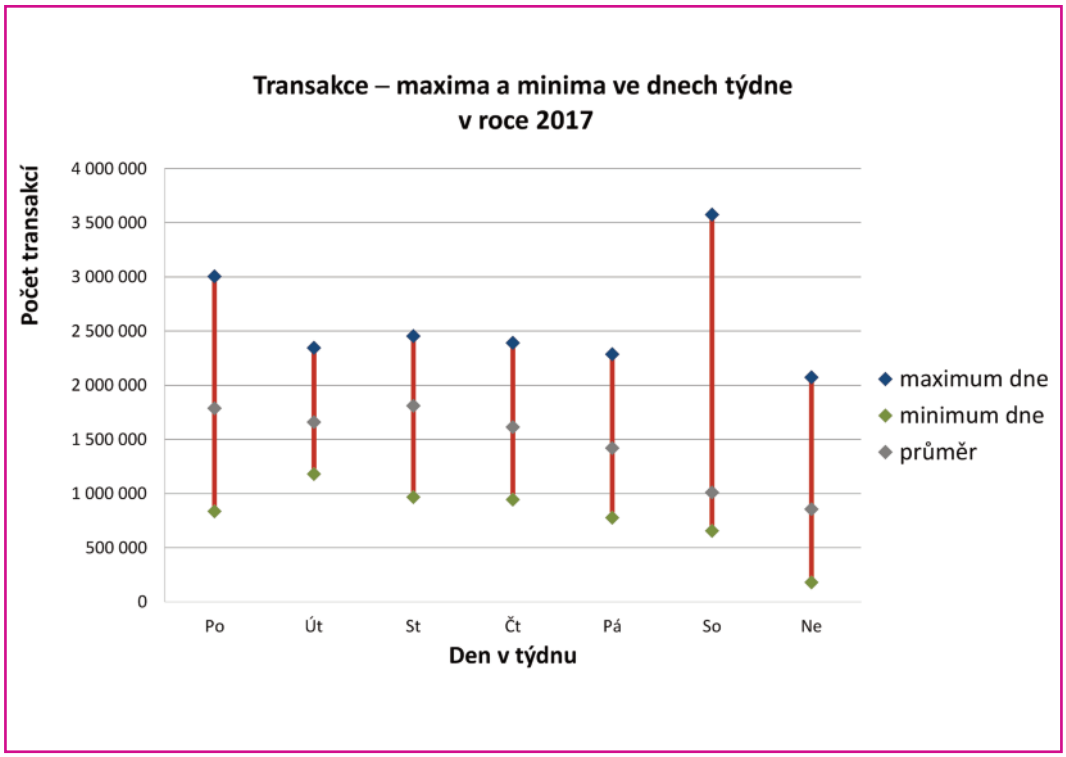
Zobrazení nárůstu počtu transakcí proti předchozímu roku v procentech je na grafu „Procentní přírůstky počtu transakcí".



Rozložení požadavků na systém základních registrů v průběhu roku je vidět na grafu „Měsíční počet transakcí v roce 2017". Maximální zatížení bylo 10. června 2017 s počtem transakcí 3 573 612. Minimální pak bylo 19. srpna 2017 s počtem transakcí 654 069.

Další graf ukazuje vytížení systému během týdne. Jsou zde uvedeny maximální a minimální hodnoty počtu transakcí v jednotlivých dnech. Je zde vidět, že maximální zatížení systému z 10. června 2017 bylo v sobotu. S největší pravděpodobností se týkalo údržby databází a celého systému.





Personální obsazení Úřadu

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

V roce 2017 činil celkový počet systemizovaných míst 109.

Fluktuace zaměstnanců se v roce 2017 v meziročním srovnání s předchozím rokem zvýšila z 9,8 procenta na 16,6 procenta.

Plynule pokračoval chod jednotlivých procesů personální správy Úřadu v návaznosti na vývoj zákona o státní službě a dalších relevantních změn legislativy.

Počátkem roku 2017 bylo provedeno služební hodnocení státních zaměstnanců zařazených k výkonu služby v Úřadu. Na základě těchto hodnocení bylo jeden 1 zaměstnanec jako dostačující. Žádný státní zaměstnanec nebyl hodnocen jako nevyhovující.

Do služebního poměru bylo nově přijato šest zaměstnanců a 11 zaměstnanců služební poměr ukončilo. Do pracovního poměru pak bylo přijato deset zaměstnanců, přičemž šest zaměstnanců ho ukončilo.

V rámci Úřadem zajišťované zvláštní části úřednické zkoušky pro obor služby „ochrana osobních údajů“ bylo vyzkoušeno sedm žadatelů, z nichž šest žadatelů ji složilo úspěšně.

K 1. lednu 2017 bylo v Úřadu v evidenčním stavu 99 zaměstnanců, k 31. prosinci 2017 byl pak jejich počet 100.

Průměrný evidenční přepočtený počet zaměstnanců za rok 2017 činil 98,5.

Dalších 34 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 je předpoklad úplného středoškolského vzdělání.

Úřad umožňuje a zabezpečuje odborný rozvoj svých zaměstnanců. Zajišťuje jim prohlubování odborné kvalifikace a v případě potřeby i její zvýšení. Rovněž Úřad umožňuje navštěvování jazykových kurzů. Tyto jazykové znalosti pak mohou zaměstnanci uplatnit při výkonu práce nebo služby. Studentům středních a vysokých škol poskytuje Úřad možnost absolvovat odbornou praxi. Tím podporuje jejich zájem o problematiku ochrany osobních údajů a zároveň tak vyhledává nové potenciální zaměstnance.

Členění zaměstnanců ÚOOÚ podle věku a pohlaví – stav k 31. prosinci 2017

Celý soubor	muži	ženy	celkem
do 20 let	0,00	0,00	0,00
od 21 do 30 let	6,00	4,00	10,00
od 31 do 40 let	5,00	12,00	17,00
od 41 do 50 let	7,00	11,00	18,00
od 51 do 60 let	13,00	20,00	33,00
61 a více	13,00	9,00	22,00
Celkem	**44,00**	**56,00**	**100,00**

Členění zaměstnanců ÚOOÚ podle vzdělání a pohlaví – stav k 31. prosinci 2017

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	2	4
L – Úplné střední odborné + VL	1	2	3
M – Úplné střední odborné	3	14	17
N – Vyšší odborné vzdělání	0	0	0
R – Bakalářské	0	1	1
T – Vysokoškolské	37	34	71
Celkem	**44**	**56**	**100**

Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 457/2016 Sb., o státním rozpočtu České republiky na rok 2017.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

	v tisících Kč
Souhrnné ukazatele	
Příjmy celkem	1 394,27
Výdaje celkem	153 794,88
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	1 394,27
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	0,00
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	1 394,27
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	153 794,88
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	56 666,97
Povinné pojistné placené zaměstnavatelem*)	19 092,86
Převod fondu kulturních a sociálních potřeb	1 106,64
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	11 029,90
Platy zaměstnanců na služebních místech podle zákona o státní službě	34 063,10
Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	10 089,05
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	13 736,90

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

1. Příjmy

Příjmy pro rok 2017 nebyly schváleným rozpočtem stanoveny.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů byl naplněn částkou 1 394,27 tisíc Kč.

Jednalo se především o:

- refundace zahraničních cest zaměstnanců Úřadu Evropskou komisí,
- sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti,
- sankce uložené podle zákona č. 101/2000 Sb., o ochraně osobních údajů a jiných zákonů,
- náhrady nákladů řízení,
- příjmy vztahující se k roku 2016 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2016).

2. Výdaje

Čerpání výdajů ve výši 153 794,88 tisíc Kč zahrnuje:

- veškeré náklady na platy a související výdaje,
- kapitálové výdaje, spojené s objektem Úřadu, obnovou informačních systémů, jak samotného ÚOOÚ, tak i IS ORG,
- 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 a údržby,
- výdaje související s neinvestičními nákupy.

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

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 76 866,48 tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. prosinci 2017 byl **100 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“ a programu 043V10 „Rozvoj a obnova materiálně technické základny Úřadu pro ochranu osobních údajů od r. 2017“ bylo celkem vyčerpáno **13 736,90 tisíc Kč**.

Přehled čerpání rozpočtu v roce 2017

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2017 v tis. Kč	Konečný rozpočet 2017 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2017 v tis. Kč	Skutečný konečný rozpočet v %
2211, 2212, 2324, 3113, 4132	Ostatní nedaňové příjmy	0,00	0,00	1 394,27	
	Příjmy celkem	**0,00**	**0,00**	**1 394,27**	
501	Platy	55 003,89	56 023,67	55 182,05	98,50
5011	Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	10 251,05	11 160,81	11 029,90	98,83
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	34 400,45	34 510,45	34 063,10	98,70
5014	Platy zaměst. odvozov. od platů úst. činitelů	10 352,40	10 352,40	10 089,05	97,46
502	Ostatní platby za provedenou práci	1 495,99	1 792,18	1 484,93	82,86
5021	Ostatní osobní výdaje	1 495,99	1 792,18	1 484,93	82,86
5024	Odstupné	0,00	0,00	0,00	0,00
503	Povin. pojist. plac. zaměstnavatelem	19 209,96	19, 657,39	19 092,86	97,13
5031	Povin. pojist. na sociál. zabezpečení	14 124,97	14, 453,96	13 997,85	96,84
5032	Povin. pojist. na veřej. zdrav. pojištění	5 084,99	5 203,43	5 095,02	97,92
513	Nákup materiálu	1 576,00	1 900,80	1 693,38	89,09
514	Úroky a ost. fin. výdaje	65,00	50,00	27,21	54,43
515	Nákup vody, paliv a energie	2 110,00	1 712,00	1 593,60	93,08
516	Nákup služeb	16 236,00	65 057,01	52 113,61	72,77
517	Ostatní nákupy	41 993,83	8 268,79	4 796,02	58,00
518	Poskyt. zálohy, jistiny, záruky a vládní úvěry	480,00	480,00	0,00	0,00
519	Výdaje souvis. s neinv. nákupy, příspěvky, náhrady a věcné dary	2 913,20	2 920,62	2 790,81	95,56

534	Převody vlastním fondům a ve vztahu k útv. bez plné práv. subjektivity	1 100,08	1 120,47	1 106,64	98,77
5342	Převody fondu kulturních a soc. potřeb a soc. fondů obcí a krajů	1 100,08	1 120,47	1 106,64	98,77
536	Ost. neinv. transf. jin. veřej. rozp. platby daní a další povinné platby	11,00	12,00	10,24	85,33
542	Náhrady plac. obyvatelstvu	90,00	170,00	166,63	98,02
5424	Náhrady v době nemoci	90,00	170,00	166,63	98,02
	Běžné výdaje celkem	**142 284,95**	**159 164,93**	**140 057,98**	**88,00**
611	Pořízení dlouh. nehmot. majetku	7 600,00	7 054,20	2 940,82	41,69
612	Pořízení dlouh. hmot. majetku	9 800,00	13 822,10	10 796,08	78,11
	Kapitálové výdaje celkem	**17 400,00**	**20 876,30**	**13 736,90**	**65,80**
	VÝDAJE CELKEM	**151 648,58**	**180 041,23**	**155 189,15**	**86,20**

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 12. 2017.

INTERNÍ AUDIT

Plán interního auditu ÚOOÚ na rok 2017 ukládal provedení tří auditorských šetření, v průběhu roku byly na základě oznamovacích dopisů a programů auditů provedeny následující audity:

01/17 Audit

Audit vykazování cest služebními auty

Cílem auditu bylo prověření a vyhodnocení nákladů na jednotlivá vozidla vlastněná Úřadem z hlediska 3E dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, spolu s prověřením a vyhodnocením procesního způsobu žádostí o přidělení služebního vozidla, jejich schvalování, užívání a zároveň v souladu s jinými evidencemi (cestovní příkazy, kniha jízd, záznamy z GPS). Dále pak prověření správnosti vykazování v knize jízd, počátečních a koncových stavů tachometrů, prověření ročních souhrnů a jednotlivých účetních dokladů, správnosti vykazování kilometrů v návaznosti na trasy vozidel, provedení kontroly dokladů o čerpání PHM v době provozu vozidel vzhledem k povoleným a schváleným trasám.

Ze šetření provedených v průběhu auditu vyplynulo, že procesní postupy uvedené ve směrnici o autoprovozu odpovídají skutečnostem vedeným v jednotlivých evidencích týkajících se služebních vozidel, všechny testované operace byly v souladu se směrnicí v oblasti žádosti o vozidlo, přidělení vozidla a jeho vrácení. Informace uvedené v jednotlivých knihách jízd odpovídaly informacím na cestovních příkazech osob, které vozidla využívaly.

V rámci dodržování kritérií 3E (hospodárnost, efektivnost a účelnost) nedošlo k pochybení při jednotlivých úkonech údržby vozidel.

Bylo konstatováno, že systém autoprovozu je nastaven a funguje správně a není třeba do něj zasahovat. Je však nutné přehodnotit celkovou účelnost provozování šesti vozidel pro potřeby Úřadu.

02/17 Audit

Audit uveřejňování smluv v registru smluv

Cílem auditu bylo prověřit a vyhodnotit procesní způsob uveřejňování smluv v registru smluv se zaměřením zejména na to, zda nedochází k systémovému pochybení při určování, které smlouvy budou v registru smluv uveřejněny. Dále pak prověřit, zda smlouvy určené k uveřejnění jsou uveřejňovány v souladu se zákonem, se zaměřením na uváděná metadata, formát přílohy a informace uváděné v uveřejňovaných smlouvách a také na prověření a vyhodnocení efektivnosti procesu uveřejňování v registru smluv z hlediska jeho návaznosti na další související procesy v ÚOOÚ a prověřit, zda nedochází k duplicitním či nadbytečným činnostem.

Audit zjistil, že uveřejňování v registru smluv bylo jako proces zavedeno při určování, které smlouvy budou v registru uveřejňovány, nedochází k systémovým či vědomým porušením zákona, při prověřování, zda jsou smlouvy uveřejňovány v souladu se zákonem, bylo konstatováno, že nebyla odhalena žádná systémová porušení zákona o registru smluv.

03/17 Audit

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. Dále pak prověřit a vyhodnotit způsobilost vnitřního kontrolního systému Úřadu včas zjišťovat, vyhodnocovat a minimalizovat provozní, finanční, právní a další rizika, vznikající v souvislosti s plněním schválených záměrů a cílů Úřadu (§ 25, odst. 1, písm. b) zákona o finanční kontrole). Součástí auditu bylo i ověřit plnění doporučení z dřívějších auditů a navrhnout doporučení k nápravě zjištěných nedostatků a k odstranění možných rizik v prostředí ÚOOÚ.

Audit byl ukončen konstatováním, že vnitřní předpisy Úřadu jsou z hlediska vnitřního kontrolního systému v souladu se zákonem o finanční kontrole i s ostatními obecně platnými právními předpisy a v praxi plní úlohu, kterou zákon o finanční kontrole stanoví a ukládá v oblasti účinnosti vnitřního kontrolního systému, 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.

Strategie auditorské činnosti ÚOOÚ je zaměřena především do oblasti ekonomické s cílem dosahování maximální hospodárnosti. Z dlouhodobého hlediska pak do oblasti rizik (v souladu se strategií MF ČR) s cílem jejich včasného podchycení a co nejrychlejší minimalizace.

Dále byly zpracovány:

- Roční plán činnosti interního auditu Úřadu na rok 2017
- Střednědobý plán činnosti interního auditu na roky 2017–2018
- Souhrnná zpráva o činnosti IA za rok 2016 pro předsedkyni Úřadu a
- Zpráva o výsledcích finančních kontrol za rok 2016 dle přílohy č.1a k vyhlášce č. 416/2004 Sb. pro MF ČR.

ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2017 a informace o jejím předání proběhne v řádném termínu do 31. července 2018 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 ÚOOÚ povinnost schvalovat účetní závěrku auditorem.

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

Úřadu bylo v roce 2017 adresováno celkem 30 žádostí o poskytnutí informací vztahujících se k jeho působnosti. V plném rozsahu byla informace poskytnuta ve 24 případech. Ve třech případech ÚOOÚ poskytnout informaci zcela odmítl a ve třech případech byla žádost o informace částečně odmítnuta. Důvodem odmítnutí či částečného odmítnutí byla ochrana osobních údajů osob, které byly obsaženy v požadovaných dokumentech, anebo skutečnost, že šlo o požadavek na informace, které nelze dle § 11 zákona č. 106/1999 Sb., o svobodném pří-stupu k informacím, poskytnout. Na postup Úřadu při odmítnutí či částečném odmítnutí poskytnutí informace nebyla registrována stížnost tazatelů. V jednom případě obdržel ÚOOÚ stížnost na formu poskytnuté informace, která byla vyřešena poskytnutím informace tazateli v požadované formě, tj. strojově čitelném formátu.

Tazatelé se v žádostech o informace zaměřovali především na rozhodovací a kontrolní činnost Úřadu, tj. na výsledky správních řízení (správní rozhodnutí) a výsledky kontrol (kontrolní protokoly). Dále ÚOOÚ zaznamenal mimo jiné dotaz týkající se jeho systematizace podle zákona č. 234/2012 Sb., o státní službě, či počtu provedených kontrol v minulých letech, a to včetně jednotlivých měsíců a rozčlenění na inspektory.

Poskytnuté informace byly zveřejňovány v souladu s § 5 odst. 3 zákona č. 106/1999 Sb.

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2017
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 2018 na svých webových stránkách.

Editor: Mgr. Tomáš Paták, telefon 234 665 286
Redakční zpracování: Mgr. Vojtěch Marcín
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 Munipress Brno, 2018

ISBN 978-80-210-8914-3