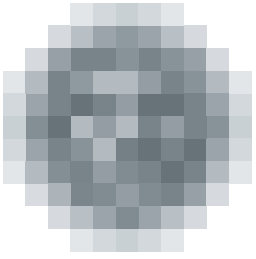
Výroční zpráva 2018



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-9224-2
ISBN 978-80-210-9225-9 (online: pdf)

Úvodní slovo předsedkyně

Dámy a pánové,

otvíráte výroční zprávu Úřadu pro ochranu osobních údajů za rok 2018, který pro nás všechny byl ve znamení obecného nařízení o ochraně osobních údajů, obecně označovaného GDPR. V propojeném globalizovaném světě se tento soubor pravidel pro zpracování osobních údajů stává globálním standardem. Přibližovat se mu začínají i významní hospodářští partneři Evropské unie – Spojené státy americké a Japonsko. Znamená to jediné – zásady a pravidla, které GDPR vyžaduje, odpovídají potřebám společnosti a jsou použitelné i v rozdílných právních řádech demokratických států. Na naplňování tohoto standardu se Úřad podílí nejen „domácí" činností, ale také tematicky poměrně pestrou účastí v rámci Evropského sboru pro ochranu osobních údajů a na ni navazující další spoluprací.

Náš příspěvek k naplňování potenciálu obecného nařízení je spojen také se zapojením do kontrol v mechanismu spolupráce dozorových úřadů členských zemí EU, který je jak pro subjekty údajů, tak pro správce, významný jediným kontaktním místem. Nám v něm připadla dvakrát úloha vedoucího dozorového úřadu.

Hodně sil věnujeme v posledních dvou letech konzultační a informační podpoře těch, jimž ze zpracování osobních údajů vznikají povinnosti – někdy to nejde jinak, než formou uvádění rad a tvrzení na pravou míru. V tom i v dozorové působnosti v užším slova smyslu byl fenoménem roku 2018 souhlas subjektu údajů se zpracováním. Tento institut svrchovaně naplňující ústavně zakotvené právo každého, jehož osobní údaje někdo jiný zpracovává, na ochranu před počínáním v rozporu se zákonem, je velmi často nepochopen nebo zneužíván. V posledním roce to je zejména v souvislosti s tzv. „přesouhlasováním," které, až na vzácné výjimky, bylo buď prostě nadbytečné či dokonce manipulativní a přispívalo k vytváření pokřiveného obrazu GDPR. Zde samozřejmě lidi dotčené takovým postupem v mezích své působnosti Úřad podporuje a pomáhá jim, kromě jednotlivých případů, především informační kampaní.

Příprava na nabytí účinnosti GDPR 25. května a očekávání vnitrostátní adaptační legislativy spojené s nepřetržitým zapojením, výrazně poznamenaly celý rok 2018 i obsah této výroční zprávy. Úkoly Úřadu však s obecným nařízením ani nezačínají, ani nekončí. Ochrana osobních údajů „dobíhá" podle zákona o ochraně osobních údajů, který ke dni, kdy píši tyto řádky, je stále ještě účinnou součástí právního řádu České republiky a v plném rozsahu platí pro oblasti, které nejsou pokryté GDPR.

Úřad také prosazuje ochranu osobních údajů podle dalších zákonů. Všechny formy dozorové působnosti – od konzultací a upozornění až po kontroly, správní řízení a ukládání pokut – se uplatňují v oblasti nevyžádaných, elektronicky šířených obchodních sdělení, která adresáti vnímají právem jako obtěžující. Za porušení zákona v této oblasti byla uložena polovina všech pokut za loňský rok.

Úřad rovněž provozuje významnou součást elektronicky vykonávaných agend veřejné správy v České republice, známou pod zkratkou ORG, která je pro občany doslova neviditelná, ale pro ochranu osobních dat v systému veřejné správy má klíčový význam. Systém ORG v rámci základních registrů významně přispívá k bezpečnosti a má strategický význam.

Ze zprávy, kterou máte před sebou, mimo jiné seznáte, že rok 2018 byl nepochybně přelomový pro ochranu soukromí v éře digitalizace, která je všudypřítomná a je trvalým ústředním bodem programového prohlášení vlády.

Věřím, že tato slova pro Vás obraz práce Úřadu pro ochranu osobních údajů v uplynulém roce zarámují.

JUDr. Ivana Janů
předsedkyně Úřadu pro ochranu osobních údajů

Obsah

Úřad v číslech 2018

Dotazy a konzultace	dotazů celkem	4161
	telefonní konzultační GDPR linka	2800
	telefonní konzultační linka ke kamerovým systémům	1900
	předchozí konzultace ve smyslu článku 36 GDPR	0
	ostatní konzultace	20
Podání a stížnosti	přijaté podněty	3616
	vyřízeno upozorněním správce na možné porušení	462
	předáno ke kontrole nebo jinému řízení	193
	postoupené věci od orgánů činných v trestním řízení a správních orgánů	57
	ohlášení o porušení zabezpečení osobních údajů ve smyslu článku 33 GDPR	260
	poskytnutí součinnosti orgánům činným v trestním řízení	10
Kontrolní činnost (s výjimkou kontrol týkajících se nevyžádaných obchodních sdělení)	zahájeno	76
	ukončeno	89
	z toho z předchozích let	36
	uložená opatření k nápravě	28
	napadeno námitkami	16
	námitkám vyhověno	2
	nevyhověno	11
	částečně vyhověno	3
	pokuty za neposkytnutí součinnosti v kontrole	4
	vyřízeno bez zahájení kontroly (odloženo, postoupeno)	27

Obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	2901
	zahájených kontrol	22
	ukončených kontrol	17
	z toho z předchozích let	6
	napadeno námitkami	5
	námitkám vyhověno	0
	nevyhověno	5
	částečně vyhověno	0
	řízení o sankci	26
	pokuty za neposkytnutí součinnosti v kontrole	10
	vyřízeno bez zahájení kontroly upozorněním subjektu na možné porušení povinností	414
Správní trestání (s výjimkou řízení týkajících se nevyžádaných obchodních sdělení)	řízení o sankci vedená s právnickými osobami a fyzickými osobami podnikajícími	39
	řízení o sankci s fyzickými osobami	17
	upuštění od uložení pokuty podle § 40a zákona č. 101/2000 Sb.	38
	odloženo	17
Rozhodování předsedkyně Úřadu	rozklady napadená rozhodnutí	25
	zamítnutých rozkladů	22
	zrušeno a vráceno k novému projednání	7
	zrušených rozhodnutí a zastaveno řízení	4
	změna rozhodnutí	3
Soudní přezkum (Pozn.: * *celkem od r. 2001*)	podaných žalob k soudu	8 (155)*
	zamítnutých žalob soudem	1
	zrušených rozhodnutí soudem	4
	ukončených/neukončených soudních řízení od roku 2001	133/22
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	3
	rozhodnutí o povolení předávání	1
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	2
Stížnosti podle § 175 správního řádu	přijatých stížností	12
	vyřízených jako důvodné	2
	vyřízených jako částečně důvodné	0
	vyřízených jako bezdůvodné	7

Žádosti podle zákona o svobodném přístupu k informacím	přijatých žádostí	56
	zcela vyhověno	45
	částečně odmítnuto	7
	odmítnutých žádostí	2
	požadavek na úhradu nákladů za mimořádné vyhledávání informací	2
	z toho uhrazených	0
Připomínkované návrhy	věcné záměry zákonů	8
	zákony	68
	prováděcí předpisy	85
	návrhy nařízení vlády	17
	návrhy vyhlášek	68
	nelegislativní dokumenty	63

Kontrolní činnost

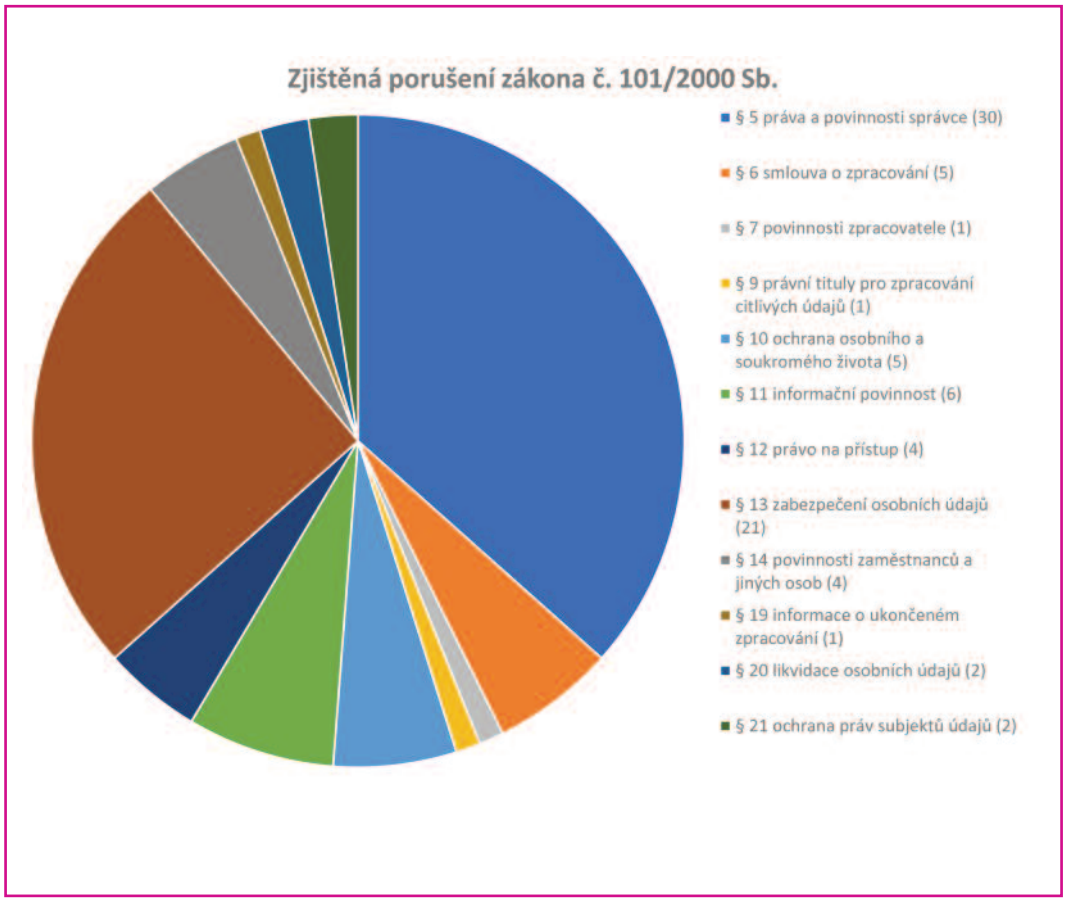
Kontrolní činnost Úřadu byla v roce 2018 zásadně dotčena účinností obecného nařízení[1] o ochraně osobních údajů. Pro praktický výkon kontroly tato skutečnost znamenala, že se jednotlivé kontroly v průběhu roku uskutečnily v různých režimech.

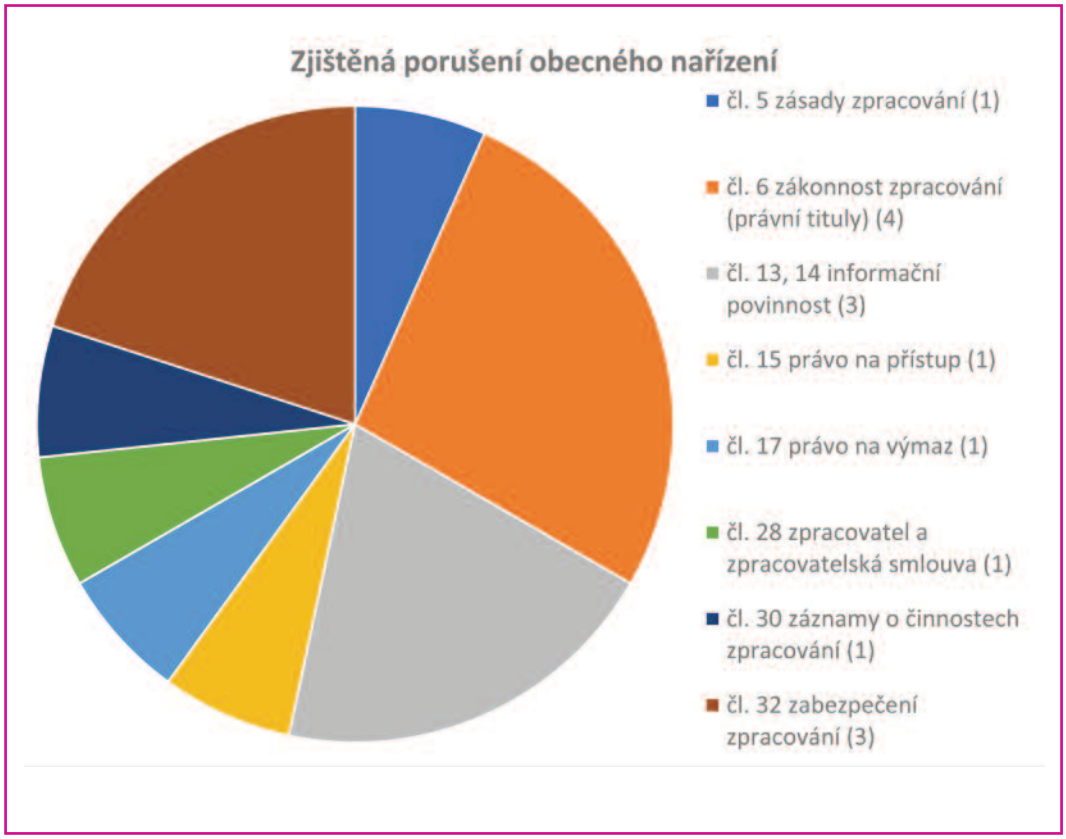
Jednalo se především o kontroly, které byly ukončeny před 25. květnem 2018, tedy před účinností obecného nařízení. V těchto kontrolách byly zjištěné skutečnosti posuzovány výlučně podle pravidel stanovených zákonem č. 101/2000 Sb.

Další významnou skupinu tvořily kontroly, které byly prováděny (třeba jen částečně) již za účinnosti obecného nařízení. V těchto případech bylo pro rozhodnutí o tom, podle kterého právního režimu bude posouzení provedeno, zásadní, kdy se uskutečnilo zpracování, které bylo předmětem kontroly. V případě, že bylo posuzováno zpracování prováděné před 25. květnem 2018, příp. incident, ke kterému došlo před tímto datem, byl posuzován primárně též soulad se zákonem č. 101/2000 Sb. Současně však byla zohledněna i příslušná ustanovení z obecného nařízení, kde kontrolující konstatovali, že ke stejným závěrům by dospěli i v případě, kdy by se již aplikovalo nařízení. V případě rozdílných závěrů pak uváděli konkrétní vysvětlení jejich odlišnosti. Poslední skupinu zmiňovaných kontrol pak tvořily ty, kde byl posuzován soulad pouze ve vztahu k obecnému nařízení.

Bližší přehled toho, jaká konkrétní porušení jednotlivých ustanovení Úřad v provedených kontrolách zjistil, poskytují tyto grafy:

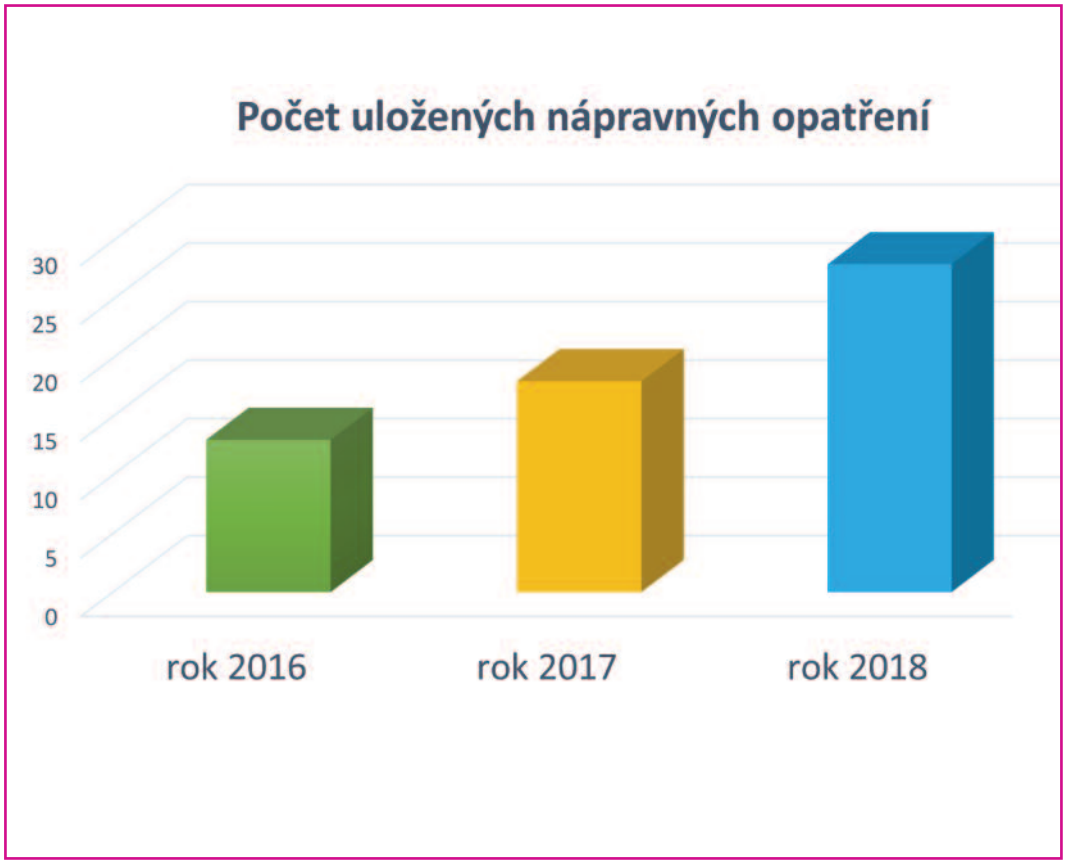
1 Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES).


Zjištěná porušení zákona č. 101/2000 Sb.
§ 5 práva a povinnosti správce (30)
§ 6 smlouva o zpracování (5)
§ 7 povinnosti zpracovatele (1)
§ 9 právní tituly pro zpracování citlivých údajů (1)
§ 10 ochrana osobního a soukromého života (5)
§ 11 informační povinnost (6)
§ 12 právo na přístup (4)
§ 13 zabezpečení osobních údajů (21)
§ 14 povinnosti zaměstnanců a jiných osob (4)
§ 19 informace o ukončeném zpracování (1)
§ 20 likvidace osobních údajů (2)
§ 21 ochrana práv subjektů údajů (2)


Zjištěná porušení obecného nařízení
čl. 5 zásady zpracování (1)
čl. 6 zákonnost zpracování (právní tituly) (4)
čl. 13, 14 informační povinnost (3)
čl. 15 právo na přístup (1)
čl. 17 právo na výmaz (1)
čl. 28 zpracovatel a zpracovatelská smlouva (1)
čl. 30 záznamy o činnostech zpracování (1)
čl. 32 zabezpečení zpracování (3)

Obecné nařízení s sebou přineslo mimo jiné zásadní důraz na spolupráci dozorových úřadů jednotlivých členských států, která má směřovat primárně k jednotnému posuzování prováděných zpracování. Součástí tohoto systému je i mechanismus jediného kontaktního místa („one-stop-shop mechanism“) pro případy přeshraničního zpracování osobních údajů. V rámci tohoto mechanismu je jeden dozorový úřad v roli vedoucího (úřad pro hlavní nebo jedinou provozovnu správce nebo zpracovatele) a ostatní úřady mohou být za určitých podmínek tzv. dotčenými dozorovými úřady (např. pokud jsou zpracováním podstatně dotčeny subjekty údajů s bydlištěm v členském státě tohoto úřadu). V rámci kontrol, které byly zahájeny v roce 2018, vystupoval Úřad v roli vedoucího dozorového úřadu ve dvou kontrolách. Jakmile budou tyto kontroly ukončeny, bude Úřad o jejich výsledku veřejnost informovat.

Jedním ze základních nástrojů, jehož cílem je (zpravidla na základě výsledků kontroly) dosáhnout nápravy stavu, který kontrola vyhodnotila jako porušení právních předpisů v oblasti ochrany osobních údajů, je uložení opatření k nápravě. Je třeba zdůraznit, že tato opatření se neukládají v případě, že příslušný správce či zpracovatel stav dobrovolně a včas napraví. V takovém případě by totiž řízení o uložení opatření nebylo hospodárné ani by nešetřilo práva dotčených osob. S ohledem na účinnost obecného nařízení je třeba uvést, že v ukládání opatření k nápravě nedošlo k žádným zásadnějším změnám oproti postupu podle zákona č. 101/2000 Sb. Další graf ukazuje vývoj počtu uložených opatření k nápravě za poslední tři roky (pozn.: v jednom rozhodnutí je zpravidla obsaženo více opatření k nápravě a graf ukazuje počet uložených opatření, nikoli vydaných rozhodnutí).



• KONTROLNÍ PLÁN

Kontrolní plán Úřadu byl v roce 2018 sestaven tak, aby reflektoval skutečnost, že ještě před ukončením prvního pololetí dojde k významné změně účinné právní úpravy. Zahájení jednotlivých kontrol podle kontrolního plánu tak nebylo určováno jednotlivými čtvrtletími, jak bylo do této doby obvyklé, ale právní úpravou, jejíž soulad měl být u konkrétních zpracování kontrolován.

Součástí kontrolního plánu pro rok 2018 byly dvě kontroly, které je Úřad povinen (na základě příslušných evropských právních předpisů) pravidelně provádět. Jednalo se o kontrolu zpracování osobních údajů v Celním informačním systému (CIS) a kontrolu zpracování osobních údajů ve vnitrostátní části Vízového informačního systému (VIS). Kontrola VIS, společně s již dříve provedenou kontrolou vnitrostátní součásti Schengenského informačního systému (SIS), je přitom zásadní i z toho hlediska, že v roce 2019 bude v České republice probíhat tzv. schengenské hodnocení, tedy kontrola fungování českého národního řešení SIS, a to včetně oblasti ochrany osobních údajů.

Dále byly předmětem kontrol prováděných na základě kontrolního plánu poznatky z předchozí dozorové činnosti Úřadu. Z tohoto důvodu (v návaznosti na kontrolu provedenou u společnosti SOLIDIS s.r.o. a následné řízení o sankci) proběhla například kontrola společnosti, která se zabývá obchodem s databázemi využívanými pro marketingové účely, resp. která zpracovává osobní údaje využívané pro marketingové účely. Taktéž v návaznosti na předchozí kontrolní činnost byla provedena kontrola u společnosti, která shromažďuje osobní údaje získávané finančními poradci, kteří s ní spolupracují. Předmětem kontroly bylo i zpracování osobních údajů u personální agentury, a to v návaznosti jednak na předchozí poznatky z kontrolní činnosti a dále s ohledem na zpřísnění podmínek činnosti těchto subjektů v důsledku změny zákona č. 435/2004 Sb., o zaměstnanosti. S ohledem na podnět Veřejné ochránkyně práv pak byla provedena kontrola u poskytovatele služeb tzv. hybridní pošty.

Některé kontroly byly do kontrolního plánu zařazeny v přímé souvislosti s účinností obecného nařízení.[2] To sice staví na shodných obecných zásadách ochrany osobních údajů, ale v jednotlivých detailech se přeci jen liší. Jednou z těchto drobnějších odlišností je skutečnost, že v obecném nařízení není výslovně jako právní důvod (titul) pro zpracování osobních údajů uvedeno, že lze zpracovávat bez souhlasu dotčených subjektů údajů oprávněně zveřejněné osobní údaje (viz § 5 odst. 2 písm. d) zákona č. 101/2000 Sb.). Takovým případem byla například kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků.

V září 2018 byl kontrolní plán doplněn převážně o kontroly zpracování systémů využívajících biometrické údaje (dynamický biometrický podpis, hlasová biometrie, technologie FaceID).

Více je možné se k některým případům, které byly předmětem kontroly na základě kontrolního plánu, dozvědět v následující části této výroční zprávy. Některé z kontrol, které byly zahájeny na základě kontrolního plánu pro rok 2018, nebyly v tomto kalendářním roce ukončeny. O jejich výsledcích bude Úřad informovat standardním způsobem na svých webových stránkách.

[2] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

• POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

Inspektorka Jana Rybínová

Únik osobních údajů z personálních spisů společnosti CHRIST CAR WASH s.r.o.

Úřad provedl kontrolu společnosti CHRIST CAR WASH s.r.o., se sídlem Koterovská 534/175, Koterov, 326 00 Plzeň (dále také „ChCW" nebo „kontrolovaná osoba").

Kontrola byla zahájena na základě podnětů, které obdržel Úřad v průběhu prosince 2017 od zaměstnanců ChCW a na základě postoupení spisů od Policie ČR v lednu 2018. Obsahem podnětů byla skutečnost, že došlo k úniku osobních údajů ze spisů zaměstnanců ChCW, resp. že zaměstnanci ChCW opakovaně obdrželi e-maily, jejichž přílohou byly kopie dokumentů z jejich personálních spisů. Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb., v souvislosti se zpracováváním osobních a citlivých údajů zaměstnanců, které společnost zpracovává v rámci pracovněprávních vztahů, a dále se zaměřením na plnění povinností správce osobních údajů ve smyslu § 13 zákona č. 101/2000 Sb.

Zákoník práce neuvádí žádnou definici, resp. výčet údajů, které má obsahovat personální spis. Rozsah z právních předpisů je tak možné dovodit. V souladu se zákoníkem práce může personální spis obsahovat jen písemnosti obsahující osobní údaje, které jsou nezbytné pro výkon práce v pracovněprávním vztahu, tedy jejichž rozsah je zároveň v souladu s ustanovením § 5 odst. 1 písm. d) zákona č. 101/2000 Sb.

Kontrolou bylo zjištěno, že kontrolovaná osoba v rámci personálních spisů uchovává kopie různých dokladů – např. kopie občanského průkazu, kopie rodného listu, kopie průkazu zdravotního pojištění, kopie evidenčního průkazu zdravotního pojištění, kopie výpisu z evidence rejstříku trestů fyzických osob, kopie karty klienta banky s číslem bankovního účtu.

V protokolu o kontrole bylo dále konstatováno, že není možné veškeré požadované informace dokládat kopiemi všech uvedených dokladů a tyto kopie uchovávat v personálních spisech. Povinností zaměstnance je doložit správnost určitých skutečností (např. výpis z evidence rejstříku trestů fyzických osob) tak, aby zaměstnavatel mohl splnit svou zákonnou povinnost. K tomuto však zaměstnavateli stačí do personálního spisu uvést, že požadované informace byly doloženy, a potvrdit, kdo, kdy a na základě jakých dokladů toto ověřil (dle dokladu, smlouvy, rodného listu apod.).

Dále bylo zjištěno, že kontrolovaná osoba uchovává kopie rodných listů dětí některých zaměstnanců, taktéž uchovává skenované fotografie zaměstnanců. Zároveň uchovává kopie občanských průkazů, a to v rozporu s povinností uloženou v § 15a odst. 2 zákona č. 328/1999 Sb., o občanských průkazech. I kdyby kontrolovaná osoba disponovala a doložila souhlas subjektu údajů s pořízením a uchováním kopie jeho občanského průkazu (naplnila by ustanovení § 15a odst. 2 zákona č. 328/1999 Sb.), je pořízení kopie občanského průkazu se souhlasem zaměstnance možné pouze za podmínky, že všechny osobní údaje, které jsou v občanském průkazu uvedeny, budou shromažďovány, a tedy i dále zpracovávány pouze v souladu s účelem, který si správce osobních údajů určil. Pokud nemá kontrolovaná osoba určený účel pro shromažďování dalších osobních údajů uvedených na občanském průkazu v rozsahu fotografie zaměstnance, případně jméno a příjmení manžela/ky, jeho rodné číslo, jména a příjmení dětí

a jejich rodná čísla, není oprávněna tyto osobní údaje shromažďovat. Podobná pravidla platí i pro účel zaměstnavatele týkající se uzavření pracovněprávního vztahu a k vedení personální evidence zaměstnance.

V protokolu o kontrole bylo uvedeno, že kontrolovaná osoba zpracovává ve své personální evidenci osobní údaje v rozporu s povinností uloženou jí jako správci osobních údajů v ustanovení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. Důvodem je shromažďování osobních údajů neodpovídajících pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu a současně v rozporu s povinností správce osobních údajů dle § 5 odst. 2 zákona č. 101/2000 Sb., neboť k danému zpracování osobních údajů nedisponuje žádným právním titulem pro jejich zpracování.

Nezjištěným způsobem navíc došlo k „úniku" osobních a citlivých údajů 62 zaměstnanců ChCW. Tyto byly zpětně neznámým odesílatelem přeposlány 28 zaměstnancům. Kontrolovaná osoba tedy nepřijala taková opatření, aby zabránila úniku osobních a citlivých údajů zaměstnanců z personálních složek, čímž porušila povinnost uloženou ji jako správci osobních údajů dle § 13 odst. 1 zákona č. 101/2000 Sb. Zároveň Úřad zjistil, že automatizované systémy, které kontrolovaná osoba využívá za účelem zpracování osobních a citlivých údajů v oblasti personalistiky, nejsou vybaveny systémem logování, tedy není možné určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. Proto kontrolovaná osoba nepořizovala elektronické záznamy přístupů (logování) k osobním údajům zpracovávaným v rámci personalistiky, a tedy neplní povinnosti uložené § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

Kontrolovaná osoba proti zjištěním uvedeným v protokolu o kontrole podala námitky. Vzhledem k tomu, že nebyla dodržena lhůta pro podání námitek, byly předsedkyní Úřadu zamítnuty z důvodu jejich opožděnosti.

Ve věci bylo s ChCW následně vedeno řízení o uložení opatření k odstranění zjištěných nedostatků a byla jí uložena pokuta ve výši 180 000 Kč.

Dodržování povinností správce ve společnosti Lidl Česká republika v.o.s.

Úřad provedl na základě kontrolního plánu pro rok 2018 komplexní kontrolu bez iniciačního podnětu ve společnosti Lidl Česká republika v.o.s., která v sobě zahrnovala kontroly v oblasti personalistiky, mzdové, zákaznických vztahů, dohledových systémů, kde nebylo možno předjímat, jaké konkrétní podmínky zpracování budou kontrolovanou osobou nastaveny. Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených v hlavě II zákona č. 101/2000 Sb. při zpracování osobních údajů zaměstnanců a zákazníků společnosti.

Kontrolovaná osoba v rámci kontroly předložila přehled všech databází. V těch zpracovává osobní údaje zákazníků a zaměstnanců spolu s uvedením účelů zpracování, prostředků a způsobů zpracování, včetně přehledu plnění všech podmínek vztahujících se k jednotlivým zpracováním. Za účelem detailnější kontroly vybrali kontrolující následující systémy: kamerový systém se záznamem; databáze elektronických vstupních karet a databáze škodních událostí zpracovávaných ve specializovaných softwarových aplikacích.

Kontrolou bylo zjištěno, že kontrolovaná osoba instalovala v některých svých objektech kamerový systém se záznamem, jehož prostřednictvím dochází ke zpracování osobních údajů zaměstnanců, zákazníků a dalších osob nacházejících se v prostorách monitorovaných tímto kamerovým systémem. Účelem provozu kamerového systému je ochrana života, zdraví a majetku zákazníků; ochrana života, zdraví a majetku zaměstnanců a ochrana majetku kontrolované osoby.

Dále bylo zjištěno, že doba uchování záznamů z kamerového systému je nastavena v souladu s ustanovením § 5 odst. 1 písm. e) zákona č. 101/2000 Sb., stanovená doba uchování odpovídá účelu zpracování; využívání kamerového systému je plně v souladu se stanoveným účelem; prostřednictvím kamerového systému nedochází, kromě minimalizovaného rozsahu, ke sledování činnosti zaměstnanců v průběhu výkonu jejich práce a nejsou sledovány prostory určené pro jejich „soukromé" aktivity, jako jsou šatny a odpočinkové místnosti.

Kontrolovaná osoba uzavřela smlouvy se zpracovateli osobních údajů v souladu s ustanovením § 6 zákona č. 101/2000 Sb., plní svoji informační povinnost vůči subjektům údajů ve smyslu § 11 odst. 1 zákona č. 101/2000 Sb. a akceptovala a v rámci kontroly dokumentovala přijatá technicko-organizační opatření pro zajištění ochrany zpracovávaných osobních údajů, a že veškeré operace s kamerovým systémem jsou logovány ve smyslu § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

V rámci kontroly zpracování osobních údajů zaměstnanců prostřednictvím elektronického vstupního systému bylo zjištěno, že je prováděno automatizovaně, údaje o elektronické vstupní kartě a přístupech zaměstnance do prostor kontrolované osoby jsou vedeny v samostatné databázi, databáze sama o sobě nezaznamenává přístupy. Přístupy do databáze jsou zaznamenávány v rámci vzdáleného serveru umístěného na centrále kontrolované osoby, jehož prostřednictvím je do databáze přistupováno. Doba uchování je nastavena v souladu s ustanovením § 5 odst. 1 písm. e) zákona č. 101/2000 Sb. a odpovídá účelu zpracování. Kontrolovaná osoba vede databázi elektronických vstupních karet sama na svém serveru a sama také provádí její administraci. Z tohoto důvodu nemá uzavřenu žádnou smlouvu o zpracování osobních údajů s třetí osobou.

Kontrolou bylo konstatováno, že kontrolovaná osoba přijala dostatečná technicko-organizační opatření pro zajištění ochrany osobních údajů zpracovávaných v rámci uvedeného systému; přístupy do systému jsou logovány v souladu s ustanovením § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

Za účelem evidence a vyřízení jednotlivých škodních událostí vede kontrolovaná osoba jejich databázi obsahující vedle údajů k jednotlivým událostem, jako jsou výše škody, škodní průběh apod., také osobní údaje zákazníků jako škůdců či poškozených. Doba uchování osobních údajů je kontrolovanou osobou stanovena v souladu s ustanovením § 5 odst. 1 písm. e) zákona č. 101/2000 Sb., stanovená doba uchování odpovídá účelu zpracování.

Kontrolovaná osoba zásadně nepředává osobní údaje vedené za účelem evidence a vyřízení škodní události třetím osobám, výjimku představuje předání celé škodní události k posouzení specializovanému pojišťovacímu makléři, se kterým kontrolovaná osoba uzavřela zpracovatelskou smlouvu v souladu s ustanovením § 6 zákona č. 101/2000 Sb.

Kontrolovaná osoba přijala a dokumentovala dostatečná technicko-organizační opatření pro zajištění ochrany osobních údajů zpracovávaných v rámci uvedené evidence. Úřad nezjistil porušení povinnosti kontrolované osoby uložené jí jako správci osobních údajů v § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

Inspektor František Bartoš

Internet Mall, a.s. – zaznamenání narušení bezpečnosti při správě osobních údajů

Úřad obdržel od společnosti Internet Mall, a.s. (dále jen „Internet Mall") písemnou informaci Oznámení o narušení bezpečnosti při správě osobních údajů. Obsahem sdělení byla informace, že společnost, která v rámci svého předmětu podnikání provozuje internetovou nákupní galerii MALL.CZ, oznamuje, že dne 25. srpna 2017 zaznamenala narušení bezpečnosti při správě osobních údajů.

V blíže neupřesněné době od 31. prosince 2014 do 23. července 2017 neznámá osoba nebo neznámé osoby odcizily ze serverů společnosti Internet Mall elektronickou databázi uživatelských účtů jejích klientů. Databáze obsahovala osobní údaje klientů v rozsahu e-mailový kontakt, přístupové heslo (v šifrované podobě), jméno, příjmení a telefonní kontakt. Dle sdělení bylo celkem odcizeno 766 421 elektronických záznamů, z nichž 735 956 obsahovalo unikátní e-mailové adresy. Celkem bylo odcizeno cca 20 procent záznamů z celkové zákaznické databáze a zhruba 350 tisíc záznamů bylo aktivních i v roce 2017, kdy bylo odcizení odhaleno.

Kontrolou bylo zjištěno, že společnost Internet Mall byla na zpřístupnění její databáze klientů (uživatelských účtů) upozorněna fyzickou osobou, prostřednictvím elektronické zprávy. Šetřením a porovnáním zpřístupněných údajů byla zveřejněná databáze ztotožněna s databází vlastních klientů z roku 2014 (internetové servery provozované v roce 2014 společností Internet Mall: www.mall.cz, www.korunka.cz, www.azelektro.cz a hfishop.cz).

Společnost následně po obdržení informace požádala provozovatele webového portálu www.ulozto.cz, firmu Uloz.to Cloud, a.s., o odstranění zpřístupněné databáze. Téhož dne společnost Uloz.to Cloud, a.s., zajistila smazání výše uvedené databáze. Následně společnost Internet Mall rozeslala svým zákazníkům prostřednictvím e-mailu informaci o možnosti úniku jejich osobních údajů s doporučením na změnu svých přístupových jmen a hesel.

Dále bylo kontrolou konstatováno odcizení databáze 766 421 záznamů o zákaznících společnosti Internet Mall, ke kterému došlo v období od 31. prosince 2014 do 23. července 2017 neznámým pachatelem či pachateli. Databáze obsahovala 735 956 unikátních adres zákazníků v rozsahu jméno, příjmení, uživatelské heslo, e-mailová adresa a číslo telefonu, které měla uloženy v ICT systémech. Společnost Internet Mall přitom jako správce osobních údajů neoprávněnému přístupu a odcizení databáze uživatelů nejen nezabránila, ale ani jej nezaznamenala a nezjistila. Porušila tak povinnost správce osobních údajů uloženou jí § 13 odst. 1 zákona č. 101/2000 Sb., neboť jako správce nepřijala taková opatření, aby nedošlo k neoprávněnému odcizení výše uvedené databáze záznamů vlastních zákazníků. Následkem porušení této povinnosti bylo zveřejnění databáze 766 421 záznamů o zákaznících společnosti Internet Mall obsahujících 735 956 unikátních adres zákazníků v rozsahu jméno, příjmení, uživatelské heslo, e-mailová adresa a číslo telefonu na veřejně přístupném webovém portálu www.ulozto.cz po dobu od 27. července 2017 do 25. srpna 2017.

Současně nebylo možné zjistit, kolika osobám byla databáze odcizených osobních údajů zpřístupněna, kdo ji v současné době má v držení a kolik kopií bylo pořízeno. V následném správním řízení byla společnosti uložena pokuta ve výši 1,5 mil. Kč.

INTER – IVCO, s.r.o. – dodržování povinností správce osobních údajů

Na základě stížností a plánu kontrol provedl Úřad kontrolu ve společnosti INTER – IVCO, s.r.o. (dále také „kontrolovaná osoba") ve věci dodržování povinností správce osobních údajů

stanovených zákonem č. 101/2000 Sb. při zpracování osobních údajů subjektů údajů v registru dlužníků umístěného na webových stránkách www.rejstrikdluhu.cz, se zaměřením na právní titul zpracování osobních údajů, včetně jejich zpřístupňování a zveřejňování.

Kontrolou bylo zjištěno, že kontrolovaná osoba na webových stránkách www.rejstrikdluhu.cz zpracovávala nepravdivé údaje. Ty se týkaly osoby stěžovatele, který se o tom, že je dlužníkem vysoké částky, dozvěděl prostřednictvím své partnerky, která byla na tuto skutečnost upozorněna anonymním e-mailem. Kontrolou bylo zjištěno, že pro zadávání, uchovávání a ani pro opravy nepravdivých zápisů nemá kontrolovaná osoba přijata žádná pravidla. Bylo zjištěno, že jakoukoli informaci o nesplaceném dluhu nebo pohledávce může oproti úhradě finančního poplatku a potvrzení souhlasu se všeobecnými obchodními podmínkami učinit kdokoli. Takový provozovatel však neověřuje zadané informace ani totožnost pisatele příspěvku. Rovněž tak žádným způsobem neověřuje totožnost osob, které se na něj obrátily s žádostí o výmaz nepravdivého příspěvku. Kontrola například ukázala, že pouze na základě telefonického rozhovoru provozovatel stránek změnil obsah zveřejněné informace. I za tuto službu požadoval úhradu poplatku.

V průběhu místního šetření v době kontroly bylo zjištěno, že je na webových stránkách www.rejstrikdluhu.cz celkem 779 položek od 431 zadavatelů. Tento soubor obsahoval osobní údaje o větším počtu fyzických osob, právnických osobách a podnikajících fyzických osobách.

Bylo konstatováno, že v případě osobních údajů stěžovatele byly na webových stránkách www.rejstrikdluhu.cz vedeny jeho osobní údaje v rozsahu jméno, příjmení a jeho adresa a informace o údajné výši dluhu a fiktivního věřitele, a to minimálně po dobu devíti měsíců, aniž by o tom stěžovatel obdržel jakoukoli informaci. Nepravdivý záznam smazal provozovatel na základě telefonické stížnosti stěžovatele.

Zpracování a zveřejňování osobních údajů tzv. dlužníků v registru www.rejstrikdluhu.cz kontrolující vyhodnotili jako nepřípustné zasahování do soukromého a osobního života dotčených osob. Zpřístupněním osobních údajů v registru dlužníku, který byl získán na základě soukromoprávního vztahu, bez souhlasu a vědomí dlužníka, totiž docházelo k poškození dobrého jména jednotlivců, kteří byli do registru dlužníků zapsáni omylem nebo v některých případech na základě úmyslu poškodit jinou osobu. Vzhledem k tomu, že společnost neověřovala podklady, na základě kterých byla fyzická osoba do registru dlužníků www.rejstrikdluhu.cz zapsána, může docházet k újmě na jejích právech v mnoha dalších vztazích, jak soukromoprávních, tak i veřejnoprávních. Zpřístupnit osobní údaje bez souhlasu dlužníka lze pouze oprávněným osobám (např. Policie ČR). Správce osobních údajů může údaje zveřejnit nebo zpřístupnit pouze se souhlasem dlužníka.

Kontrolou bylo zjištěno, že kontrolovaná osoba byla správcem osobních údajů a za zpracování, zveřejnění a získání souhlasu se zpracováním osobních údajů fyzických osob v rejstříku dlužníků www.rejstrikdluhu.cz plně odpovídá ve smyslu povinností správce osobních údajů, stanovených mu v zákoně č. 101/2000 Sb. Tuto odpovědnost kontrolované osoby nelze v žádném případě přenést na věřitele. Podle § 5 odst. 4) zákona č. 101/2000 Sb. musí být správce osobních údajů schopen prokázat souhlas se zpracováním osobních údajů po celou dobu jejich zpracování, což kontrolovaná osoba nemohla učinit.

Kontrolovaná osoba nedisponovala souhlasem stěžovatele ani žádným jiným souhlasem ostatních osob se zpracováním jeho osobních údajů v registru dlužníků zveřejněném na webových stránkách www.rejstrikdluhu.cz, ani jiným právním titulem pro zpracování osobních údajů ve smyslu § 5 odst. 2 písm. a) – g) zákona č. 101/2000 Sb.

Kontrolovaná osoba zpracovávala osobní údaje 477 subjektů údajů na svých webových stránkách formou tzv. nabídky pohledávek, aniž by disponovala souhlasem jednotlivých subjektů údajů nebo jiným právním titulem pro jejich zpřístupňování. Kontrolovaná osoba zpracovávala osobní údaje v rozporu s ustanovením § 5 odst. 2 zákona č. 101/2000 Sb.

Kontrolou bylo konstatováno, že kontrolovaná osoba v souvislosti se zpracováním osobních údajů stěžovatele a jejich zveřejněním v registru dlužníků www.rejstrikdluhu.cz bez jeho souhlasu porušila ustanovení § 5 odst. 2 zákona č. 101/2000 Sb.

V návazném správním řízení byla uložena pokuta ve výši 90 000 Kč. Vzhledem k tomu, že v průběhu kontroly kontrolovaná osoba ukončila provoz webových stránek www.rejstrikdluhu.cz, nebylo nutné přistoupit k řízení o uložení opatření k nápravě.

Inspektor Daniel Rovan

Kontrola mobilního operátora týkající se vyžadování souhlasu

Úřad na základě stížností provedl a ukončil kontrolu mobilního operátora. Stěžovatelé shodně uváděli, že prostředí elektronické aplikace je podle nich nastaveno tak, že přístup klienta k nasmlouvaným službám společnosti je podmíněn udělením jeho souhlasu se zpracováváním osobních údajů zákazníků služeb operátora pro obchodní účely. Tento souhlas nemusí klient udělit ihned, ale v blíže neurčené budoucnosti. Stěžovatelé uváděli, že je přesvědčivě vzbuzován dojem, že souhlas musí tak či tak udělit; oproti tomu volba odmítnutí souhlasu se zpracováním osobních údajů pro obchodní účely v prostředí aplikace chyběla. Druhým typem stížnosti bylo upozornění stěžovatele na zpracování (předávání) jeho osobních údajů v rámci zpracování Telcoscore. Vzhledem k tomu, že kontrola byla zahájena po nabytí účinnosti obecného nařízení,[3] byly prověřovány a hodnoceny články nařízení čl. 4 (vymezení pojmů), čl. 5 (povinnosti), čl. 6 (zákonnost), čl. 7 (souhlas) a čl. 28 (zpracovatelé).

Věcně se kontrola týkala dvou okruhů, a to jednak souhlasů a možnosti jejich odvolání a jednak předávání osobních údajů v rámci služby Telcoscore. Z kontrolních zjištění vyplynulo, že kontrolovaná osoba připravila a svým klientům předložila k podpisu nový formulář souhlasu[3] Starý souhlas platil do 24. května 2018, nový pak od 25. května 2018. Vzhledem k velkému množství klientů začala kontrolovaná osoba „nabírat" nové souhlasy již od února 2018. Vznikla tedy situace, kdy někteří klienti měli podepsané dva souhlasy. To bylo pro ně matoucí, a proto se rozhodli jeden ze souhlasů odvolat. Pokud se jednalo o „nový" souhlas, obdrželi informaci, že jej lze odvolat až s účinností obecného nařízení, tedy po 25. květnu 2018. Kontrolující tento výklad vyhodnotili jako chybný s tím, že souhlas má subjekt údajů právo odvolat kdykoli.

Při kontrole zpracování (předávání) osobních údajů v rámci služby Telcoscore bylo prověřeno a kontrolovanou osobou doloženo, že scoring je prováděn ze strany kontrolované osoby ve dvojím právním režimu, a to:

- na základě souhlasu subjektu údajů pro účely služby Telcoscore, která je poskytována prostřednictvím jiné společnosti dle smluvních ujednání zúčastněných stran. Tato služba u některých poskytovatelů finančních produktů nahrazuje u klientů bez finanční historie (mladí,

[3] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

zejména studenti) hodnocení bonity klienta vzhledem k jeho věku. Služba je poskytována v zájmu žadatele a vždy s jeho písemným souhlasem,

- na základě oprávněného zájmu kontrolovaného, spočívajícího ve vyhodnocování chování zákazníka při využívání jeho služeb (telcoscoring), včetně platební morálky zákazníka, a to pro potřeby kontrolovaného při rozhodování o nabídkách svým zákazníkům. Zde se jednalo o interní záležitost kontrolovaného a nedocházelo k žádnému předávání osobních údajů třetím osobám.

Kontrola neprokázala, že by kontrolovaná osoba výsledky telcoscoringu předávala třetím stranám. V této části kontroly Úřad nezjistil porušení obecného nařízení.

Prověřování dostatečnosti zabezpečení osobních údajů u Generálního finančního ředitelství (EET)

Úřad na základě kontrolního plánu pro rok 2017 provedl a ukončil kontrolu Generálního finančního ředitelství v souvislosti se zpracováním osobních údajů Finanční správou České republiky (dále také „kontrolovaná osoba") se zaměřením na zpracování údajů podle zákona č. 112/2016 Sb., o evidenci tržeb v rámci EET. Současně obdržel Úřad podnět s podezřením na nedostatečné zabezpečení osobních údajů, který v průběhu kontroly prověřil. Správce daně zveřejňuje způsobem umožňujícím dálkový přístup podmínky a postup pro přístup na společné technické zařízení správce daně umožňující poplatníkovi správu certifikátu pro evidenci tržeb a údajů pro správu evidence tržeb. Komunikace probíhá přes daňový portál, viz http://adisspr.mfcr.cz/adist/idpr_pub/dpr/uvod.faces. Daňový portál obecně slouží pro komunikaci s Finanční správou České republiky a k získávání informací v rámci správy daní, přičemž provozovatelem daňového portálu je Generální finanční ředitelství.

Kontrolovaná osoba provozuje automatizovaný daňový informační systém. V analytickém prostoru, který není v pravém slova smyslu aplikací, jsou data uložena na databázovém serveru. Automatizovaný daňový informační systém byl určen jako IS kritické informační infrastruktury podle zákona č. 181/ 2014 Sb., o kybernetické bezpečnosti, a navazující vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Požadavky výše zmiňovaných dokumentů hovoří o bezpečnostních opatřeních. Mezi ně patří i technická opatření, mimo jiné i opatření uživatelského rozhraní informačního systému a jeho bezprostředního systémového okolí (operační systémy, databáze, webové služby).

Vzhledem k tomu, že kontrola proběhla ještě před účinností obecného nařízení, byly prověřovány povinnosti správce dle zákona č. 101/2000 Sb., konkrétně ty vyplývající z § 5 odst.1 písm. b), d), e), § 5 odst. 2, § 6 a § 13. Z kontrolních zjištění vyplynulo, že je působnost podle zákona o evidenci tržeb vykonávána orgány Finanční správy České republiky, tedy Generálním finančním ředitelstvím. Automatizovaný daňový informační systém, který data zpracovává, byl určen jako informační systém kritické informační infrastruktury podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a navazující vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Tato skutečnost automaticky nastavuje standardy jeho zabezpečení. Kontrola prověřila jejich dodržování.

Provedena byla fyzická kontrola datového úložiště a aplikační serverovny v datovém centru, jehož služby kontrolovaný využívá. Dále se kontrolující zaměřili také na fyzickou kontrolu jednoho

z IT pracovišť kontrolované osoby zaměřeného na správu informačního systému, a to Odboru daňových informačních systémů, a dále kontrolu pracoviště využívajícího informační systém ke své činnosti, a to Finančního úřadu pro hlavní město Prahu. Na všech pracovištích bylo prověřeno, že pracovníci kontrolované osoby jsou proškoleni a poučeni o bezpečnostních opatřeních, že znají své povinnosti a dodržují je. Dále bylo ověřeno zabezpečení přístupů do chráněných pracovišť a to, že vstup do prostředí odpovídá dokumentaci předložené kontrolovaným.

Stížnost se týkala toho, že kontrolovaná osoba implementovala komerční produkt reCAPTCHA společnosti Google Inc. v souvislosti se zpracováním aplikací elektronické evidence tržeb (EET) do finanční správou provozovaného automatizovaného daňového informačního systému. Z kontrolních zjištění vyplynulo, že tento produkt byl do systému zařazen jen jako doplňkový. Kontrolovaná osoba navíc tento komerční produkt nahradila v průběhu kontroly vlastním řešením. Kontrola nezjistila porušení zákona č. 101/2000 Sb.

Inspektor Josef Vacula

Zpracování osobních údajů v systému CERD na www.centralniregistrdluzniku.cz a www.cerd.cz (překlápění veřejných rejstříků, zveřejňování nepravdivých informací, zásah do soukromého života a neinformování subjektů údajů)

Úřad zahájil 31. března 2016 kontrolu u společnosti CSR & Protikorupcnilinka.cz s.r.o., a to v návaznosti na velké množství obdržených stížností. Stěžovatelé obecně zjišťovali, že jejich osobní údaje jsou na výše uvedených internetových stránkách zveřejňovány, přičemž jsou k těmto jejich osobním údajům přiřazovány nepravdivé informace např. o tom, že jsou dlužníci či že je s nimi stále vedeno insolvenční řízení. Počet těchto stěžovatelů se pohyboval v řádu několika desítek.

V rámci shromažďování podkladů pro kontrolní řízení Úřad pracoval s otevřenými zdroji, především s obchodními rejstříky. Jednalo se o český obchodní rejstřík a obchodní rejstřík některých amerických států. Kontrolou bylo zjištěno, že na zpracování osobních údajů v rámci systému CERD se podílejí rovněž zahraniční společnosti (např.: CERD SYSTEM LLC, CENTRAL REGISTER OF DEBTORS INC. či CERD LLC, REGISTRY LLC). Dále pracoval Úřad s veřejně dostupnými informacemi o registrátorech doménových jmen.

Na základě důkladné analýzy informací získaných z těchto zdrojů bylo kontrolou zjištěno, že osobou, která všechny společnosti zúčastněné na zpracování osobních údajů na shora uvedených internetových stránkách zakládala a ovládá, je fyzická osoba. Ukázalo se, že tato osoba vytvořila spletitou strukturu českých a zahraničních právnických osob, které měly zakrýt pravého správce osobních údajů, tedy tuto fyzickou osobu. Ta navíc na shora uvedených internetových stránkách uváděla nepravdivé informace, např. že jím vydávané potvrzení o bezdlužnosti je zcela validní a všeobecně přijímané či že s tímto registrem dlužníků spolupracují státní orgány.

Po pečlivém vyhodnocení získaných informací Úřad koncipoval závěry své kontrolní činnosti tak, že shora uvedená společnost CSR & Protikorupcnilinka.cz s.r.o. je v postavení zpracovatele osobních údajů ve smyslu § 4 písm. k) zákona č. 101/2000 Sb., zatímco správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., a tedy odpovědným subjektem za veškerou činnost související se zpracováním osobních údajů, je fyzická osoba. Dále Úřad v této kontrole konstatoval několik závažných porušení zákona č. 101/2000 Sb. Namátkou je možné vybrat porušení ustanovení § 5 odst. 2 návětí zákona č. 101/2000 Sb., neboť na internetových stránkách bylo možné bez jakékoli kontroly či ověření uvádět konkrétní fyzické osoby a uvést je jako

dlužníky, včetně případné dlužné částky, aniž by tito lidé skutečně dlužníky byli či alespoň věděli, že je o nich v tomto kontextu někde veden záznam. Dále bylo kontrolou konstatováno porušení ustanovení § 11 cit. zákona, kdy správce osobních údajů nedostatečně či nepravdivě informuje subjekty údajů o zpracování jejich osobních údajů, či ustanovení § 10 cit. zákona, kdy bylo kontrolou zjištěno, že správce osobních údajů svou činností hrubým způsobem zasahoval do soukromého života subjektů údajů, neboť nejenže inicioval a umožňoval nepravdivé zveřejňování o dlužnících (viz výše), ale také překlápěl oficiální insolvenční rejstřík vedený a spravovaný Ministerstvem spravedlnosti ČR a takto získaný obsah však dále neaktualizoval, čímž na svých internetových stránkách uváděl nepřesné (nepravdivé) informace o subjektech údajů. Takové informace pak měly vliv také na jejich osobní život, zvlášť v případě, kdy se jednalo o fyzické osoby podnikající. Tehdy takováto informace měla vliv i na výkon jejich činnosti.

Je třeba zdůraznit, že kontrolující se po celou dobu vedení řízení potýkali nejen s velmi náročnou komunikací s oficiálními zahraničními místy, ale rovněž se součinností hraničící s obstrukcemi ze strany kontrolované osoby, a především pak s osobními útoky včetně urážek a napadání od fyzické osoby na jednotlivé členy kontrolního týmu. Přes všechny tyto obtíže se podařilo 30. července 2018 kontrolní řízení ukončit. Kontrolované osobě bylo doručeno rozhodnutí předsedkyně Úřadu o podaných námitkách, které byly tímto rozhodnutím zamítnuty v celém rozsahu.

Důležitost kontrolního řízení a nebezpečnou povahu činnosti fyzické osoby podtrhuje též skutečnost, že stížnosti na shora uvedené internetové stránky obdržela i Evropská komise. Ta požádala Úřad, jakožto orgán, který dokázal tuto problematiku vyřešit, o příspěvek na konferenci k ochraně spotřebitele a ochraně dat, jakým způsobem byla tato celoevropská kauza vyřešena.

Eltodo, a. s., – kontrola kamerového systému na vozidlech monitorujících zónové parkování

Kontrolu u výše zmíněné společnosti zahájil Úřad na základě kontrolního plánu pro rok 2018, kdy reagoval na větší množství dotazů směřujících na „autíčko s kamerami". Kontrola tak byla zaměřena na zpracování osobních údajů v souvislosti s monitorováním prováděným prostřednictvím automobilů provozovaných kontrolovanou osobou za účelem kontroly placení parkovného v zónách placeného stání na území hlavního města Prahy v rámci projektu www.parkujvklidu.cz.

Obecné fungování kamerových vozidel je možné popsat tak, že vozidla objíždějí předem určené zóny placeného stání v desetiminutových intervalech. Při prvním průjezdu čtyři kamery umístěné na vozidle monitorujícím tyto zóny snímají registrační značky zaparkovaných vozidel. Pořízený snímek registrační značky vozidla se v online režimu prověří v centrálním informačním systému, kdy dochází ke zjištění, zda dané vozidlo (resp. daná registrační značka) má uhrazené parkovné. Pakliže dojde ke zjištění, že registrační značka uhradila parkovné, nedochází k uložení takového snímku, ale k jeho okamžitému výmazu. Pokud ovšem daná registrační značka nemá uhrazeno parkovné, jsou snímky z kamery uchovány a v okamžiku dalšího průjezdu vozidla s kamerami dochází také k pořízení fotodokumentace u vozidel, která nemají uhrazeno parkovné, a to za účelem pořízení důkazu pro případné správní řízení. Tato fotodokumentace se pořizuje dalšími dvěma kamerami. Na shora uvedených internetových stránkách jsou pak zveřejněny informace o zpracování osobních údajů v rozsahu registrační značka, údaje o místě (GNSS souřadnice, informace o poloze snímajícího monitorovacího vozidla a snímaného vozidla), času stání snímaného vozidla, identifikace úseku zóny placeného stání ve vztahu k parkovací relaci, platnost parkovací relace, ID parkovací relace a informace o existenci dlouhodobého parkovacího oprávnění.

Za účelem posouzení postavení, v jakém se kontrolovaná osoba ve vztahu k osobním údajům nachází, si kontrolující vyžádali smluvní dokumentaci. Na základě analýzy příslušných smluv dospěli k závěru, že správcem osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. je hlavní město Praha a zpracovatelem osobních údajů ve smyslu § 4 písm. k) zákona č. 101/2000 Sb. je Technická správa komunikací hl. m. Prahy, a.s., přičemž kontrolující konstatovali, že příslušná zpracovatelská smlouva byla uzavřena v souladu s § 6 zákona č. 101/2000 Sb. Kontrolovaná osoba, tedy společnost Eltodo, a.s., byla ve vztahu k osobním údajům shledána v postavení osoby zpracovávající osobní údaje na základě smlouvy se zpracovatelem osobních údajů ve smyslu § 14 zákona č. 101/2000 Sb.

Inspektorka Božena Čajková

Zpracování osobních údajů klientů při poskytování úvěru společností BNP Paribas Personal Finance SA, odštěpný závod

Úřad zahájil kontrolu na základě kontrolního plánu pro rok 2018, do kterého byl zařazen i podnět týkající se podezření z neoprávněného zpracování osobních údajů stěžovatele kontrolovanou osobou, resp. zpracování osobních údajů po uplynutí lhůty určené k jejich likvidaci.

Kontrolující se zaměřili na plnění povinností vyplývajících společnosti BNP Paribas Personal Finance SA, odštěpný závod (dále jen „společnost BNP Paribas“ nebo „kontrolovaná osoba“) ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v souvislosti se zpracováním osobních údajů klientů při poskytování úvěru.

Kontrolou bylo zjištěno, že smlouva o úvěru je s klienty uzavírána v listinné nebo elektronické formě. Klienti mohou zažádat o úvěr osobně, a to na pobočce kontrolované osoby, příp. též při nákupu zboží na splátky u smluvního partnera kontrolovaného (dále jen „prodejce“) na pobočce prodejce, nebo online prostřednictvím webového portálu kontrolované osoby či prodejce. V případě uzavření smlouvy v listinné formě na pobočce prodejce je pak prodejce v postavení zpracovatele osobních údajů. V ostatních případech (uzavření smlouvy online či osobně v elektronické formě) prodejce osobní údaje klientů dále neuchovává. Postavení zpracovatele osobních údajů mají v souvislosti s poskytováním úvěrů také dodavatelé informačních technologií („dodavatelé“). S prodejci i dodavateli uzavřela společnost BNP Paribas smlouvu o zpracování osobních údajů, která splňuje náležitosti dle § 6 zákona č. 101/2000 Sb. Rozsah informací o klientech, požadovaný v souvislosti se sjednáním úvěru, je shodný bez ohledu na skutečnost, zda je tato žádost činěna osobně na pobočce nebo online. Společnost BNP Paribas v souvislosti s poskytováním úvěrů zpracovává osobní a citlivé údaje klientů, přičemž u citlivých údajů (biometrický podpis klienta) tak činí pouze v případě podpisu smlouvy v elektronické formě. Osobní údaje klientů jsou zpracovávány na základě plnění právní povinnosti společnosti BNP Paribas a souhlasu klientů, citlivé údaje (biometrický podpis) na základě jejich výslovného souhlasu. Účelem zpracování je pak zejména plnění zákonných povinností společnosti dle zvláštních právních předpisů, posuzování žádostí o poskytnutí finanční služby, uzavření a plnění smlouvy s klientem, ochrana práv a oprávněných zájmů společnosti, činnosti v pojišťovnictví, vytvoření souboru informací v rámci registrů klientských informací vypovídajících o bonitě, důvěryhodnosti a platební morálce klienta a marketingové účely.

Kontrolou bylo zjištěno porušení § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. spočívající ve zpracování biometrického podpisu klientů, ačkoli zpracování tohoto údaje není nezbytné pro naplnění účelu zpracování, kterým je dle společnosti BNP Paribas zjednodušení identifikace

klienta. Vzhledem k rozsahu údajů shromažďovaných v souvislosti s poskytnutím úvěru je dle kontrolujících zřejmé, že klienti jsou vůči společnosti identifikováni zcela dostačujícím způsobem. Nadto lze u společnosti BNP Paribas uzavřít smlouvu o úvěru také v listinné formě, která zavazuje společnost i klienta stejným způsobem a ve stejném rozsahu jako smlouva v elektronické formě opatřená biometrickým podpisem klienta.

Dále bylo kontrolou zjištěno, že společnost BNP Paribas uchovává zvukové záznamy telefonních hovorů s klienty, s nimiž byla uzavřena smlouva, po dobu deseti let od ukončení smlouvy. V této souvislosti bylo konstatováno porušení § 5 odst. 1 písm. e) zákona č. 101/2000 Sb., neboť jednotná desetiletá doba uchování záznamů všech telefonních hovorů s klienty, s nimiž byla uzavřena smlouva, není nezbytná. V této souvislosti je Úřad toho názoru, že v případě záznamů telefonních hovorů (za předpokladu, že budou vyhodnoceny jako skutečně nezbytné k naplnění některého legálního účelu), je nutno odlišit jednotlivé typy hovorů a tomu odpovídající účel jejich dalšího uchování. Uvedená doba uchování je pak relevantní pouze v případě, kdy je v rámci telefonního hovoru dán příkaz k transakci. Naopak v případě např. servisního poradenství je taková doba zjevně nepřiměřená. Co se týče běžných hovorů informativního charakteru, je nutné zvážit nezbytnost pořizování záznamů z těchto hovorů, případně pak adekvátně přizpůsobit dobu jejich dalšího uchování.

Porušení ustanovení § 5 odst. 1 písm. e) zákona č. 101/2000 Sb. kontrolující konstatovali také v souvislosti s podnětem stěžovatele doručeným Úřadu. V podnětu stěžovatel uvádí, že společnost BNP Paribas zpracovávala jeho osobní údaje získané v souvislosti s žádostí o zřízení běžného účtu po dobu delší, než jaká byla určena k jejich likvidaci. Tuto skutečnost potvrdila i daná společnost PNB Paribas s tím, že závadný stav (způsobený pravděpodobně přechodem na nový vnitřní informační systém) byl již napraven a v době podání podnětu již osobní údaje stěžovatele nezpracovávala.

Už v průběhu kontroly a následně po předání protokolu o kontrole byli kontrolující informováni o přípravě opatření, které společnost BNP Paribas v souvislosti s konstatovaným porušením v protokolu připravuje. Změny se týkají opatření v souvislosti s délkou uchování zvukových záznamů a opatření týkajících se kontrolou namítaného zpracování biometrického podpisu klienta. S ohledem na uvedené proto nebylo důvodné ukládat kontrolované osobě opatření k odstranění zjištěných nedostatků.

Zpracování osobních údajů na webových stránkách společnosti Mladá fronta, a.s.

Na základě kontrolního plánu pro rok 2018, v němž byla definována jako kontrola zveřejňování osobních údajů na internetu v tzv. klonech veřejných rejstříků, byla zahájena kontrola zaměřená především na zjištění právního titulu pro takové zpracování osobních údajů v návaznosti na právní úpravu dle obecného nařízení a s přihlédnutím k § 60 odst. 3 písm. b) zákona č. 455/1991 Sb., o živnostenském podnikání (dále jen „živnostenský zákon").

Kontrolou bylo zjištěno, že kontrolovaná osoba prostřednictvím informací uvedených na webových stránkách www.finance.cz, resp. webovém portálu rejstriky.finance.cz, nabízí uživatelům (návštěvníkům portálu) službu ve formě informací o právnických osobách a fyzických osobách podnikajících shromážděných z veřejných rejstříků vedených příslušnými úřady České republiky, a to včetně historických informací.

Dle § 60 odst. 3 písm. b) živnostenského zákona dochází po uplynutí čtyř let ode dne zániku posledního živnostenského oprávnění podnikatele k převedení informací o podnikateli z veřejné

části živnostenského rejstříku do části neveřejné. Po tomto převedení se dané osobní údaje již z povahy věci nedají považovat za údaje zveřejněné a aplikace čl. 6 odst. 1 písm. f) obecného nařízení již není možná. Současně není možné na takové zpracování aplikovat ani jiný z právních titulů definovaných v čl. 6 odst. 1 uvedeného nařízení, vyjma souhlasu subjektů údajů. Ve vztahu k těmto osobním údajům tak kontrolovaná osoba nedisponuje žádným právním titulem.

Kontrolovaná osoba současně porušila povinnost vyplývající z čl. 5 odst. 1 písm. d) obecného nařízení, neboť zpracovávala osobní údaje podnikatelů, aniž by zajistila, že tyto osobní údaje budou aktualizované. Kontrolovaná osoba byla v návaznosti na citované ustanovení povinna přijmout vhodná opatření k zajištění pravidelné aktualizace zdrojové databáze podnikatelů.

V průběhu kontroly a následně i po jejím ukončení bylo zjištěno, že v návaznosti na technické přenastavení parametrů zdrojové databáze osobních údajů podnikatelů kontrolovaná osoba závadný stav postupně upravuje. Byla nastavena kompletní aktualizace údajů všech podnikatelů, která povede k tomu, že osobní údaje přeřazené do neveřejné části živnostenského rejstříku budou odstraněny kompletně.

Vzhledem k závěrům kontroly bylo zahájeno správní řízení o uložení pokuty.

Inspektorka Jiřina Rippelová

Kontrola společnosti NaturaMed Pharmaceuticals s.r.o., týkající se povinností správce

Úřad provedl v roce 2018 kontrolu společnosti NaturaMed Pharmaceuticals s.r.o. (dále jen „NaturaMed"), která se zabývá nabídkou a následným prodejem výživových doplňků. Nabídku zboží realizuje tato společnost prostřednictvím kuponů, které jsou rozesílány, roznášeny do schránek či vkládány do časopisů. Potenciální klienti jsou kontaktováni také prostřednictvím e-mailů a telefonicky prostřednictvím call centra. Ve všech uvedených případech (kupony, e-maily i telefonní hovory) jsou přitom využívány nejen kontakty na bývalé zákazníky společnosti NaturaMed, ale také kontakty z databází jiných subjektů, které tato společnost pro tento účel kupuje, resp. pronajímá.

Kontrola byla zaměřena na společnost NaturaMed na základě většího množství obdržených podnětů. Obvykle se tyto podněty týkaly situace, kdy dotčená osoba nebyla v postavení bývalého zákazníka společnosti NaturaMed, a nebylo jí tedy ani známo, z jakého zdroje společnost její osobní údaje získala. Další skupinou byli bývalí zákazníci společnosti, kteří však další nabídku zboží již výslovně odmítli, tj. odvolali souhlas se zpracováním osobních údajů, a přesto byli dále oslovováni.

Jak bylo již zmíněno, kontrolou bylo zjištěno, že společnost NaturaMed využívá k nabízení svého zboží nejen kontaktní údaje svých bývalých zákazníků, ale také údaje, které získává od jiných subjektů, a to ve formě koupě, případně tzv. pronájmu databáze. Na tyto subjekty pak odkazuje v případě, kdy se dotčené osoby ptají na právní titul (dalšího) zpracování svých osobních údajů, případně chtějí odvolat svůj souhlas či uplatnit právo na výmaz osobních údajů. Společnost tak sice kontaktní údaje získává a využívá jednoznačně za účelem propagace a nabídky vlastního zboží (a je tedy v postavení správce osobních údajů), ve vztahu k subjektům údajů nicméně žádnou odpovědnost nepřijímá. Původci kontaktních údajů (tj. prodejci či pronajímatelé databází), na které společnost NaturaMed odkazuje, pak bývají často nekontaktní. Dotčené osoby se tak obvykle nedomohou nápravy ani touto cestou.

Kontrola byla proto uzavřena se závěrem, že společnost porušila povinnosti správce osobních údajů, a to povinnost zpracovávat osobní údaje výhradně na základě zákonem předvídaného právního titulu (v tomto případě primárně souhlasu). Tento závěr se vztahuje k těm osobním údajům, které získala či převzala z databáze jiných subjektů. Stalo se tak, aniž by zajistila či ověřila, že se souhlas se zpracováním osobních údajů, který dotčené osoby poskytly, vztahuje i na předání osobních údajů a jejich další využití.

Porušení povinností v oblasti zpracování osobních údajů bylo zjištěno i ve vztahu k bývalým zákazníkům společnosti NaturaMed. U těchto osob je obecně dán právní titul k dalšímu využití kontaktních údajů pro nabídku zboží v budoucnosti, a to do doby, než dotčený subjekt údajů vyjádří svůj nesouhlas s tímto postupem. Současně je omezen rozsah osobních údajů, které lze za tímto účelem využívat (jedná se o jméno, příjmení a adresu subjektu údajů, přičemž s ohledem na vývoj komunikačních technologií lze k vyjmenovaným osobním údajům přiřadit také e-mail, neboť tento údaj má v elektronické komunikaci stejný charakter jako adresa). Společnost nicméně uchovávala a využívala pro marketingové účely také telefonní čísla svých bývalých zákazníků, resp. i dalších osob, jejichž údaje získala nákupem či pronájmem databáze.

Kontrolou bylo dále zjištěno porušení informační povinnosti. Společnost NaturaMed informuje subjekty údajů o zpracování jejich osobních údajů odlišně (dle způsobu získávání osobních údajů), avšak vždy nedostatečně. Absentuje zejména přesné vymezení všech osobních údajů, které skutečně zpracovává, a označení právního titulu, na jehož základě se tak děje. Společnost NaturaMed také řádně neinformuje subjekty údajů o jejich právech.

Proti kontrolním závěrům podala společnost NaturaMed námitky, jimž však předsedkyně Úřadu nevyhověla. Odpovědnost za popsané porušení povinností při zpracování osobních údajů pak byla předmětem navazujícího správního řízení, ve kterém byla společnosti uložena sankce ve výši 30 000 Kč za neoprávněné zpracování osobních údajů nejméně pěti osob.

Pravidelná kontrola Schengenského informačního systému

V roce 2018 provedl Úřad pravidelnou kontrolu Schengenského informačního systému. Pravomoc takovou kontrolu provést vyplývá z čl. 44 nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) a také z čl. 60 rozhodnutí Rady 2007/533/SV o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II). Podle citovaných ustanovení je povinen i Úřad provést kontrolu zpracování osobních údajů v národní součásti SIS II (N.SIS II) nejméně jednou za čtyři roky, a to v souladu s mezinárodními auditorskými standardy. Předmětem kontroly bylo jak plnění povinností stanovených citovanými evropskými předpisy správci osobních údajů (Policie ČR), případně zpracovatelů, tak i výkon práv, která mají ve vztahu k SIS II dotčené osoby (subjekty údajů).

SIS byl zřízen Úmluvou ze dne 19. června 1990 k provedení Schengenské dohody o postupném odstraňování kontrol na společných hranicích (tzv. Schengenská prováděcí úmluva). V současné době je členskými státy využíván SIS druhé generace (SIS II), jehož zřízení a provoz jsou upraveny výše citovanými právními předpisy EU. Česká republika se schengenské spolupráce účastní od 21. prosince 2007.

Účelem SIS II (druhá generace systému je užívána od dubna 2013) je zajištění a udržení vysokého stupně bezpečnosti na území členských států (s ohledem na absenci kontrol na vnitřních hranicích schengenského prostoru), a to s využitím informací předávaných prostřednictvím

tohoto systému. Jedná se tedy o zásadní kompenzační nástroj za zrušení policejních kontrol na vnitřních hranicích.

Technická infrastruktura SIS II je opět na základě výše citovaných předpisů definována tak, že SIS II se skládá z centrální části, vnitrostátní části a komunikační infrastruktury.

Odpovědnost za provoz centrální databáze SIS II a komunikační infrastruktury je na straně Evropské unie a agentury EU-LISA (Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva). Členské státy mají odpovědnost za zřízení a funkčnost vnitrostátní části a za její připojení k jednotnému vnitrostátnímu rozhraní. Veškeré údaje se do SIS II vkládají a vyhledávají prostřednictvím vnitrostátní části SIS II, která je kopií centrální databáze SIS II. Přístup do vnitrostátní části SIS II jiných členských států není možný.

Z pohledu zákona č. 101/2000 Sb., který je pro zpracování osobních údajů v SIS II podpůrným právním předpisem k nařízení (ES) č. 1987/2006 a rozhodnutí Rady 2007/533/SV, vyplynulo, že správcem osobních údajů zpracovávaných ve vnitrostátní části SIS II je Policie ČR, která předmětné zpracování provádí a rovněž za něj odpovídá. Účel tohoto zpracování definují právní a interní předpisy Policie ČR.

Zpracování osobních údajů v SIS II se dále účastní subjekty v postavení zpracovatele osobních údajů. Těmi jsou: Generální ředitelství cel, Ministerstvo vnitra ČR (Odbor azylové a migrační politiky), Ministerstvo zahraničních věcí a obecní úřady obcí s rozšířenou působností.

Rozsah zpracovávaných osobních údajů je poměrně široký a opět je stanoven citovanými právními předpisy. Kromě osobních údajů jsou zpracovávány i citlivé údaje, jako jsou např. otisky prstů či jakékoli zvláštní objektivní a nezměnitelné tělesné znaky. Policie ČR interním předpisem stanovila přehled záznamů a souvisejících zdrojových informačních systémů, včetně požadavků na vložení záznamu. Rovněž stanovila detailní postupy při zpracování osobních údajů v SIS II (vkládání, vyhledávání – přístup, aktualizaci a likvidaci). Patří sem i činnost centrály SIRENE s požadavky na zajištění provozu SIS II způsobem, který odpovídá požadavkům vyplývajícím z právních předpisů.

Kontrolou bylo zjištěno přijetí potřebných opatření k tomu, aby bylo zajištěno řádné přijímání a vyřizování žádostí subjektů údajů na realizaci práva na přístup k osobním údajům. V průběhu kontroly byly vyhodnoceny i konkrétní případy. Nebylo zde zjištěno, že by přijatá opatření nebyla v praxi řádně dodržována.

Také v oblasti opatření, která Policie ČR přijala za účelem zajištění bezpečnosti osobních údajů zpracovávaných ve vnitrostátní části SIS II (a jejichž rozsah je rámcově upraven v právních předpisech EU), Úřad neshledal, že by Policie ČR nepřijala či neplnila opatření směřující k zajištění bezpečnosti zpracovávaných osobních údajů v rozsahu, jaký je vyžadován v čl. 10 nařízení (ES) č. 1987/2006 a čl. 16 rozhodnutí Rady 2007/533/SV.

Inspektor Petr Krejčí

Odbor dopravněsprávních činností Magistrátu HMP – neoprávněné zpřístupnění osobních údajů jiným subjektům údajů

Úřad provedl a ukončil kontrolu na pracovišti odboru dopravněsprávních činností Magistrátu HMP Na Pankráci 1685/17-19, 140 21 Praha 4. Kontrolovaná osoba vede mimo jiné i aktuální stav provozovatelů vozidel/přestupců.

Předmětem kontroly bylo dodržování povinností správce/zpracovatele osobních údajů stanovených zákonem č. 101/2000 Sb. v souvislosti se zpřístupněním osobních údajů ve výzvě na zaplacení pokuty za dopravní přestupek.

Úřadu bylo postupně doručeno více podnětů, ve kterých mj. oznamovatelé poukázali na skutečnost, zda není v rozporu se zákonem o ochraně osobních údajů, pokud došlo k zaslání výzev k úhradě určené částky týkající se provozovatelů vozidla ze 3. ledna 2018 na adresy jiných příjemců zásilky. Tím došlo ke zpřístupnění osobních údajů v rozsahu uvedených ve výzvách, které obsahovaly jméno, příjmení, datum narození, adresu trvalého bydliště, registrační značku vozidla, místo a čas, kde se přestupek stal, popis přestupku, výši určené částky, popis způsobu úhrady přestupku, datum vyhotovení výzvy, spisovou značku, číslo jednací a na zadní straně výzvy poučení, neuhradí-li provozovatel vozidla ve výzvě určenou částku. Některé podněty obsahovaly i výzvy, včetně obálky, a/nebo odkazy nebo tisky z webových stránek médií/sdělovacích prostředků s popisem uvedených skutečností.

Kontrolou bylo zjištěno, že postup kontrolované osoby byl v souvislosti s uzavřenou smlouvou s Českou poštou, s.p., týkající se doručování zásilek prostřednictvím hybridní pošty následující: Kontrolovaná osoba v předmětné věci předala 3. ledna 2018 České poště, s.p., datový soubor, který obsahoval dva a půl tisíce výzev k uhrazení určené částky za dopravní přestupek ve formátu PDF, a textový soubor, ve kterém jsou uvedeny adresy, kam výzvy rozeslat. To doložila print screenem obrazovky, resp. seznamem všech souborů předaných na CD a print screenem textového souboru s uvedením v PIDu výzvy a adresy, na které se má výzva odeslat, včetně vyplněné konkrétní výzvy, a souborem odeslaných dat České poště, s.p., dle objednávky prostřednictvím protokolu, resp. na adresu na internetovém portálu České pošty, s.p. Na ten se přihlašuje dodavatel softwaru, zajišťující zpracování výzev a předání dat ke zpracování České poště, s.p. Kontrolovaná osoba zdokumentovala zabezpečení odesílání dat odesílaných do hybridní pošty České pošty, s.p., v příloze k dohodě uzavřené mezi kontrolovanou osobou a Českou poštou, s.p.

Kontrolovaná osoba tak doložila odeslání elektronicky správně spárovaných obsahů výzev s adresami provozovatelů vozidel. K tomu dokázala i způsob, jakým dochází automatizovaně k registraci zakázky, kterou posílá Česká pošta, s.p., na Magistrát hl. m. Prahy a softwarové firmy, potvrzující přijetí objednávky – hybridní pošty.

Již po několika dnech představitelé České pošty, s.p., oznámili veřejnosti, že chyba v odesílané poště je skutečně na její straně, a uvedli, jak k pochybení došlo.

Kontrolou bylo zjištěno, že Česká pošta, s.p., na základě údajů, které obdržela od kontrolované osoby, provedla 5. ledna 2018 strojové zpracování dodávky (objednávky), tj. že na základě předaných výzev provedla jejich vytištění a vložení do obálek a provedla jejich rozeslání adresátům uvedeným na obálkách doporučenými zásilkami určenými do vlastních rukou. Celý proces vyplněných výzev předaných od kontrolované osoby a jejich vkládání do obálek, včetně natištění obálek jménem a adresou, je strojově automatizován a provádí se na obálkovací lince České pošty, s.p. Pokud došlo u výzev z 3. ledna 2018 k chybnému doručování na adresy jiných příjemců, než kteří jsou uvedeni ve výzvě, stalo se tak proto, že došlo dle opakovaného sdělení České pošty, s.p., na jednání z 31. ledna 2018 mezi kontrolovanou osobou a Českou poštou, s.p., údajně k technologické chybě (posunu řádků u oznámení o pokutě a přiřazené adresy přestupce). Ta byla řešena s českým zástupcem zahraničního dodavatele.

Kontrolovaná osoba zcela vyloučila, že by se chyba stala na její straně resp., že by došlo k pochybení jejím konkrétním zaměstnancem. První podnět byl kontrolované osobě doručen 9. ledna 2018 a poté zahájila jednání o nápravě s Českou poštou, s.p., o čemž svědčí vzájemná e-mailová korespondence, včetně urgence k zaslání vyjádření k incidentu, zápis z jednání z 31. ledna 2018 a zpráva – vyjádření České pošty, s.p., k incidentu z 30. ledna 2018.

Byla provedena mimo jiné také kontrola elektronického zabezpečení ochrany osobních údajů, zejména v oblasti požadavků na automatizované zpracování, tzv. logování, na pracovišti odboru dopravněsprávních činností s tím, že používané aplikace splňují dané požadavky. Kontrolovaná osoba vydala veřejný příslib u nesprávně doručených výzev z 3. ledna 2018 o tom, že adresátům z nich nehrozí žádné postihy, chybně obeslaní lidé tedy nemají nic platit, výzvy mohou považovat za bezpředmětné a nesprávně zaslané písemnosti tak nemohou ze zákona vyvolat žádné právní důsledky, tedy ani exekuci.

Vysvětlení chybného doručování bylo sděleno všem dotčeným subjektům údajů v celkovém počtu 2 500 prostřednictvím vyjádření ve sdělovacích prostředcích, včetně informace publikované na webových stránkách Magistrátu HMP, a bylo provedeno nové doručení výzev již na správné adresy. Provedená kontrola jednoznačně vyvrátila tvrzení, že za pochybení v této kauze je odpovědný odbor dopravněsprávních činností Magistrátu hlavního města Prahy. Kontrolou bylo potvrzeno, že za pochybení v případu chybného rozeslání a doručování písemností, resp. výzev z 3. ledna 2018 provozovatelům vozidla je odpovědná jen Česká pošta, s.p. Kontrolovaná osoba v rozsahu předmětu kontroly neporušila žádné ustanovení zákona č. 101/2000 Sb.

Česká pošta, s.p., přijala opatření, aby k podobnému incidentu v budoucnu již nedošlo. Za výše popsané protiprávní jednání byla společnosti uložena pokuta ve výši 250 000 Kč.

Záměna daňových subjektů stejného jména a data narození při doručování písemností Generálním finančním ředitelstvím

Úřad provedl kontrolu Generálního finančního ředitelství, Finančního úřadu pro Ústecký kraj, územní pracoviště v Lounech, Rybalkova 2376, 440 01 Louny, IČ: 72080043.

Kontrola byla zahájena na základě podnětu, v němž oznamovatel upozorňoval na zřejmou systémovou chybu a žádal její odstranění, aby se neopakovaly případy, pokud se neztotožňují fyzické osoby podle jedinečného identifikátoru, jako je rodné číslo nebo bydliště či místo podnikání, a že tak může dojít k chybě v požadavku kontrolované osoby na plnění povinností od jiného než povinného subjektu údajů, jehož důsledkem může být až exekuce vedená proti nesprávnému daňovému subjektu. Oznamovatel uvedl opakování případu konkrétního daňového subjektu, kterému byla kontrolovanou osobou vyměřena pokuta ve výši 2 000 Kč za to, že podal daňové přiznání za rok 2015 na papírovém formuláři, nikoliv datovou schránkou, ač ji nemá zřízenou. Tímto způsobem doručovala kontrolovaná osoba do datové schránky i další písemnosti, tj. jinému daňovému subjektu stejného jména a data narození. Na základě chybného doručování, resp. neztotožněním správného daňového subjektu podle adresy či rodného čísla, došlo k vydání několika písemností (rozhodnutí) kontrolovanou osobou, která byla doručována jiné osobě. Nebyl však důvod je doručovat ani daňovému subjektu, který nebyl vlastníkem datové schránky, a proto jeho povinností nebylo podat daňové přiznání přes datovou schránku. V důsledku této záměny byla věc napravena až na základě vyvolaného správního řízení, v němž se musel dotčený daňový subjekt domoci svých práv až na základě podaného opravného prostředku vůči kontrolované osobě, přičemž kontrolovaná osoba uznala pochybení a platební výměr na pokutu zrušila.

V průběhu kontroly kontrolovaná osoba potvrdila, že k chybě došlo v důsledku stávajícího systémového řešení v informačním systému finanční správy společném pro všechny finanční úřady s tím, že při ručním zpracování a ověřování je správný výběr datové schránky závislý na zodpovědnosti a pozornosti zaměstnance, který všechny údaje potřebné k porovnání shody subjektů

fyzických osob – jméno, příjmení, datum narození a adresu – má v elektronickém systému užívaném kontrolovanou osobou.

Informační systém kontrolované osoby je nastaven tak, že příslušný zaměstnanec ověřuje podle jména, příjmení a data narození, zda má adresát písemností aktivní datovou schránku. Jejím prostřednictvím je pak doručována příslušná listina. V daném případě se jednalo o shodu ve jménu, příjmení i datu narození, a tím došlo k nesprávnému přiřazení nabídnuté datové schránky z informačního systému k daňovému subjektu pro odeslání písemnosti. Jednalo se o chybu, kdy byla listina obsahující osobní údaje jiného daňového subjektu, než komu byla určena, zaslána, resp. zpřístupněna jinému adresátu z důvodu shodného jména, příjmení a data narození. V zásilce obsahující vyrozumění o výši nedoplatku a platebního výměru na pokutu, vložené do datové schránky jiného daňového subjektu, byly mj. tyto osobní údaje: jméno, příjmení, bydliště, rodné číslo, výše nedoplatku a důvod jeho vyměření.

Kontrolovaná osoba provedla po zjištění záměny daňových subjektů opatření přímo u zaměstnankyně kontrolované osoby, která je odpovědná za odesílání písemností, resp. zpřístupnění písemností jinému daňovému subjektu do datové schránky. Tato zaměstnankyně byla na chybné doručení upozorněna a zároveň poučena o příčinách chybného vložení datové schránky v adresátech písemnosti. U kontrolované osoby na územním pracovišti v Lounech proběhla informativní schůzka, na níž byl tento konkrétní případ popsán a rozebrán. Zaměstnanci byli výslovně upozorněni i písemnou formou rozesláním e-mailové zprávy na možnost vložení chybné datové schránky při ověřování existence datových schránek u adresátů v evidenci písemností. Na spisu daňového subjektu bylo v tomto smyslu kontrolovanou osobou vyznačeno upozornění.

Pokud bylo zjištěno a v protokolu o kontrole konstatováno porušení ustanovení § 13 zákona č. 101/2000 Sb., bylo v této souvislosti kontrolované osobě uloženo *„dokončit urychleně systémové opatření pro celou finanční správu tak, aby již v budoucnu nemohlo dojít, a to ani na jiných pracovištích kontrolované osoby, k chybám v doručování písemností. Do té doby kontrolovaná osoba zajistí, že její zaměstnanci budou v případě jakýchkoliv pochybností či nesrovnalostí u daňového subjektu ověřovat při odeslání písemností, zejména adresy trvalého pobytu, včetně jejich porovnávání či jejich ověřování, v případě shodného jména, příjmení i data narození, a to tak, aby nemohlo dojít ke zpřístupnění osobních údajů subjektů údajů neoprávněné osobě, tj. doručením písemnosti jinému příjemci/daňovému subjektu, než komu je písemnost skutečně určena."*

Protokol o kontrole jednoznačně doložil, že došlo k dalšímu pochybení (předtím řešenému Úřadem v roce 2015 na jiném územním pracovišti) téhož druhu v systému kontrolované osoby, a opatření deklarovaná kontrolovanou osobou tudíž zjevně nebyla dostatečně účinná.

Za porušení povinnosti z ustanovení § 13 zákona č. 101/2000 Sb. (povinnost správce 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) uložil Úřad pokutu ve výši 5 000 Kč ve správním řízení.

Ostatní dozorová činnost

• DOZOROVÁ ČINNOST V OBLASTI OBCHODNÍCH SDĚLENÍ

V důsledku nabytí účinnosti 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) došlo v rámci Úřadu k jistým změnám, kdy se dozorovou činností v oblasti ochrany osobních údajů zabývají jednotlivé inspektoráty. Dozorová činnost v oblasti nevyžádaných obchodních sdělení, která byla dříve vykonávána jedním z inspektorátů, pak byla od 1. srpna 2018 svěřena samostatnému nově vzniklému oddělení.

Toto oddělení v rámci své činnosti provádí veškeré úkony spjaté s nevyžádanými obchodními sděleními. Především se jedná o analýzy jednotlivých podání, pro které je na webových stránkách Úřadu vytvořen speciální formulář. Analýzou hlaviček e-mailových zpráv a samotných textů sdělení se zjišťuje odesílatel obchodních sdělení či osoba, v jejíž prospěch jsou obchodní sdělení šířena, a zda se skutečně o obchodní sdělení jedná.

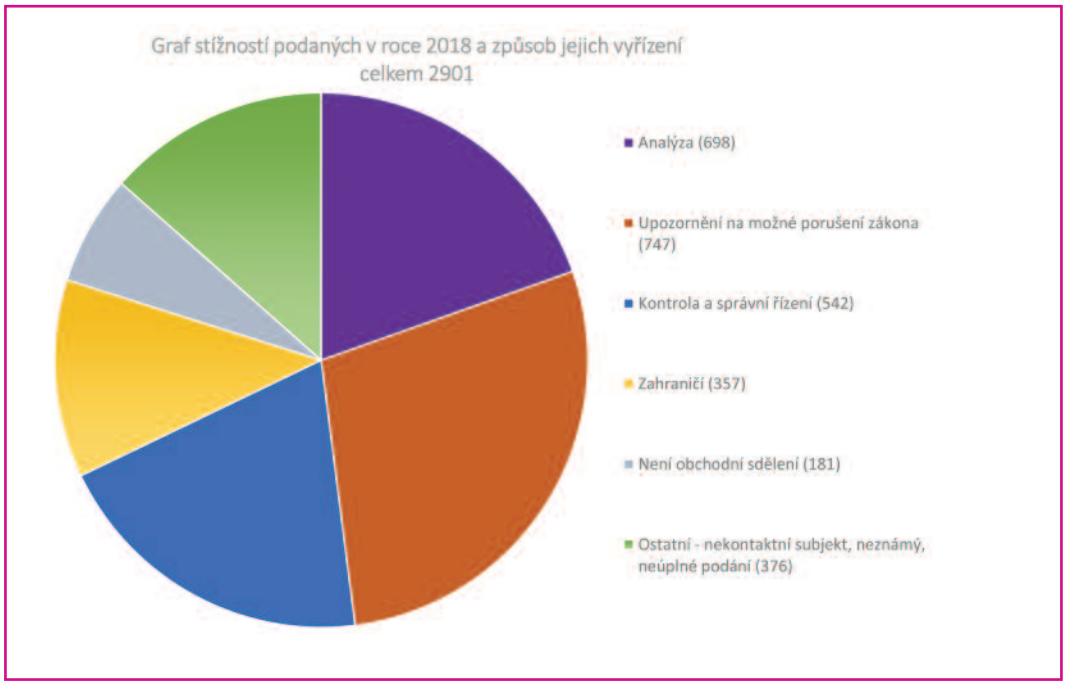
Nejdůležitější a nejrozsáhlejší činností tohoto oddělení je provádění kontrolních a správních řízení. Jak je vidět z přiloženého grafu, zabývalo se toto oddělení v roce 2018 celkem 30 kontrolními řízeními a s 26 subjekty vedlo správní řízení, jehož výsledkem bylo uložení sankce. Celková výše sankce, kterou toto oddělení za šíření nevyžádaných obchodních sdělení udělilo, byla 3 464 360 Kč. V deseti případech bylo vedeno rovněž správní řízení o uložení pořádkové pokuty za neposkytování součinnosti v rámci prováděné kontroly, kdy celková výše uložené sankce činila 905 000 Kč.

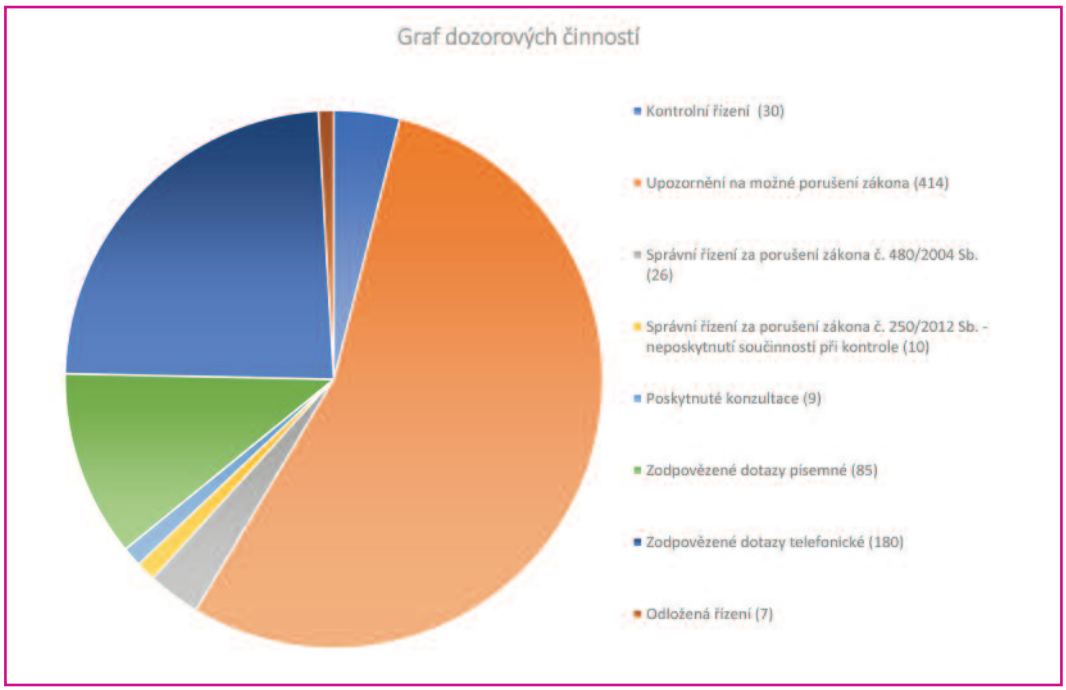
Neméně významné jsou však také úkony spojené s upozorněním jednotlivých subjektů na možné porušení zákona, které se provádí v případech, kdy Úřad obdrží jen několik málo stížností v určeném období vůči jednomu subjektu a zásah do soukromí v elektronické komunikaci tak není značný. Toto upozor-

není plní především preventivní funkci a je spojeno také s náležitým vysvětlením jednotlivých podmínek, za kterých je zasílání obchodních sdělení umožněno. Funkci preventivní a výchovnou či osvětovou plní také další činnosti tohoto oddělení, jako je poskytování konzultací v této oblasti a vyřizování jednotlivých písemných nebo telefonických dotazů či zobecňování výsledků kontrol a správních řízení v podobě vydávání tiskových zpráv a stanovisek.

V rámci mezinárodní spolupráce pak toto oddělení postupuje jednotlivé stížnosti, kde je dohledán zahraniční odpovědný subjekt usídlený v rámci Evropské unie, příslušnému zahraničnímu dozorovému orgánu.

V neposlední řadě sestavuje jednotlivé statistiky, které znázorňuje také v podobě grafů.





Kontrola společnosti Widder Gilde, s.r.o.

Kontrola u této společnosti byla zahájena na základě podaných stížností. Jejím 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 Úřad zjistil, že kontrolovaná osoba uzavřela smlouvu s ukrajinskou společností POLITEKS LTD., kdy smluvní povinností této společnosti je propagace produktů kontrolované osoby. Jedná se mj. o „*zasílání sdělení o výrobcích a službách Widder na e-mailové adresy, k čemuž bude mít Partner* (pozn.: POLITEKS LTD.) *souhlas příslušných osob*". Kontrolovaná osoba tak sama obchodní sdělení neodeslala, ale za tímto účelem uzavřela smlouvu se společností POLITEKS LTD., která rozesílky obchodních sdělení provedla. K faktickému odeslání obchodních sdělení došlo z vůle společnosti Widder Gilde, s.r.o., na základě jí vydaného příkazu k odeslání.

Kontrolující tedy konstatoval, že odpovědným subjektem za šíření obchodních sdělení je jak kontrolovaná osoba, tak také společnost POLITEKS LTD. Vycházel přitom z příslušných ustanovení zákona č. 480/2004 Sb., kde sám zákonodárce předpokládá, že šiřitel může šířit obchodní sdělení nejen vlastními silami, ale i prostřednictvím jiného subjektu. Podle ustanovení § 7 odst. 4 písm. b) zákona č. 480/2004 Sb. *a contrario* musí každé obchodní sdělení obsahovat informaci o odesílateli, jehož jménem se komunikace uskutečňuje, resp. v jehož prospěch je obchodní sdělení šířeno. Jedině takový výklad je eurokonformní a v souladu s účelem zákona. V rámci kontroly pak kontrolující především zkoumal, zda odpovědný subjekt disponuje právním titulem k zasílání obchodních sdělení. Na základě provedených kontrolních úkonů a zjištění dospěl k závěru, že kontrolovaná osoba se žádným způsobem neujistila, zda její smluvní partner disponuje validními souhlasy se zasíláním obchodních sdělení, tak jak to deklaroval v článku 3.5. smlouvy.

Úřad tak konstatoval, že kontrolovaná osoba se dopustila porušení § 7 odst. 2 zákona č. 480/2004 Sb., jelikož šířila obchodní sdělení bez předchozího prokazatelného souhlasu adresátů a další porušení bylo konstatováno ve vztahu k § 7 odst. 4 písm. a) zákona č. 480/2004 Sb., jelikož šířená obchodní sdělení nebyla zřetelně a jasně jako obchodní sdělení označena. Kontrolovaná osoba podala vůči závěrům kontrolního protokolu námitky, které byly předsedkyní Úřadu zamítnuty.

Se společností Widder Gilde, s.r.o., bylo posléze vedeno správní řízení. K tomuto řízení je třeba dodat, že § 11 odst. 1 zákona č. 480/2004 Sb. je konstruován na základě objektivní odpovědnosti, tj. odpovědnosti za právní stav, kdy ve vztahu k právnické osobě není třeba zkoumat zavinění vzniklého protiprávního stavu. Právě z tohoto důvodu a z důvodu naplnění vůle zákonodárce, tj. chránit soukromí v co nejširší možné míře, je třeba za šiřitele obchodních sdělení považovat také ty osoby, které k faktickému odeslání udělily pokyn, příkaz, uzavřely smlouvu či jiným způsobem faktické odeslání obchodních sdělení iniciovaly. Proto je třeba, aby si šiřitelé obchodních sdělení, ať už jde o zadavatele (objednatele) či faktické rozesílatele, vždy dostatečně prověřili, zda adresáti obchodních sdělení udělili souhlas pro takové zasílání, resp. v obecnosti, zda rozesílka probíhá zákonným způsobem. Na základě výše uvedeného kontrolního řízení měl správní orgán za prokázané, že pro předmětné adresáty obchodních sdělení neměla obviněná společnost právní titul pro šíření obchodních sdělení a ani žádným dostatečně průkazným způsobem neověřila, že takovými právními tituly disponuje její partner, se kterým za účelem rozeslání obchodních sdělení uzavřela smlouvu. Ke vztahu odpovědnosti obviněné

společnosti a jejího partnera lze dodat, že každý z těchto subjektů nese svůj vlastní díl odpovědnosti za své jednání naplňující znaky přestupku. Šiřitel v pozici objednatele tedy nese svou vlastní odpovědnost bez ohledu na povinnosti dalších osob, a ve smyslu § 11 odst. 1 zákona č. 480/2004 Sb. je tedy možno za toto jednání postihnout šiřitele v pozici objednatele, tedy společnost Widder Gilde, s.r.o.

V rámci tohoto správního řízení tak byla této společnosti uložena sankce ve výši 80 000 Kč. Obviněná společnost proti rozhodnutí o pokutě podala nejprve odpor, posléze též rozklad, který byl předsedkyní Úřadu zamítnut, a bylo potvrzeno napadené rozhodnutí. Předmětem jak podaných námitek, tak také odporu a rozkladu byl především nesouhlas obviněné s její odpovědností za rozesílání obchodních sdělení.

K tomu je třeba dále blíže uvést další argumenty, které byly použity též v rozhodnutí o rozkladu. Ve prospěch závěru o odpovědnosti obviněné svědčí i systematika a účel zákona č. 480/2004 Sb., kdy ustanovení § 7 a § 11 zákona č. 480/2004 Sb. je nutno vnímat nikoliv odděleně, ale v kontextu zejména se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Ze spisové dokumentace v rámci kontrolního řízení je zřejmé, že obchodní sdělení neměla být určena výhradně právnickým osobám, a proto s ohledem na rozsudek Nejvyššího správního soudu čj. 9 As 34/2008-68 je nutno na podrobnosti elektronického kontaktu nahlížet jako na osobní údaje. Ze smlouvy o marketingové spolupráci vyplývá, že obviněná pověřila partnera propagací jejích produktů a služeb, a to kromě jiného zasíláním sdělení na e-mailové adresy. Obviněná tak určila jak účel, tak i prostředky zpracování osobních údajů, čímž naplnila definici správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. Vzhledem k tomu, že je primárně povinností správce zajistit souladnost zpracování se zákonnými podmínkami, je to právě správce, jenž nese hlavní odpovědnost za případné porušení zákona. Dále lze rovněž poukázat na jeden ze stěžejních principů ochrany osobních údajů, a sice právo subjektu údajů na přístup k informacím. Toto právo je uplatnitelné zejména vůči správci osobních údajů, neboť právě ten odpovídá za zákonnost zpracování a za to, kdo disponuje osobními údaji konkrétního subjektu. Proto je zapotřebí mít povědomost o identitě správce. Jedině tak se lze dovolat práva na přístup k osobním údajům, jejich změnu či likvidaci. Z tohoto důvodu zákonodárce zakotvil povinnost uvádět v každém obchodním sdělení totožnost odesílatele – toho, v jehož prospěch je obchodní sdělení šířeno. Pokud by bylo možno smluvně přenést odpovědnost za nezákonné šíření obchodních sdělení na jiný subjekt, a to včetně subjektů mimo místní působnost státních autorit, výše uvedená práva a principy ochrany osobních údajů, jakož i soukromí v obecném slova smyslu, by byla zcela anulována, a to za současného profitu odesílatele obchodních sdělení, jenž proces faktické rozesílky inicioval a řídil. Za situace, kdy směrnice 2002/58/ES, resp. zákon č. 480/2004 Sb. byly přijímány právě za účelem zvýšení bezpečnosti a ochrany osobních údajů s ohledem na zvláštní rizika internetu a elektronických komunikací, by takovýto závěr byl absurdní a zcela proti smyslu presumpce rozumného zákonodárce, který zamýšlel zajistit co nejvyšší úroveň ochrany.

• STÍŽNOSTI, OHLAŠOVÁNÍ PORUŠENÍ ZABEZPEČENÍ A KONZULTACE

V druhé polovině roku 2017 docházelo ve spojitosti s blížící se účinností obecného nařízení[4] k pozvolnému nárůstu počtu dotazů a posléze, z důvodu postupné medializace nařízení, i k nárůstu počtu stížností subjektů údajů. Proto byla od počátku roku 2018 rozdělena oddělení stížností a konzultací, spadající pod odbor pro styk s veřejností, na oddělení podnětů a stížností a oddělení konzultací. Tento krok umožnil, aby se vedoucí těchto oddělení efektivně věnovali svým agendám. Současně byl odbor pro styk s veřejností přejmenován na odbor konzultačních agend. Tento název lépe vystihuje jeho komplexní činnost, do které účinností obecného nařízení přibylo i vyhodnocování přijatých ohlášení porušení zabezpečení osobních údajů a poskytování předchozích konzultací dle obecného nařízení.

STÍŽNOSTNÍ AGENDA

Stížnostní agendu výrazně ovlivnil přelom účinnosti obecného nařízení. V tomto období směřovala velká část stížností proti postupu správců osobních údajů při získávání souhlasu dotčených subjektů údajů v situaci, kdy správce

- neoprávněně podmiňoval poskytnutí služby (tj. uzavření smlouvy) souhlasem se zasíláním obchodních sdělení či jinými nikoli nezbytnými marketingovými aktivitami,
- získával souhlas manipulativně např. tím, že vyjádření souhlasu nebylo srozumitelně odděleno od správcem poskytované informace o zpracování osobních údajů či samotného smluvního ujednání.

Po účinnosti obecného nařízení, jehož jedním z pilířů jsou práva subjektu údajů, zaznamenal Úřad zvýšený počet stížností na nevykonávání těchto práv ze strany správců. Jednalo se zejména o právo na přístup k osobním údajům, kdy subjektu údajů často nebyla na jeho žádost poskytnuta informace nebo bylo znesnadňováno uplatnění tohoto práva neadekvátními požadavky na způsob ověření jeho identity. Uplatnění tohoto práva nabývá na významu například v oblasti častých stížností na nevyžádaný telemarketing, jelikož umožňuje subjektu údajů získat nejen kopii zpracovávaných osobních údajů, ale i informaci o zdroji osobních údajů. To mu umožňuje efektivně rozhodnout o dalším postupu.

Po účinnosti obecného nařízení došlo rovněž k nárůstu počtu stížností na kopie veřejných rejstříků internetu, provozované soukromými subjekty. Zpravidla se jednalo o další publikování údajů o podnikatelské činnosti fyzických osob či údajů z insolvenčního rejstříku. V návaznosti na to Úřad, mimo jiné, předložil na svých webových stránkách návod dotčeným osobám, jakým způsobem uplatnit u provozovatele předmětných databází a internetových stránek práva přiznaná obecným nařízením.

Stížnosti v roce 2018 se týkaly také zveřejňování osobních údajů na internetu a souvisejícího práva být zapomenut, kdy musel být, pro zvolení dalšího postupu, hodnocen vztah práva na

[4] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

informace a na soukromí. Tradiční součástí stížnostní agendy byly stížnosti na kamery, nejčastěji využívané v rámci sousedských (občanskoprávních) sporů, zaměstnavatelem nebo k ochraně veřejného majetku.

Z procesního hlediska Úřad v méně závažných případech porušení či podezření z porušení, a to jak zákona č. 101/2000 Sb., tak od 25. května 2018 obecného nařízení, přistupoval k osvědčenému informování správců o možném porušení pravidel ochrany osobních údajů. V drtivé většině těchto případů bylo už v této fázi dosaženo nápravy, aniž musely být uplatněny kroky z moci úřední. Těchto informativních dopisů, do velké míry přispívajících ke kultivaci prostředí, zaslal Úřad správcům v roce 2018 téměř pět set.

Velká část informativních dopisů se týkala oblasti zveřejňování adresních údajů žadatelů o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Šlo zejména o obce, které v rámci usnadnění této agendy velmi často přistupují ke zveřejnění dokumentu s poskytnutou informací, aniž by zároveň odstranily adresní údaje žadatelů. V této souvislosti se Úřad setkal i se zneužitím obecného nařízení, kdy žadatel, s vědomím, že obce mnohdy postupují tímto nesprávným krokem, odeslal stovkám obcí žádost o informace s úmyslem vyvolat tento závadný stav. Následně po nich žádal náhradu újmy podle obecného nařízení v podobě finančního zadostiučinění.

OHLAŠOVÁNÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Účinností obecného nařízení vznikla správcům nová povinnost, spočívající v ohlašování rizikových porušení zabezpečení osobních údajů Úřadu. V rámci této agendy bylo možné v prvé řadě vysledovat, že jelikož jde pro správce o novou povinnost, mnohdy nereflektovali požadavky obecného nařízení na obsah ohlášení. Velmi často totiž chyběl popis pravděpodobných důsledků incidentu pro dotčené osoby a také popis opatření, která správce přijal s cílem vyřešit daný incident. To jsou velmi podstatné náležitosti nezbytné pro posouzení přijatého ohlášení.

Opakovaným předmětem ohlášení porušení zabezpečení osobních údajů bylo napadení tzv. ransomwarem, který protiprávně zašifroval informace. Pachatel následně požadoval výkupné. Mezi další častá ohlášení patřila ztráta zařízení či dokumentů, obsahujících osobní údaje. Nejčastěji se v takových případech jednalo o selhání lidského faktoru či krádež.

KONZULTACE

Účinnost obecného nařízení výrazně ovlivnila i konzultační agendu. Její osvětový význam, ve spojitosti s tímto novým právním předpisem, nabyl ještě více na důležitosti. Mnohdy totiž bylo nutné mírnit paniku, která se kolem obecného nařízení vytvořila. Ve vhodných případech pak Úřad tazatelům zdůrazňoval základní kontinuitu pravidel s dřívějším zákonem č. 101/2000 Sb. Počátek roku a přelom účinnosti obecného nařízení se nesl v extrémním náporu dotazů ze strany široké veřejnosti. Úřad se po několik měsíců potýkal s dvojnásobným počtem dotazů, než bylo obvyklé v minulých letech. Proto, z důvodu větší efektivity, v průběhu roku výrazně zaktualizoval rubriku Často kladených otázek a pro lepší orientaci ji rozdělil do jednotlivých částí dle oblastí, kterých se otázky týkají. Rovněž byly průběžně doplňovány informační materiály na webových stránkách Úřadu, aby veřejnost nalezla všechny podstatné informace o obecném nařízení, bez nutnosti kladení písemných dotazů.

Ke dni účinnosti obecného nařízení začala být každodenně provozována telefonní informační linka určená k poskytování rychlých a jednodušších informací o obecném nařízení veřejnosti,

zvláště malým a středním podnikatelům. Zároveň začala být k dispozici dvakrát týdně telefonní linka pro dotazy týkající se kamer a kamerových systémů.

Největší část konzultační agendy tradičně představovalo odpovídání na písemné dotazy, které se, vzhledem k prolínání problematiky ochrany osobních údajů všemi aspekty lidského života, obsahově týkaly velmi různorodých otázek.

Před účinností, ale i po účinnosti obecného nařízení, bylo často potřeba objasňovat, v jakých případech vzniká, respektive nevzniká povinnost jmenovat pověřence pro ochranu osobních údajů, např. v případě některých typů příspěvkových organizací.

U dotazů na uplatňování práv subjektů údajů bylo v některých případech třeba vysvětlovat, že ani obecné nařízení nepřináší změnu tam, kde je určitý postup stanoven zvláštním zákonem, tedy např. nelze uplatňovat právo na výmaz, jestliže zákon stanoví delší dobu pro uchovávání údajů.

Vysvětlovat bylo nutné i přísnější výklad Pracovní skupiny 29 (po účinnosti obecného nařízení byla nahrazena nově ustanoveným Evropským sborem pro ochranu osobních údajů) k povinnosti vést záznamy o činnostech zpracování, který se i v případě menších podniků týká každého stále prováděného zpracování osobních údajů. To správci poskytuje užitečný přehled o jím prováděných činnostech.

V některých případech žádost směřovala k tomu, zda má správce provádět posouzení vlivu na ochranu osobních údajů podle článku 35a. V této souvislosti bylo upozorňováno, že rozhodnutí vypracovat posouzení vlivu je na správci, který má s Úřadem konzultovat až případná zbytková vysoká rizika podle článku 36 obecného nařízení. Kvalifikovanou žádost o předchozí konzultaci podle tohoto článku však Úřad v roce 2018 neobdržel.

Nedílnou součástí konzultační agendy bylo i poskytování osobních konzultací sdružením správců, samotným správcům či jejich pověřencům pro ochranu osobních údajů. Úřad tak například poskytl osobní konzultaci zástupcům bankovního sektoru, významnému zástupci automobilového průmyslu nebo řadě ústředních státních úřadů či státních orgánů.

Za účelem zvyšování osvěty a povědomí byly na půdě Úřadu, ve spolupráci s příslušnými útvary Úřadu, uspořádány semináře pro pověřence jmenované podle článku 37 odst. 1 písm. a) až c) obecného nařízení, které se setkaly s velmi kladným ohlasem a pro všechny účastníky měly vysokou informační hodnotu.

• UKLÁDÁNÍ SANKCÍ

Úřad uložil v roce 2018 pokuty za přestupky (resp. porušení obecného nařízení[5]) v souhrnné výši 7 202 360 Kč, z toho za nevyžádaná obchodní sdělení 3 464 360 Kč. Shrnutí statistických informací o řízeních, která Úřad v roce 2018 vedl, lze nalézt v části této výroční zprávy nazvané Úřad v číslech.

Ochrana osobních údajů v České republice, resp. v celé Evropské unii, byla v roce 2018 spojena s obecným nařízením.Hlavní téma spojené s obecným nařízením přitom pro laickou veřejnost (i část odborné) nepochybně představovaly pokuty. Podle obecného nařízení lze totiž uložit

[5] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

správní pokuty až do výše 20 milionů eur, nebo jedná-li se o podnik, až do výše čtyř procent celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší. Současně však obecné nařízení výslovně stanovuje, že ukládání správních pokut musí být v každém jednotlivém případě účinné, přiměřené a odrazující. S ohledem na tyto požadavky a také s přihlédnutím k ustálené judikatuře nejvyšších českých soudů, podle které nesmí být uložená sankce likvidační (viz např. nález pléna Ústavního soudu sp. zn. Pl. ÚS 3/02 ze dne 13. srpna 2002), nelze předpokládat, že sankce ukládané za porušení povinností stanovených obecným nařízením budou standardně dosahovat řádů milionů či dokonce desítek až sta milionů korun. Při ukládání správních pokut podle obecného nařízení je třeba přihlížet k řadě okolností, které jsou například vyjmenovány v čl. 83 odst. 2 nařízení. Z těchto okolností lze zdůraznit třeba míru spolupráce s dozorovým úřadem za účelem nápravy daného porušení, zmírnění jeho možných nežádoucích následků nebo i způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil.

Je třeba v této souvislosti připomenout, že nejvyšší sankce uložená Úřadem podle zákona č. 101/2000 Sb. za 15 let jeho činnosti v této oblasti byla ve výši 3 600 000 Kč (přičemž maximální hranice činila podle tohoto právního předpisu 10 000 000 Kč). Jednalo se tedy o pokutu uloženou nad hranicí jedné třetiny zákonem stanovené sazby. Obecně sankce ve výši nad 1 000 000 korun byly spíše výjimečné.

Přestože v roce 2018 nabylo účinnosti obecné nařízení, řízení o přestupcích, která Úřad vedl, se vztahovala k protiprávním jednáním, k nimž došlo za účinnosti zákona č. 101/2000 Sb. Za významné, a to nejen z hlediska výše pokut, lze (nad rámec některých z případů uvedených v části této výroční zprávy nazvané Poznatky inspektorů z kontrolní činnosti) považovat zejména tyto případy:

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZA ÚČELEM VYTVÁŘENÍ DATABÁZÍ K DALŠÍMU PRODEJI

Na základě kontroly provedené v roce 2017 zahájil Úřad řízení o přestupku se společností Solidis s.r.o., ve kterém jí byla uložena pokuta ve výši 800 000 Kč.

Úřad v řízení konstatoval, že společnost zpracovávala bez zákonného důvodu osobní údaje přesně nezjištěného počtu osob v řádech statisíců, nejméně v rozsahu jméno, příjmení, adresa a telefonní číslo, které získala od třetích osob. Tím porušila povinnost stanovenou v § 5 odst. 2 zákona č. 101/2000 Sb., tedy povinnost zpracovávat osobní údaje se souhlasem subjektu údajů nebo v případech stanovených v § 5 odst. 2 písm. a) až g) tohoto zákona.

Společnost v rámci své podnikatelské činnosti shromážděné osobní údaje (od jiných společností, případně i z vlastní činnosti) dále využívala pro vytváření databází pro své klienty na základě objednávek. Tím určila účel a prostředky zpracování osobních údajů, a byla tedy správcem osobních údajů. Na tom nic nemění ani skutečnost, že osobní údaje, které poskytovala za úplatu svým klientům, byly strukturované dle požadavků jednotlivých klientů, ani že jejich zdrojem byly jiné subjekty. Současně platí, že to, že je společnost správcem ve vztahu k jednomu ze zpracování osobních údajů, které provádí, nijak nevylučuje, aby se v případě některých jiných konkrétních zpracování nalézala v postavení zpracovatele.

Osobní údaje společnost získala na základě licenčních smluv, resp. objednávky, dle kterých byl souhlas s oslovováním garantován poskytovatelem, nebo se mělo jednat o oprávněně zveřejněné údaje. To však nelze považovat za vyjádření souhlasu splňujícího nezbytné náležitosti

(tj. svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů). Podle § 5 odst. 4 zákona č. 101/2000 Sb. musí být navíc subjekt údajů při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování.

Z uvedeného je zřejmé, že souhlasem pro další zpracování osobních údajů (vytváření databází využívaných k nabízení obchodu a služeb) společnost, jakožto správce, nedisponovala. Je přitom znovu potřeba zdůraznit, že by se muselo jednat o souhlasy, ve kterých by jako správce osobních údajů byla uvedena ona sama. Odpovědnosti za doložení právního titulu ke zpracování osobních údajů se přitom nemůže správce zprostit odkazem na smluvní dokumentaci, která má zaručovat, že předmětný právní titul (tedy v tomto případě souhlas) existuje. Je jeho povinností u svého smluvního partnera tuto skutečnost ověřit a zajistit, že bude schopen souhlasy doložit, byť by byly třeba uloženy u druhé smluvní strany.

Rozklad podaný společností proti rozhodnutí správního orgánu prvního stupně předsedkyně Úřadu zamítla.

ZAKOUPENÍ NELEGÁLNĚ ZÍSKANÉ DATABÁZE OSOBNÍCH ÚDAJŮ

V létě roku 2016 uložil Úřad doposud nejvyšší pokutu za porušení pravidel při zpracování osobních údajů. Jednalo se o pokutu ve výši 3 600 000 Kč, která byla uložena společnosti T-Mobile Czech Republic a.s. Úřad konstatoval, že společnost nepřijala dostatečná opatření k zabezpečení osobních údajů obsažených v elektronické interní databázi, která obsahovala osobní údaje zhruba 1,2 milionu jejích zákazníků – fyzických osob.

V říjnu roku 2016 Úřad zaznamenal v médiích zprávy o tom, že odcizená data klientů společnosti T-Mobile Czech Republic a.s. zakoupila společnost STEM/MARK, a.s. V návaznosti na tyto informace zahájil u této společnosti neprodleně kontrolu. V jejím rámci však uvedená společnost odmítla poskytnout nezbytné podklady k jejímu provedení s odkazem na skutečnost, že ve věci je vedeno trestní řízení. Aby nedošlo k uplynutí lhůt pro případné uložení sankce, zahájil Úřad v lednu 2017 ve věci řízení pro podezření ze spáchání správního deliktu. Řízení však muselo být v červenci 2017 přerušeno vzhledem ke skutečnosti, že Policie České republiky prováděla ve shodné věci prověřování všech skutečností nezbytných pro rozhodnutí o zahájení trestního stíhání. Od srpna 2018 Úřad ve svém řízení pokračoval, neboť mu byla postoupena kopie části spisové dokumentace policie a došlo k odevzdání věci k projednání správního deliktu.

V září 2018 vydal Úřad rozhodnutí o uložení pokuty ve výši 400 000 Kč společnosti STEM/MARK, a.s., neboť neoprávněně zpracovávala v období od března do května 2016 osobní údaje zákazníků společnosti T-Mobile Czech Republic a.s. Jednalo se o osobní údaje dvou tisíc fyzických osob (v rozsahu jméno, příjmení, adresa bydliště, pohlaví, věk a telefonní číslo) a dále osobní údaje zhruba 81 tisíc fyzických osob podnikajících (v rozsahu jméno, příjmení, telefonní číslo, počet sim karet užívaných osobou, způsob provádění plateb za služby operátora a název banky, ze které platby přicházejí). Tím společnost porušila povinnost stanovenou v § 5 odst. 2 zákona č. 101/2000 Sb., tedy povinnost zpracovávat osobní údaje se souhlasem subjektu údajů nebo v případech stanovených v § 5 odst. 2 písm. a) až g) tohoto zákona, protože pro jejich zpracování neměla žádný právní titul.

Ze spisového materiálu vyplynulo, že společnost byla v průběhu února 2016 oslovena s nabídkou ke koupi databáze, o kterou projevila zájem. Po prodejci požadovala (z hlediska rozsahu databáze) pouze poštovní směrovací číslo a telefonní číslo. Prodejce nebyl schopen databázi takto upravit, proto koupila databázi celou. Jednalo se o databázi dvou tisíc fyzických osob a dále databázi 260 tisíc právnických osob a fyzických osob podnikajících. Ze zjištění Úřadu vyplynulo, že databáze obsahovala osobní údaje zhruba 81 tisíc fyzických osob podnikajících. Zakoupená data společnost dále nevyužila, protože je v té době nepotřebovala, a následně jí byla zabavena Policií České republiky. Za uvedenou databázi zaplatila společnost částku přibližně 120 000 Kč.

Proti rozhodnutí o uložení pokuty podala společnost rozklad, který odůvodnila zejména tím, že není odpovědná za protiprávní jednání, kterého se dopustil její zaměstnanec (tehdejší zástupce ředitele a člen dozorčí rady).

Rozklad podaný proti rozhodnutí předsedkyně Úřadu zamítla a rozhodnutí o pokutě tak nabylo právní moci v prosinci 2018. Ve svém rozhodnutí předsedkyně mimo jiné uvedla, že odpovědnost za protiprávní jednání je třeba přičíst společnosti, neboť nešlo o zjevný exces jejího zaměstnance.

• POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

Některá rozhodnutí Úřadu byla v roce 2018, stejně jako v letech předchozích, předmětem soudního přezkumu. Řada dalších rozhodnutí Úřadu na soudní přezkum stále čeká. Pokud jde o konkrétní poznatky z předmětné soudní praxe, lze poukázat na několik rozsudků, týkajících se zejména:

- zveřejňování osobních údajů,
- rozsahu shromažďovaných osobních údajů nutných k uzavření soukromoprávního kontraktu,
- instalace kamerových systémů zaměstnavatelem.

1. Veřejný zájem na zveřejnění informací o odposlechu a záznamu telekomunikačního provozu a informací získaných z odposlechu a záznamu telekomunikačního provozu tiskem a veřejně přístupnou počítačovou sítí převažuje nad právem na ochranu soukromí v případě informování veřejnosti o relevantním ovlivňování mocenského rozhodování předsedy vlády osobou, jíž takové jednání formálně nepříslušelo.

Nejvyšší správní soud ve svém rozsudku ze dne 3. května 2018 v řízení o kasační stížnosti společnosti MAFRA, a.s., proti rozsudku Městského soudu v Praze ze dne 9. srpna 2017, především konstatoval, že ve shodě s Úřadem a Městským soudem v Praze považuje za dostatečně prokázané, že informace zveřejněné společností společnosti MAFRA, a.s., jsou informacemi získanými z odposlechů a ze záznamů telekomunikačního provozu pořízených v režimu předpokládaném v § 8c trestního řádu, přičemž žádná z osob, jichž se týkají, nedala ke zveřejnění souhlas a nejednalo se o informace již užité v řízení před soudem. Dále pak Nejvyšší správní soud uvedl, že: *„Zákaz stanovený v § 8c trestního řádu byl porušen a ke zveřejnění informací došlo*

prostřednictvím tisku a veřejně přístupné počítačové sítě. Tím byly naplněny formální znaky správního deliktu podle § 45a odst. 1 zákona o ochraně osobních údajů. Nejde ovšem o deliktní jednání, pokud jsou splněny podmínky § 8d trestního řádu, v daném případě podmínky veřejného zájmu na zveřejnění informací, převažuje-li ten nad právem na soukromí dotčené osoby, a to každé z nich. Zde má místo posouzení proporcionality mezi právem na informace a právem na ochranu soukromí osob dotčených zveřejněním."

Nejvyšší správní soud rovněž přisvědčil Úřadu i Městskému soudu v Praze, že za souhlas nelze považovat skutečnost, že se osoby dotčené tímto správním deliktem žádným způsobem nevymezily proti následnému zveřejnění informací. Úplné zveřejnění odposlechů a záznamů telekomunikačního provozu bylo dle Nejvyššího správního soudu problematické a bylo namístě rozsah zveřejňovaných informací omezit. Nelze však upřít převahu veřejného zájmu na zveřejnění informací tam, kde tyto informace seznamují veřejnost s tím, že předseda vlády byl při svém mocenském rozhodování relevantně ovlivňován osobou, jíž takové jednání formálně vzato nepříslušelo. Tato osoba však přesto komunikovala s pracovníky zpravodajských služeb ve věcech svého soukromého zájmu týkajícího se premiéra.

Tyto závěry Nejvyššího správního soudu Úřad v novém řízení v předmětné věci plně reflektoval.

2. K uzavření smlouvy o poskytování přepravy s cestujícím jednoznačně postačuje jméno, příjmení, datum narození a adresa cestujícího. Tyto údaje jsou obecně postačující při uzavírání všech soukromoprávních kontraktů. Technická realizace plnění uzavřené smlouvy nemůže ospravedlňovat nezákonné shromažďování osobních údajů. Správce osobních údajů musí s každou sadou shromážděných osobních údajů a příslušným souhlasem s jejich zpracováním nakládat individuálně, tedy musí být schopen ukončit jejich zpracování a údaje zlikvidovat poté, co byl odňat příslušný souhlas s jejich zpracováním, popř. pokud odpadly zákonné důvody pro zpracovávání osobních údajů bez souhlasu.

Městský soud v Praze ve svém rozsudku ze dne 7. prosince 2017, který byl doručen dne 8. ledna 2018, zamítl žalobu společnosti ČSAD Karviná a.s. proti rozhodnutí předsedy Úřadu ze dne 30. července 2015. Předmětným rozhodnutím předseda Úřadu potvrdil prvoinstanční rozhodnutí, kterým Úřad společnosti ČSAD Karviná a.s. jako správci osobních údajů, udělil pokutu ve výši 60 000 Kč za porušení povinnosti stanovené v § 5 odst. 1 písm. d) a § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. K porušení výše uvedené zákonné povinnosti došlo tím, že správce zpracovával osobní údaje obsažené ve stornované žádosti/smlouvě o vydání elektronického peněžního prostředku (EM CARD). Tímto jednáním se společnost ČSAD Karviná a.s. dopustila správního deliktu dle § 45 odst. 1 písm. c) a písm. e) zákona č. 101/2000 Sb. V dané věci bylo předmětem sporu výhradně právní hodnocení Úřadu, nikoliv rozporování skutkového stavu.

Městský soud v Praze ohledně správního deliktu podle § 45 odst. 1 písm. c) zákona č. 101/2000 Sb., jehož spáchání bylo společností ČSAD Karviná a.s. rozporováno, přisvědčil argumentu Úřadu stran nadbytečnosti uvádění rodného čísla, když dle jeho názoru je plně dostačující jméno, příjmení, datum narození a adresa trvalého pobytu žadatele o vydání EM CARD. Zároveň Městský soud v Praze uvedl, že rozsudek Nejvyššího správního soudu č.j. 7 A 58/2002-40 ze dne 22. října 2013, z něhož lze dovodit poměrně široké možnosti využití rodného čísla tam, kde je potřeba jednoznačně identifikovat osoby, považuje v tomto směru za již překonaný, neboť pochází z doby, kdy nebylo rodné číslo považováno za osobní údaj zvláštní povahy ve smyslu čl. 8 odst. 7 směrnice 95/46/ES a na jeho použití se nevztahovala zvláštní

právní úprava v § 13, resp. § 13c zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), implementovaná až po novelizaci provedené zákonem č. 53/2004 Sb., účinným od 1. dubna 2004. Rodné číslo slouží, dle názoru Městského soudu v Praze, k identifikaci občanů ve vztahu ke státu, resp. jeho orgánům. Použití určitých prostředků technické realizace pak nemůže ospravedlňovat nezákonné shromažďování osobních údajů. Dotčená společnost tedy měla technicky zajistit fungování systému tak, aby elektronické odbavovací zařízení a příslušná karta či jiné technické prostředky ke svému provozu rodné číslo nevyžadovaly. Jak uvedl dále Městský soud v Praze: „*S ohledem na vývoj právní úpravy, kdy lze dovodit, že od 1. 4. 2004 je nutné nahlížet na shromažďování rodných čísel restriktivně, měl žalobce více než 10 let k patřičné úpravě systému. Soud uzavírá, že žalobce ostatně již nyní vydává kartu ODISka, která rodné číslo nevyžaduje, což svědčí o technické proveditelnosti systému bez používání rodných čísel cestujících*."

Ohledně naplnění skutkové podstaty správního deliktu podle § 45 odst. 1 písm. e) zákona č. 101/2000 Sb. dal Městský soud v Praze rovněž za pravdu Úřadu, když uvedl, že „*… jeden a ten samý správce osobních údajů může shromažďovat shodné osobní údaje totožné osoby za stejným účelem vícekrát, pokud je každé shromáždění založeno samostatným jednáním, přičemž k jednotlivým shromážděním osobních údajů a souhlasům k jejich zpracování je nutné přistupovat odděleně.*" Nová žádost o vydání nové karty je tak shromažďování osobních údajů odlišné od předchozí žádosti o vydání karty, k němuž lze samostatně odejmout souhlas se zpracováváním osobních údajů, který se ovšem nijak nedotkne předchozího souhlasu, a to i když jsou zúčastněné subjekty, osobní údaje a účel zcela shodné. Nadto Městský soud v Praze upozornil, že „*… žalobce by zřejmě v případě stornování žádosti zcela nového žadatele o vydání EM CARD, jehož osobními údaji by nedisponoval z dřívějška, postupoval metodicky stejně, tedy navzdory nesouhlasu subjektu osobních údajů by si tuto vyplněnou žádost obsahující osobní údaje, byla-li by již opatřena číslem, ponechal do skartace, kdy by ani nemohl použít svůj argument stran ryze formálního nakládání s již jednou zákonně shromážděnými a zpracovanými údaji.*" Přestože zákon o ochraně osobních údajů výslovně neuvádí, v jaké lhůtě mají být osobní údaje zlikvidovány, lze dle Městského soudu v Praze dovodit, že k likvidaci osobních údajů musí dojít bez zbytečného odkladu, jinak by předmětná ustanovení zákona směřující k ochraně před neoprávněným shromažďováním osobních údajů pozbývala smyslu.

3. Provoz automobilové přepravy jako takové bez dalšího nepředstavuje vysoce nebezpečný provoz podle § 316 odst. 2 zákoníku práce. Aplikace § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. vyžaduje naplnění kritéria vhodnosti i kritéria potřebnosti.

Nejvyšší správní soud rozsudkem č.j. 10 As 245/2016–41 ze dne 20. prosince 2017, který nabyl právní moci dne 15. ledna 2018, zamítl kasační stížnost společnosti STUDENT AGENCY k.s., a potvrdil tak rozhodnutí Městského soudu v Praze č.j. 5 A 107/2013–38 ze dne 18. října 2016.

Společnost STUDENT AGENCY k.s. zamýšlela v přední části svých autobusů umístit kameru, která by snímala pouze obrazový záznam zabírající řidiče a stevarda, a to za účelem ochrany svého majetku, zaměstnanců a přepravovaných osob, včetně ochrany jejich zdraví. K použití záznamů mělo dojít při řešení dopravních nehod nebo stížností cestujících. V tom společnost spatřovala naplnění výjimky pro zpracování osobních údajů bez souhlasu subjektu údajů podle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Úřad však registraci takového zpracování osobních údajů podle § 17 odst. 2 zákona č. 101/2000 Sb. nepovolil.

Společnost STUDENT AGENCY k.s. se proto obrátila se žalobou na Městský soud v Praze, který se však zcela ztotožnil s testem proporcionality provedeným Úřadem, kdy byly poměřovány zájmy zaměstnavatele, tj. ochrana jeho majetku a života a zdraví zaměstnanců a cestujících, a na druhé straně právo zaměstnanců na ochranu jejich soukromí na pracovišti. Na základě provedeného testu Úřad konstatoval, že kamera monitorující řidiče a stevarda a jejich bezprostřední okolí je nedůvodným a nepřiměřeným zásahem do jejich soukromí, a proto nelze ve věci aplikovat § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Městský soud v Praze rovněž konstatoval, že odůvodnění rozhodnutí správních orgánů obou stupňů Úřadu jsou „*…velmi pečlivá, určitá a logická…*", vydaná v souladu se zákonem a ustálenou judikaturou soudů. Žalobu proto jako nedůvodnou podle § 78 odst. 7 soudního řádu správního zamítl.

Proti rozhodnutí Městského soudu v Praze č j. 5 A 107/2013–38 ze dne 18. října 2016 podala společnost STUDENT AGENCY k.s. kasační stížnost. Nejvyšší správní soud pak v rozhodnutí o kasační stížnosti uvedl, že rozhodnutí Úřadu i Městského soudu byla správná, neboť v daném případě nebylo naplněno kritérium potřebnosti zpracování osobních údajů, pouze kritérium vhodnosti. Podle Nejvyššího správního soudu nejsou kamerové systémy zárukou zamezení vzniku nežádoucí události, mají však významný vliv například na možnost následného uplatnění práv poškozených a zabránění opakování takové činnosti v budoucnu, jakož i představují odstrašující prvek, aby vůbec k protiprávnímu jednání nedocházelo. Kritérium potřebnosti vychází jak z nemožnosti uplatnit méně invazivní prostředky k dosažení cíle sledovaného správcem osobního údajů, tak existence reálného ohrožení právem chráněných hodnot správce osobních údajů, které společnost STUDENT AGENCY k.s. nedoložila.

S ohledem na výše uvedené konstatoval Nejvyšší správní soud, že „*nedospěl k závěru, že by již z povahy autobusové dopravy jako takové bez dalšího vyplývalo, že ke stěžovatelkou popisovaným situacím z povahy věci s vysokou mírou pravděpodobnosti docházet může. Tak tomu může být u některých vysoce nebezpečných provozů, tedy situací, na které pamatuje § 316 odst. 2 zákoníku práce hovořící o zvláštní povaze činnosti zaměstnavatele. Lze souhlasit s tím, že při chybách v řízení autobusu může docházet k ohrožení většího množství osob i majetku. Pokud by však soud přisvědčil tomu, že již jen tato okolnost představuje zvláštní povahu činnosti zaměstnavatele, pak by ji musel přiznat jakékoliv automobilové přepravě, neboť jakýkoliv řidič může porušením povinností účastníka silničního provozu způsobit jak škodu na zdraví, tak i na majetku i třetích osob, a to značného rozsahu.*"

Nejvyšší správní soud proto dospěl k závěru, že pouze z povahy autobusové přepravy nelze předpokládat trvale zvýšené riziko, pro které by bylo nezbytné monitorovat po celou dobu jízdy vnitřek autobusu.

• OSVĚDČENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (CERTIFIKACE)

Obecné nařízení[6] zavádí mechanismy pro vydávání osvědčení, pečetí a známek dokládající ochranu údajů pro účely prokázání souladu s nařízením (čl. 42 a 43). Osvědčení (certifikát) o ochraně osobních údajů je dokument vydaný subjektem pro vydávání osvědčení, kterým subjekt (správce, zpracovatel, výrobce atd.) prokazuje zajištění souladu s požadavky obecného nařízení.

Vydávání osvědčení se týká:

1. operací zpracování osobních údajů (tj. jednotlivých nebo více zpracování osobních údajů)
2. produktů (hw, sw) a služeb (recitál bod 100)

Podle obecného nařízení mohou osvědčení (certifikáty) vydávat:

1. subjekty pro vydávání osvědčení, které jsou akreditovány; nebo
2. Úřad pro ochranu osobních údajů, přičemž akreditovat (oprávnit k provádění vydávání osvědčení/certifikaci) mohou:

1. Úřad pro ochranu osobních údajů,
2. Český institut pro akreditaci či,
3. Úřad pro ochranu osobních údajů a Český institut pro akreditaci současně.

Úřad po důkladném uvážení a analýze vložil odpovědnost za vydávání akreditací do rukou národního akreditačního orgánu, kterým je Český institut pro akreditaci (v souladu s nařízením Evropského parlamentu a Rady (ES) 2008/765 a v souladu s normou ČSN EN ISO/IEC 17065 a požadavky stanovenými příslušným dozorovým úřadem). Podle navrhovaného ustanovení § 15 zákona o zpracování osobních údajů má být ČIA akreditační autoritou ze zákona. Po schválení zákona mu tedy bude výkon činnosti v oblasti udělování akreditací svěřen automaticky. Hlavním důvodem jsou dlouholeté zkušenosti ČIA s touto činností, jeho nezávislost a možnosti celoevropského uznávání takto vydaných osvědčení.

Úřad zahájil jednání s Českým institutem pro akreditaci o spolupráci na přípravě systému vydávání osvědčení o ochraně osobních údajů tak, aby vyhovoval podmínkám nařízení.

Pro vytvoření podmínek pro vydávání osvědčení je podle obecného nařízení nezbytné v gesci Úřadu vytvořit dva základní dokumenty:

- požadavky pro akreditaci subjektů pro vydávání osvědčení,
- kritéria pro vydávání osvědčení.

Úřad zahájil práce na přípravě návrhu kritérií pro vydávání osvědčení (akreditační a certifikační kritéria), které předložil k veřejné diskusi s tím, že případné připomínky měly být předloženy v lednu 2018. Na základě připomínek byl text upraven a je připraven k zaslání Evropskému sboru pro ochranu osobních údajů ke stanovisku.

---

[6] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

Právě Sboru připadá významná úloha při ovlivnění tvorby kritérií. V současné době připravuje dokument týkající se provádění certifikací a tvorby kritérií. Praxe je taková, že jakmile budou jeho pokyny hotové a schválené, Úřad je v rámci přípravy příslušných dokumentů zohlední.

Důležité je dodat, že podání žádosti o vydání osvědčení podle nařízení je dobrovolné rozhodnutí správce, jehož cílem je prokázat soulad s nařízením. Nejedná se tedy o novou povinnost správce nebo zpracovatele. V současné době zatím nelze žádat ani o vydání akreditace, ani o osvědčení.

• PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

V první polovině roku 2018 dobíhal i v oblasti předávání osobních údajů do zahraničí režim 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. Ten vyžadoval obecně pro každé předání osobních údajů do země s nedostatečnou úrovní ochrany povolení Úřadu. Počet podávaných žádostí však byl již minimální. Konkrétně Úřad v období od 1. ledna do 25. května 2018 přijal tři žádosti o povolení k předání osobních údajů do třetích zemí podle § 27 odst. 4 zákona č. 101/2000 Sb.

Z uvedených tří žádostí byla jedna odložena, neboť šlo o předání do Izraele, který je zemí s odpovídající úrovní ochrany osobních údajů podle rozhodnutí Komise ze dne 31. ledna 2011. Další řízení bylo zastaveno, neboť žadatel po konzultaci s Úřadem vzal svou žádost zpět. Úřad tedy vydal v tomto roce jediné a v režimu směrnice 95/46/ES poslední povolení. Konkrétně se jednalo o předání osobních údajů klientů cestovní kanceláře do zemí cílových destinací jejich pobytu na základě právního titulu daného ustanovením § 27 odst. 3 písm. e) zákona č. 101/2000 Sb. v souladu, s kterým šlo o předání údajů nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů.

Snížený počet žádostí lze vysvětlit skutečností, že správci se již intenzivně adaptovali na novou právní úpravu ochrany osobních údajů. Obecné nařízení[7] v ustanoveních čl. 44–50 převedlo celou oblast předávání osobních údajů do třetích zemí do samoregulačního režimu. Obecně tedy platí, že správce osobních údajů již nemusí žádat Úřad o povolení předání osobních údajů do třetích zemí, ani ho nemusí o takovém předání informovat.

Povolení Úřadu je nyní nutné pouze v případech, kdy správce hodlá předání osobních údajů do třetích zemí s nedostatečnou úrovní ochrany realizovat na základě nestandardních nástrojů pro vytvoření vhodných záruk podle čl. 46 odst. 3 písm. a) a b) obecného nařízení (tzn. nestandardní smluvní doložky; nezávazná správní ujednání mezi orgány veřejné moci nebo veřejnými subjekty zahrnující vymahatelná a účinná práva subjektů údajů). I v těchto neobvyklých případech se spíše než o povolení předání jedná o schválení nestandardního nástroje pro předávání osobních údajů, které vyžaduje plné uplatnění mechanismu jednotnosti včetně vydání

[7] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

kladného stanoviska Evropským sborem pro ochranu osobních údajů. S ohledem na uvedený charakter takových povolení nepřekvapí fakt, že takové povolení dosud nebylo vydáno nejen v rámci České republiky, ale ani v rámci celé Evropské unie.

S obecným nařízením se těžiště práce Úřadu v oblasti předávání údajů přesouvá od povolování jednotlivých konkrétních předání ke schvalování vlastních nástrojů zajišťujících zákonné předávání údajů do třetích zemí s nedostatečnou úrovní ochrany osobních údajů, tzn. vhodných záruk podle čl. 46 odst. 2 obecného nařízení. Do úvahy přitom přicházela především závazná podniková pravidla, která byla obecným nařízením povýšena na jeden ze standardních zákonných nástrojů k vytvoření vhodných záruk ochrany osobních údajů předaných do třetích zemí.

Proto se Úřad s předstihem rozhodl aktivně zapojit do náročné práce těch dozorových úřadů, které se podílejí na realizaci konkrétních schvalovacích procedur závazných podnikových pravidel (Binding Corporate Rules, BCR) a mezi které dosud patřily takřka výlučně dozorové úřady velkých „starých" členských států Evropské unie. V průběhu roku 2018 Úřad v roli spoluhodnotitele (co-reviewer) připomínkoval revidované návrhy BCR v rámci tří schvalovacích procedur vedených ještě v režimu směrnice 95/46/ES. V jednom případě byl Úřad ve stejné roli zapojen do schvalovací procedury vedené již v režimu nařízení.

V rámci těchto prací Úřad získal zkušenost, že žadatelé o schválení závazných podnikových pravidel reagují na doporučení a připomínky úřadů spoluhodnotitelů velmi vstřícně a zpravidla provedou úpravy BCR v maximálním doporučovaném rozsahu. Na základě tohoto lze konstatovat, že pečlivá práce spoluhodnotitele podstatně přispívá ke kvalitě výsledně schválených závazných podnikových pravidel a tím i ke zvýšení globální úrovně ochrany osobních údajů vůbec.

Na úrovni Pracovní skupiny podle čl. 29 směrnice 95/46/ES (dále jen „WP29"), resp. Evropského sboru pro ochranu osobních údajů se Úřad aktivně zúčastnil práce podskupiny International Transfers na přípravě výkladových stanovisek a dalších pomocných materiálů pro oblast předávání osobních údajů do třetích zemí. V oblasti BCR byla pro režim obecného nařízení finalizována a vydána řada návodných dokumentů pro skupiny podniků, které se rozhodnou vytvořit svá závazná podniková pravidla:

- Pracovní dokument vykládající schvalovací proceduru závazných podnikových pravidel pro správce a pro zpracovatele v režimu obecného nařízení (WP263),
- Standardní žádost o schválení závazných podnikových pravidel předávání osobních údajů pro správce (WP264),
- Standardní žádost o schválení závazných podnikových pravidel předávání osobních údajů pro zpracovatele (WP265),
- Pracovní dokument stanovující prvky a zásady, které musejí být součástí závazných podnikových pravidel pro správce (WP256) a
- Pracovní dokument stanovující prvky a zásady, které musejí být součástí závazných podnikových pravidel pro zpracovatele (WP257).

Vedle těchto praktických dokumentů byly rovněž finalizovány zásady pro hodnocení odpovídající úrovně ochrany osobních údajů ve třetí zemi Adequacy Referantial (WP254). Validitu všech právě uvedených dokumentů potvrdil na svém prvním zasedání dne 25. května 2018 Evropský sbor pro ochranu osobních údajů.

Ten schválil i další dvě důležitá výkladová stanoviska. Šlo o Pokyny 2/2018 k výjimkám podle článku 49 nařízení (EU) 2016/679 a Pokyny 3/2018 k teritoriální působnosti nařízení (EU)

2016/679 (článek 3). Posledně jmenovaný dokument byl koncem roku 2018 předložen k veřejné diskusi.

Rovněž se Úřad přihlásil ke spolupráci na formulaci stanoviska Sboru k návrhu rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů v Japonsku, zúčastnil se konzultací se zástupci Komise i se zástupci japonského dozorového úřadu pro ochranu osobních údajů (Personal Information Protection Commission, PPC) a mnoha osobních setkání a telekonferencí pracovního týmu. V jeho rámci připadla Úřadu zodpovědnost za zhodnocení korektnosti postupu Komise v oblastech uplatnění zásad integrity a důvěrnosti, minimalizace doby uchování a transparentnosti.

Pracovní tým identifikoval několik slabých míst, především se však musel potýkat se zásadní otázkou týkající se charakteru navrhovaného rozhodnutí Komise. Odpovídající úroveň ochrany osobních údajů v Japonsku totiž není rozhodnutím Komise konstatována pro celý japonský právní systém, ale je omezena na privátní subjekty řídící se japonským zákonem o ochraně osobních informací (Act on the Protection of Personal Information, APPI) a na evropská data. Pro ty je vytvořen zvláštní režim ochrany garantovaný dodatečnými předpisy PPC (Supplementary Rules), které jsou přílohou rozhodnutí Komise. Lze proto konstatovat, že použité schéma odpovídající úrovně ochrany se nevztahuje na celou zemi, ale je odvětvové, nebo se dokonce spíše blíží zárukám ochrany osobních údajů podle čl. 46 obecného nařízení. Podobně tomu bylo v případě rozhodnutí Komise o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí.

Rovněž bude Úřad usilovat o určující roli při formulaci výkladu vztahu mezi uplatněním čl. 3 a kapitoly V obecného nařízení, v němž mj. nepůjde o nic menšího než o explicitní definici předání osobních údajů do třetích zemí.

• SCHENGENSKÁ SPOLUPRÁCE

Tématu ochrany osobních údajů, jež jsou zpracovávány v rozsáhlých evropských informačních systémech, mezi něž patří Schengenský informační systém druhé generace (SIS II), Vízový informační systém (VIS), Eurodac a Celní informační systém (CIS), je přikládána v jejich právní úpravě značná důležitost. Úřad plní v rámci své působnosti v oblasti schengenské spolupráce úlohu vnitrostátního dozorového orgánu, který vykonává dohled nad dodržováním příslušných předpisů. Přispívá tak k ochraně základních práv osob, jejichž osobní údaje jsou předmětem zpracování v rámci schengenského prostoru. Pověřený zástupce Úřadu se navíc pravidelně účastní jednání koordinačních skupin, které byly k jednotlivým systémům zřízeny. Sem patří i speciálně zřízená Rada spolupráce pro Europol, která funguje od roku 2017.

Kromě standardního dohledu a kontroly souvisejících s požadavky na zákonné zpracování osobních údajů správci zmíněných systémů se Úřad v tomto roce zabýval rozsáhlými kontrolami národních součástí SIS II, CIS a VIS nebo připomínkováním nově vznikajících právních úprav některých systémů.

ČINNOST JEDNOTLIVÝCH KOORDINAČNÍCH SKUPIN V OBLASTI SCHENGENSKÉ, VÍZOVÉ A CELNÍ SPOLUPRÁCE

Všeprostupujícími tématy napříč skupinami byly v roce 2018:

- interoperabilita informačních systémů,
- postoje a stanoviska k legislativním změnám a
- otázka budoucnosti dozoru ve světle rozsáhlých legislativních změn v oblasti ochrany osobních údajů.

K oblasti interoperability zaslaly tři koordinační skupiny (SIS II SCG, VIS SCG, Eurodac SCG) společný dopis podporující kritické stanovisko Evropského inspektora ochrany dat (*EDPS*), Pracovní skupiny 29 (*WP29*) a Agentury Evropské unie pro základní práva (*FRA*). Adresátem byla Evropská komise, Parlament a Rada.

Pravidelně byla aktualizována doporučení na základě uskutečněných hodnocení členských států k uplatňování schengenského acquis (pro SIS II SCG a VIS SCG).

V rámci skupin byly také dokončeny některé dlouhodobé projekty a studie. Jedná se například o společný plán pro provádění inspekcí Celního informačního systému (Úřad se na jeho vypracování v minulosti podílel jako hlavní zpravodaj), studie týkající se logování na národních úrovních v SIS II a studie k implementaci čl. 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 a příručka k uplatnění práv subjektů údajů v rámci Europolu.

AKTUÁLNÍ PROBLÉMY ŘEŠENÉ V RÁMCI KOORDINAČNÍCH SKUPIN

Koordinační skupina pro systém SIS II (*SIS II SCG*) pravidelně aktualizuje vhodná doporučení pro členské státy plynoucí ze schengenských evaluací. Tato činnost je koordinována se skupinou pro systém VIS. Dalším pravidelně aktualizovaným dokumentem je příručka pro subjekty údajů k přístupu k údajům zpracovávaným v SIS II. Aktuálně skupina zpracovává studii, která by měla poskytnout přehled národní legislativy a praxe členských států při vkládání záznamů o osobách a věcech pořízených pro účely skrytých nebo zvláštních kontrol podle čl. 36 rozhodnutí Rady č. 2007/533/SVV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II), a to na základě statistik ukazujících navýšení počtu těchto záznamů.

Koordinační skupina pro systém VIS (*VIS SCG*) dokončila ke konci roku 2018 přípravu dopisu Evropské komisi, Parlamentu a Radě reflektujícího pozici skupiny vůči připravované nové legislativě upravující VIS. Skupina identifikovala zásadní problematické body, které mohou z hlediska ochrany osobních údajů vzbuzovat určité pochybnosti. Neméně intenzivně se zabývala studií, která by měla mapovat školení v oblasti ochrany osobních údajů pro pověřené zaměstnance orgánů disponujících přístupem do VIS. Finální návrh dokumentu je očekáván na příštím červnovém jednání v roce 2019.

Koordinační skupina pro Eurodac (*Eurodac SCG*) ke konci roku finalizovala případový dokument pojednávající o předčasném vymazání údajů subjektů v případě, kdy dotyčný získá občanství některého z členských států, a studii týkající se uplatňování práv subjektů údajů vůči systému Eurodac. O konečné podobě bude hlasováno na dalším jednání v červnu 2019.

Koordinační skupina pro Celní informační systém (*CIS SCG*) aktualizovala příručku pro přístup subjektů údajů k informacím v CIS. Dále byl aktualizován a schválen společný formát pro

inspekci CIS, na němž se jako hlavní zpravodaj v minulosti Úřad podílel, a modul pro inspekci zabezpečení údajů. Připravován je dotazník pro inspekci bezpečnostní politiky AFIS (Anti-Fraud Information System).

Rada spolupráce pro Europol (ECB) vypracovala stanovisko ohledně sledovacího mechanismu Europolu v kontextu čl. 39 nařízení EP a Rady (EU) č. 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol). Mezi další hlavní aktivity skupiny patřilo zpracování praktické příručky pro národní jednotky Europolu a informačního letáku pro subjekty údajů.

POČTY PODNĚTŮ, STÍŽNOSTÍ, DOTAZŮ A JEJICH VYŘÍZENÍ

Jednou z dalších povinností Úřadu je také vyřizování zaslaných podnětů subjektů údajů týkajících se zpracování jejich osobních údajů v SIS II. Úřad v roce 2018 v této věci obdržel celkem 22 podnětů, přičemž ve třech případech přezkoumával postup Policie ČR vůči zpracování osobních údajů. V jednom případě se pak podílel na přeshraniční spolupráci mezi dozorovými orgány v souvislosti s právem na přístup k osobním údajům zpracovávaným v SIS II.

Úřad dále obdržel celkem 19 podání, v rámci kterých se žadatelé dotazovali na vízovou politiku České republiky či na průběh vyřizování svých vízových žádostí. Vzhledem k tomu, že tato oblast nespadá do zákonem stanovených kompetencí Úřadu, byli jednotliví žadatelé odkázáni na Ministerstvo zahraničních věcí a v jednom z případů na Policii České republiky. Úřad v této souvislosti průběžně objasňoval své kompetence svěřené mu 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 této spolupráce. Mezi ty patří Schengenský informační systém, vízová politika, policejní spolupráce, vnější hranice, návraty a ochrana osobních údajů. Hodnotící týmy jsou vždy vytvářeny ad hoc k jednotlivým evaluacím. Jsou složeny ze zástupců Evropské komise a expertů z členských států, případně ze zástupců Evropského inspektora pro ochranu údajů (*EDPS*). Na základě předložených dokumentů a následné kontroly připraví hodnotící tým 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 institucí.

V listopadu 2018 se zaměstnankyně Úřadu účastnila jako národní expertka evaluační mise v Litvě. V roce 2019 proběhne evaluace v České republice.

Analytická činnost

Analytické oddělení plní zadané úkoly v oblasti působnosti Úřadu pro ochranu osobních údajů (Úřad) již od poloviny roku 2016. Poté, co vstoupilo v účinnost v květnu 2018 obecné nařízení o ochraně osobních údajů (obecné nařízení),[8] význam analytické práce ještě vzrostl. Ochrana osobních údajů a soukromí, která je cílem obecného nařízení, totiž předpokládá přehodnocení stávajících přístupů a nové metodické postupy při aplikaci práva na ochranu osobních údajů. Ačkoliv je obecné nařízení založeno na kontinuitě s předchozí právní úpravou, vyznačuje se řadou změn, jejichž smyslem je účinněji chránit základní práva, která upravuje, především právo na ochranu osobních údajů a soukromí. Na základě principu proporcionality však zohledňuje i další základní práva.[9]

Východiskem pro práci s nařízením je aplikace jeho obecných principů. Nadto nařízení obsahuje nové instituty, které musí být implementovány do ochrany dat (právo na přenositelnost, posouzení vlivu, hlášení incidentů). V tomto ohledu jsou významným nástrojem pro správné postupy správců a zpracovatelů stanoviska a názory Evropského sboru pro ochranu osobních údajů (EDPB), dříve Pracovní skupiny k článku 29 (WP29).[10] Analytické zkoumání je předpokladem hlubšího chápání problémů a hledání vyváženého vztahu mezi rozvojem technologií a ochranou osobních údajů. Na tomto základě budou vznikat nová konkrétní řešení zajišťující soulad s ochranou osobních údajů. Při hledání řešení nesmí být opomenuta dynamika rozvoje nových technologií, jež zvyšuje nároky na odbornost u všech, kteří mají chránit osobní údaje a soukromí.

V loňském roce analytické oddělení konkrétně poskytovalo vyjádření či rozbory k otázkám ochrany osobních údajů a soukromí státním orgánům a institucím včetně soudů, podílelo se na zajišťování vzdělávací a osvětové činnosti Úřadu i na poskytování poradenství včetně spolupráce při poskytování odpovědí na dotazy veřejnosti. Při plnění uvedených úkolů vycházelo z východisek, principů a ustanovení současně platného regulačního rámce ochrany osobních údajů a soukromí v ČR a EU. Na tomto základě formulovalo své závěry či

[8] 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).

[9] Článek 4 preambule obecného nařízení.

[10] Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů byla zřízena na základě článku 29 směrnice 95/46/ES (tzv. *Article 29 Working Party*, dále WP29). Po účinnosti obecného nařízení plní její úkoly Evropský sbor pro ochranu osobních údajů (EDPB).

doporučení ve vztahu k předloženým problémům. Z otázek, kterými se analytické oddělení v loňském roce systematicky zabývalo, je možné např. zmínit požadavky ochrany osobních údajů ve vztahu k zdravotním registrům, k vedení databáze DNA a uchovávání telekomunikačních záznamů. V dalším textu bude pojednáno o podstatných aspektech ochrany osobních údajů ve vztahu k těmto tématům.

Zdravotní registry

Úřad obecně nemá námitky vůči zavádění a existenci systémů zdravotních registrů, pokud je jejich cílem využívat současné možnosti technologického rozvoje pro optimalizaci zdravotních systémů a efektivní alokaci finančních prostředků vybraných v rámci systému zdravotního pojištění. Je však třeba vzít v úvahu, že zdravotní registry shromažďují velké objemy dat. Pokud tyto databáze neobsahují osobní informace, nepředstavují rizika z pohledu ochrany osobních údajů. Ovšem většina v současnosti generovaných dat zahrnuje osobní údaje a rozsáhlé datové soubory zvyšují rizika pro lidské soukromí a ochranu osobních údajů. Hodnota informací přitom nespočívá pouze v jejich primárním účelu, ale i v jejich sekundární aplikaci, tedy zpracování pro jiné účely, než k jakým byly původně shromážděny. Při shromažďování velkého objemu dat může dojít nejen k hrozbám pro osobní údaje a soukromí, ale také k opomenutí etických otázek, lidské důstojnosti či lidské individuality. Data velkého rozsahu jsou rovněž zmíněna jako možné riziko v již účinném obecném nařízení. Nástrojem, který má komplexně řešit závažné otázky vztahu mezi technologickým rozvojem a ochranou osobních údajů či soukromí a nastavit kritéria pro zvažování míry přiměřeného zásahu do soukromí, je nový regulatorní rámec ochrany dat v Evropské unii, především obecné nařízení. Právní rámec ochrany dat založený na obecných principech přitom ponechává větší prostor správcům (zpracovatelům) k zajištění souladu s právní úpravou oproti regulaci založené na podrobných pravidlech.

Pokud jde o zdravotní údaje, obecné nařízení je považuje za osobní údaje a definuje jako údaje týkající se tělesného nebo duševního zdraví fyzické osoby. Patří sem i údaje o poskytnutí zdravotních služeb, které vypovídají o zdravotním stavu. Tyto údaje jsou obecným nařízením výslovně řazeny do zvláštní kategorie osobních údajů, pro které je zaveden přísnější režim zacházení. Vychází se přitom z toho, že zdravotní údaje, které jsou svou povahou citlivé a podléhají etickým standardům a povinnosti lékařské mlčenlivosti, vyžadují obzvlášť vysokou úroveň ochrany. Pokud jde o zpracování zvláštních kategorií osobních údajů, článek 9 obecného nařízení jejich zpracování zakazuje, pokud není stanovena výjimka podle čl. 9 odst. 2. Správce tedy musí po účinnosti obecného nařízení pečlivě zvážit, zda mu svědčí některá z deseti výjimek uvedených ve druhém odstavci. Zpracování osobních údajů u zdravotních registrů zpravidla nevychází ze souhlasu subjektu údajů, ačkoli institut souhlasu je obecně svrchovaným a primárním z hlediska naplnění práva na informační sebeurčení. Právním důvodem zpracování bude v tomto případě právní povinnost, ovšem pouze za předpokladu existence dostatečných záruk k ochraně osobních údajů.

Při posuzování toho, zda lze vůbec zpracovávat zdravotní údaje, případně jaká opatření zavést k jejich ochraně, je potřebné vyjít jednak z obecných principů obecného nařízení, jednak je třeba zohlednit tzv. konstrukční principy, na kterých je obecné nařízení založeno. Správná aplikace obecných principů nařízení prakticky znamená položit si otázky, zda konkrétní zpracování splňuje požadavky jednotlivých principů, např. zda je stanoven účel zpracování, zda existuje právní důvod pro zpracování, zda jsou údaje minimalizovány či zda jsou zpracovávány pouze po nezbytnou dobu. Do této oblasti patří i zásadní požadavek transparentnosti zpraco-

vávání osobních údajů, s nímž souvisí i informační povinnost správce. Z nových institutů, které přináší obecné nařízení, je třeba zdůraznit institut posouzení vlivu na ochranu osobních údajů. Ten by měl být v případě zdravotních registrů, které zpracovávají citlivé údaje ve velkém rozsahu, samozřejmostí, což také vyplývá z preambule k obecnému nařízení. Význam má také princip ochrany soukromí již od návrhu (privacy by design), který požaduje takové výchozí nastavení, aby k ohrožení osobních údajů vůbec nemohlo docházet. Z konstrukčních principů obecného nařízení je třeba zmínit např. přístup založený na riziku, který předpokládá náročnější opatření v případě vyššího rizika, ale zejména preventivní přístup, který znamená, že je třeba volit přístupy, které předchází ohrožení či porušení osobních údajů. Konkrétně v řadě případů není nutné, aby správci shromažďovali osobní údaje, ale postačí jim, pokud pracují s anonymními údaji, které obecné nařízení nepovažuje za osobní údaje.

Ochrana osobních údajů a práva subjektu údajů nesmí být tedy v kontextu zdravotních registrů opomenuta. Současná právní úprava má v tomto ohledu rezervy, protože principy a pravidla ochrany osobních údajů ještě nebyly dostatečně promítnuty do právní úpravy zdravotních registrů. V tomto ohledu je návodem mj. nález Ústavního soudu Pl. ÚS 1/12 ze dne 27. 11. 2012,[11] který odkazuje na platnost obecných principů platných pro zpracování osobních údajů a aplikaci principu proporcionality na základě kritérií vhodnosti, potřebnosti a přiměřenosti. Citovaný nález srozumitelně uvádí principy, které mají být aplikovány na všechny zdravotní registry.[12] Z účelu zdravotních registrů, tak jak je zákon vyjmenovává v § 70 odst. 1 a § 73, je přitom zřejmé, že k jejich plnění by mnohdy postačovaly anonymizované údaje. V tomto ohledu by tedy stačilo, kdyby zdravotnická zařízení předávala do Národního zdravotnického informačního systému (NZIS) anonymizované údaje, které by se přirozeně nemohly stát předmětem úniku. Je třeba dodat, že pokud obecné nařízení v mezidobí od přijetí nálezu Pl. ÚS 1/12 zvýšilo standard ochrany osobních údajů oproti dřívější směrnici 95/46/ES, musely přirozeně vzrůst i požadavky kladené na ochranu osobních údajů a soukromí, které představují základní práva chráněná ústavním pořádkem.

Databáze DNA

Vedení databází DNA je dlouhodobě tématem ochrany osobních údajů. Systematický přístup k problematice genetických a biometrických údajů lze nalézt především ve výkladových stanoviscích WP29.[13] O DNA je přitom v rámci ochrany osobních údajů pojednáváno jak v souvislosti s údaji genetickými, tak biometrickými, s nimiž sdílí společné charakteristické vlastnosti. Uvedená stanoviska obsahují společná východiska pro zpracování biometrických a genetických údajů ve vztahu k ochraně osobních údajů a soukromí. Například pracovní dokument WP29 o genetických údajích z roku 2004 poprvé uvedl, že „*nejsou jakékoliv pochyby, že na obsah genetické informace se vztahuje definice osobního údaje*". V tomto materiálu se také uvádělo, že si vnitrostátní orgány stále více uvědomují rizika spojená se zpracováním genetických údajů, a proto je nutné spojit nové genetické technologie s odpovídajícími ochrannými opatřeními

[11] http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-1-12

[12] Je proto žádoucí, aby zákonodárce při přijímání nové právní úpravy Národního registru zdravotnických pracovníků pečlivě zvážil, do jaké míry z těchto hledisek obstojí i ostatní registry tvořící Národní zdravotnický informační systém, a svým včasným zásahem odstranil jejich případné nedostatky, jež by mohly vést k porušování práva pacientů, zdravotnických pracovníků či jiných osob na informační sebeurčení.

[13] Working Document on Biometrics adopted on 1 August 2003.
Opinion 3/2012 on developments in biometric technologies adopted on 27 April 2012.
Working Document on Genetic Data adopted on 17 March 2004.

k ochraně práva na soukromí. Předpokládá se obecný trend směřující k novým iniciativám ochrany dat na vnitrostátní úrovni.

Pracovní stanovisko WP29 č. 3/2012 zdůraznilo jednak cenovou dostupnost technologií, jednak to, že systémy, které analyzují DNA osob, mohou velmi účinně přispět k boji proti trestné činnosti a zjistit totožnost neznámé osoby, která je podezřelá ze spáchání závažného trestného činu. Zároveň upozornilo, že používání těchto systémů ve velkém měřítku může mít závažné vedlejší účinky pro ochranu soukromí. V případě DNA se jedná zejména o riziko, že DNA technologie nemohou zajistit úplnou přesnost a vždy existuje riziko vyplývající z nesprávné identifikace ve formě falešně pozitivních nebo falešně negativních výsledků zpracování, které se dotýkají práv jednotlivce včetně možných diskriminačních důsledků. Dále v případě DNA existuje riziko, že mohou být odhaleny citlivé údaje o zdraví dotyčné osoby či lze odhalit rasový či etnický původ. Upozorňuje se také na nebezpečí centrálního uchovávání DNA, jež by mohlo vést k propojování databází (vytváření podrobných profilů jednotlivců), i na zvláštní nebezpečí opětovného použití těchto údajů k neslučitelným účelům, zejména v případě neoprávněného přístupu.

Názory na biometrické a genetické údaje se postupně vyvíjely, přičemž stále více se prosazoval přístup, že s ohledem na extrémně jedinečnou charakteristiku genetických údajů a jejich spojení s informacemi, které mohou odhalit zdravotní stav nebo etnický původ, by s těmito informacemi mělo být zacházeno jako s „obzvláště citlivými". Diskuse o charakteru těchto údajů pokračovala i po celou dobu přípravy obecného nařízení, přičemž teprve v závěrečném stadiu příprav bylo jednak rozhodnuto, že genetické údaje budou definovány jako citlivé, a dále že budou definovány v obecném nařízení (a tedy i směrnici o vymáhání práva) jako samostatná kategorie. Článek 9 odst. 1 zařazuje „zpracování genetických údajů za účelem jedinečné identifikace fyzické osoby" do zvláštní kategorie osobních údajů, jimž je v rámci obecného nařízení přiznán zvláštní, tj. zpřísněný režim z pohledu jejich ochrany. To konkrétně znamená, že jejich použití se zakazuje, pokud se nejedná výslovně o výjimky stanovené v čl. 9 odst. 2.

K dlouhodobě závažným problémům ochrany osobních údajů v ČR patří otázky spojené se shromažďováním vzorků DNA získaných policií v souvislosti s trestnou činností osob či jejím vyšetřováním. Pro tuto oblast platí směrnice 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů (směrnice o prosazování práva). Směrnice reaguje na specifickou povahu policejní a justiční spolupráce v trestněprávních věcech a obsahuje zvláštní pravidla pro ochranu osobních údajů. Předávání osobních údajů do třetích zemí a mezi organizacemi by mělo být usnadněno při zajištění vysoké úrovně ochrany osobních údajů. Technologie, které umožňují využívat osobní údaje pro účely prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, musí být tedy doprovázeny adekvátními opatřeními.[14] Směrnice bude v ČR adaptována do vnitrostátního právního řádu prostřednictvím adaptačního zákona o zpracování osobních údajů, který dosud nebyl přijat.

Z článku 26 preambule a článku 4 směrnice vyplývají zásady zpracování osobních údajů. „Jakékoli zpracování osobních údajů musí být zákonné, korektní a transparentní ve vztahu k dotčeným fyzickým osobám a musí být prováděno pouze pro specifické účely stanovené právním předpisem. Tyto činnosti lze provádět za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost

[14] Čl. 3 a 4 směrnice o vymáhání práva.

a jejich předcházení, pokud jsou stanoveny právním předpisem a pokud jsou v demokratické společnosti s náležitým přihlédnutím k oprávněným zájmům dotčené fyzické osoby nutné a přiměřené. Fyzické osoby by měly být upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají v souvislosti s tímto zpracováním uplatňovat svá práva. Zejména je zapotřebí, aby konkrétní účely, pro které jsou osobní údaje zpracovávány, byly jednoznačné a legitimní a aby byly stanoveny v okamžiku shromažďování osobních údajů. Osobní údaje by měly být přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány. Mělo by se zajistit, aby shromažďované osobní údaje byly omezené na nezbytný rozsah a aby nebyly uchovávány déle, než je nezbytné pro účel, pro který jsou zpracovávány. Osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky. Aby se zajistilo, že údaje nebudou uchovávány déle, než je nezbytné, měl by správce stanovit lhůty pro jejich výmaz nebo pravidelný přezkum."[15]

Ke směrnici 2016/680 bylo vydáno výkladové stanovisko pracovní skupiny WP29 k některým klíčovým otázkám směrnice o prosazování práva ze dne 27. listopadu 2017, z něhož plynou některá praktická doporučení, například:

- Vnitrostátní právní předpisy o zpracování osobních údajů v oblasti působnosti směrnice by měly vždy stanovit maximální dobu uložení osobních údajů a pravidelné přezkumy potřeby uložení příslušných osobních údajů. Postup přezkumu by měl být zdokumentován a rozhodnutí o prodloužení doby uložení osobních údajů by mělo být řádně zdůvodněno.
- Na podporu dodržování zásad týkajících se kvality údajů by měla být v tomto kontextu výslovně uplatňována zásada záměrné ochrany osobních údajů. Existující a budoucí databáze by měly být organizovány/přeorganizovány tak, aby zajišťovaly automatické pravidelné přezkumy a rovněž automatický výmaz osobních údajů po dosažení maximální doby uložení.
- Posouzení potřeby dalšího uložení osobních údajů a stanovení maximální doby uložení by mělo zohledňovat různé kategorie subjektů údajů.

Lze shrnout, že vedení databáze DNA nepochybně zasahuje do práva na ochranu osobních údajů a soukromí osob a musí být přijata opatření k jejich ochraně v souladu se směrnicí. Pokud jde o situaci v ČR, žádné ustanovení zákona o Policii ČR neobsahuje výslovné zmocnění k vedení databáze DNA profilů. V zákoně o Policii ČR rovněž chybí úprava přesnějších podmínek vedení databáze, jakými je přesné vymezení lhůt uchovávání profilů v databázi, případně i podrobnější úprava likvidace osobních údajů. Podle názoru Úřadu by měl být zúžen i rozsah trestných činů, které umožňují vložení vzorku do databáze. V současné době je úprava evidencí osobních údajů pro účely identifikace v zákoně o Policii ČR velmi kusá. Možnost jejich zakládání lze dovodit až interpretací. Chybějící konkrétní lhůty pro uchovávání záznamů a přesnější podmínky výmazu jsou prozatím stanoveny v interních nařízeních policie.[16] To je opakovaně předmětem kritiky, neboť podrobnější pravidla nejsou stanovena obecně závazným a veřejnosti snadno dostupným předpisem. V uvedených otázkách by podle názoru Úřadu měla být sjednána náprava.

---

[15] Článek 26 preambule směrnice o vymáhání práva.

[16] Podrobná pravidla, na základě kterých je vedena Národní databáze DNA, jsou obsažena v závazném pokynu policejního prezidenta (ZPPP) č. 250/2014, o identifikačních úkonech. Pokyn upravuje nejen interní záležitosti Policie ČR, ale upravuje i otázky likvidace údajů a doby zpracovávání konkrétních osobních údajů. Např. je automaticky nastavena lhůta uchovávání profilu do 100 let věku osoby (čl. 68 ZPPP).

Uchovávání telekomunikačních záznamů

Telekomunikační operátoři (právnické nebo fyzické osoby zajišťující veřejnou telekomunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací) jsou v ČR povinni po dobu šesti měsíců uchovávat provozní a lokalizační údaje, které jsou zpracovávány při zajišťování jejich veřejně dostupných služeb. Provozními a lokalizačními údaji jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále zjištění data, času, způsobu a doby trvání komunikace, nikoli však jejího obsahu. Takové údaje mohou za podmínek stanovených právními předpisy požadovat zejména orgány činné v trestním řízení, Policie ČR, BIS a Vojenské zpravodajství a v některých případech ČNB. Povinnost uchovávat veškeré provozní a lokalizační údaje účastníků uložila telekomunikačním operátorům v členských zemích EU v roce 2006 směrnice, která je označována jako Data Retention.[17] Jejím účelem bylo uchovávání provozních a lokalizačních údajů z důvodu prevence trestné činnosti a boji proti ní. Tato směrnice byla přijata po teroristických útocích 11. září v reakci na zvýšenou potřebu bezpečnosti. Nicméně po vydání směrnice se objevily názory, že uchovávání telekomunikačních záznamů představuje vážný zásah do soukromí, který by měl být nastaven s mnohem větší citlivostí. To dokládají expertní materiály WP29, judikatura Soudního dvora EU i nález Ústavního soudu ČR. Zohlednění kritérií vyplývajících z níže uvedených materiálů by měla obsahovat i platná právní úprava uchovávání telekomunikačních záznamů.

Stanoviska expertní skupiny WP29 k problematice uchovávání telekomunikačních záznamů

K problematice uchovávání telekomunikačních záznamů z pohledu ochrany osobních údajů a soukromí se vyjádřily některé materiály WP29.[18] Právě WP29 ještě v době teoretických diskusí a úvah o přijetí data retention jako první upozornila[19] na potřebu vyváženého přístupu v boji proti terorismu. Konkrétně uvedla, že tato opatření mají přímý nebo nepřímý vliv na ochranu osobních údajů. Připomněla závazek demokratických společností zajistit respekt k základním právům a svobodám jednotlivce, přičemž právo jednotlivce na ochranu osobních údajů tvoří část těchto základních práv a svobod. Opatření, která jsou jednoduše „užitečná" nebo „žádaná", nesmí omezit základní práva a svobody. WP29 rovněž vyjádřila obavy z narůstající tendence označovat ochranu osobních údajů jako překážku efektivního boje proti terorismu a vyzvala k tomu, aby nebyl snížen standard lidských práv.

Další hodnocení zkoumané problematiky a návrh praktických postupů k odstranění některých rizik ve zprávě 1/2010[20] poukázalo na to, že směrnice má dalekosáhlé důsledky pro všechny evropské občany. Opatření související s rozhodnutím zavázat poskytovatele internetových a telefonních služeb uchovávat (zadržovat) provozní data všech odběratelů a poskytovatelů

---

[17] 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.

[18] Jednalo se o expertní skupinu složenou ze zástupců dozorových úřadů zabývající se ochranou osobních údajů, která je nyní nahrazena Evropským sborem pro ochranu osobních údajů.

[19] *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism (přijato 14. 12. 2001).*

[20] *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive – WP 172.*

zasahují do denního života všech evropských občanů a mohou ohrozit základní hodnoty a svobody, které požívají. Jakákoliv omezení práv jednotlivce na ochranu soukromí a osobních údajů musí být v demokratické společnosti nezbytná, vhodná a přiměřená a musí sloužit konkrétním veřejným účelům, jako je národní bezpečnost, obrana, veřejná bezpečnost nebo vyšetřování, zjišťo-vání a stíhání trestných činů. Naprosto nezbytným požadavkem je, aby taková omezení respektovala práva, svobody a zásady stanovené v Listině základních práv EU a Evropské úmluvě o ochraně lidských práv a základních svobod. Pokud jde o konkrétní záruky ve vztahu k poskytovatelům služeb, WP29 požadovala, aby byly přijaty záruky přinejmenším, pokud jde o stanovení účelu, omezení přístupu, minimalizaci dat, zákaz vytváření velkých databází k dalšímu použití, možnost soudního přezkumu oprávněnosti přístupu a zákaz jiného použití údajů provozovatelem než výlučně pro účely veřejného pořádku podle směrnice.

Citovaná zpráva dále uvedla, že dostupnost provozních a lokalizačních údajů obecně umožňuje zveřejnit preference, názory a postoje. Může také zasáhnout do soukromého života uživatelů a významně ovlivnit důvěrnost komunikace a základních práv, jako je svoboda vyjádření. Tyto scénáře mohou být pravděpodobné jak v důsledku úmyslných aktivit, tak v důsledku nedbalosti při uchovávání dat. Ve světle těchto skutečností je implementace směrnice o uchovávání osobních údajů poskytovateli elektronických komunikací a internetových služeb spojena s inherentně vysokou úrovní rizika (inherently high level of risk) vyžadující technická a organizační bezpečnostní opatření. Z výše uvedených důvodů zpráva dospěla k závěru, že je nezbytné mj. dát široké vynucovací pravomoci dozorovým úřadům na ochranu osobních údajů včetně pravomoci požadovat přístup k důvěrným obchodním informacím a zavést řadu doplňujících dílčích opatření. Bylo navrženo zvážit snížení doby uchovávání údajů, stanovit jednotné kratší období a zajistit vhodná technická a organizační opatření, která minimalizují riziko náhodných nebo neoprávněných poškození nebo změny údajů společně s rizikem neoprávněného přístupu a/nebo zpracování. Provozovatelé musí pravidelně a objektivně hodnotit rizika zpracování. Vhodné jsou také pravidelné externí audity, které přispívají k nezávislému a objektivnímu posouzení rizika.

Judikatura Ústavního soudu ČR

V ČR se k problematice uchovávání telekomunikačních záznamů vyjádřil Ústavní soud v nálezu Pl. ÚS 24/10 dne 22. března 2011,[21] ve kterém posoudil napadenou úpravu z hlediska ústavněprávních požadavků, a shledal řadu pochybení. Uvedl, že napadené ustanovení § 97 odst. 3 zákona o elektronických komunikacích obsahuje pouze vágní a neurčité stanovení povinnosti právnickým a fyzickým osobám, které provozní a lokalizační údaje uchovávají. Nemá přesně a jasně vymezen účel, za jakým jsou provozní a lokalizační údaje oprávněným orgánům poskytovány, což znemožňuje posouzení napadené právní úpravy z hlediska její potřebnosti. Napadená právní úprava nestanovuje jasná a detailní pravidla obsahující minimální požadavky na zabezpečení uchovávaných údajů, zejména v podobě zamezení přístupu třetích osob, stanovení procedury vedoucí k ochraně celistvosti a důvěrnosti údajů a postupy jejich ničení. Dále Ústavní soud napadené úpravě vytkl, že dotčení jednotlivci nedisponují dostatečnými zárukami proti riziku zneužití údajů a svévole a nejednoznačné je vymezení doby uložení údajů. Ústavní soud také

[21] http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10

vyjádřil pochybnosti nad tím, zda samotný nástroj plošného a preventivního uchovávání provozních a lokalizačních údajů o téměř veškeré elektronické komunikaci je z hlediska intenzity zásahu do soukromé sféry nezbytný. Ústavní soud proto zrušil napadená ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích, a související napadenou vyhlášku č. 485/2005 Sb.[22]

Kritéria pro data retention plynoucí z judikatury Soudního dvora EU

Rozsudek Soudního dvora EU Digital Rights Ireland (případně Tele2 Sverige AB),[23] který rozhodl o neplatnosti směrnice 2006/24/ES ve vztahu k omezení dohledu nad komunikačními daty (telefon, textové zprávy, e-mail, internetová komunikace), poukázal na hodnoty ochrany základních práv a uvedl, že směrnice 2006/24/ES představuje sama o sobě zásah do práv zaručených čl. 7 a 8 Listiny základních práv EU. Kromě toho přístup příslušných vnitrostátních orgánů k osobním údajům představuje další rozsáhlý a zvlášť závažný zásah do těchto základních práv. I když nedochází k zásahu do podstaty uvedených základních práv, protože směrnice se nevztahuje na obsah komunikace, stále se jedná o zásah do těchto práv. Okolnost, že k uchovávání údajů a jejich následnému využití dochází bez informování účastníka nebo registrovaného uživatele, může navíc v dotyčných osobách vyvolávat dojem, že jejich soukromí je pod neustálým dohledem.

Podle rozsudku je při posuzování zásahu do práv zaručených články 7 a 8 Listiny základních práv EU[24] třeba vyjít z požadavků článku 52 odst. 1 Listiny, který uvádí, že každé omezení výkonu práv a svobod zakotvených v Listině musí být stanoveno zákonem, respektovat podstatu těchto práv a svobod a omezení mohou být zakotvena při dodržení zásady proporcionality pouze tehdy, jsou-li nezbytná a odpovídají-li skutečně cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého. Co se týče otázky, zda uvedený zásah odpovídá cíli obecného zájmu, hmotněprávním cílem směrnice je přispět k boji proti závažné trestné činnosti a v konečném důsledku také k veřejné bezpečnosti. V tomto ohledu judikatura Soudního dvora EU potvrdila, že boj proti mezinárodnímu terorismu za účelem uchování mezinárodního míru a bezpečnosti a boj proti závažné trestné činnosti představují cíle obecného zájmu Unie.

Kromě splnění požadavku obecného cíle je dále třeba respektovat zásadu proporcionality, která podle ustálené judikatury Soudního dvora EU vyžaduje, aby akty unijních orgánů byly způsobilé k uskutečnění legitimních cílů sledovaných dotčenou právní úpravou a nepřekračovaly meze toho, co je přiměřené a nezbytné k dosažení legitimních cílů. Pokud jde o požadavek

---

[22] Ke změně zákona o elektronických komunikacích na základě nálezu Ústavního soudu došlo na základě novely č. 468/2011 Sb. Nálezu Ústavního soudu předcházel rozsudek Soudního dvora EU Digital Rights Ireland.

[23] Rozsudek Soudního dvora EU ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12 Digital Rights Ireland Ltd. a rozsudek Soudního dvora EU ze dne 21. prosince 2016 ve spojených věcech C-203/15 a C-698/15 Tele2 Sverige AB."

[24] Článek 7 Listiny základních práv EU Respektování soukromého a rodinného života zní: Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.
Článek 8 Listiny základních práv EU Ochrana osobních údajů zní:
1. Každý má právo na ochranu osobních údajů, které se ho týkají.
2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.
3. Na dodržování těchto pravidel dohlíží nezávislý orgán.

omezení zásahu do základních práv na nezbytné minimum, směrnice 2006/24/ES těmto požadavkům v mnoha ohledech nevyhověla, jak to uvedl rozsudek Soudního dvora EU, například:

- Směrnice nevyžadovala žádnou souvislost mezi údaji, jejichž uchovávání bylo stanoveno, a ohrožením veřejné bezpečnosti, a neomezila uchovávání údajů na určité časové období, určitou zeměpisnou oblast či okruh osob, které mohly být zapojeny do závažné trestné činnosti;
- nestanovila žádné objektivní kritérium pro přístup příslušných vnitrostátních orgánů k údajům a jejich následné využití pro účely předcházení, odhalování nebo stíhání trestných činů;
- neobsahovala hmotněprávní a procesní podmínky pro přístup příslušných vnitrostátních orgánů k údajům a jejich následné využití;
- nestanovila objektivní kritéria umožňující omezit na nezbytné minimum z hlediska sledovaného cíle počet osob, které měly oprávnění k přístupu a následnému využití uchovávaných údajů;
- přístup příslušných vnitrostátních orgánů k uchovávaným údajům nepodléhal předchozí kontrole ze strany soudu nebo nezávislého správního orgánu;
- doba uchovávání údajů nerozlišovala mezi jednotlivými kategoriemi údajů uvedenými v článku 5 směrnice podle jejich případné užitečnosti pro účely sledovaného cíle nebo podle dotčených osob;
- uchovávání nebylo založeno na objektivních kritériích tak, aby bylo omezeno na nezbytné minimum;
- nebyly stanoveny dostatečné záruky k zajištění účinné ochrany údajů proti riziku zneužití ani proti neoprávněnému přistupování k údajům a jejich protiprávnímu využívání, které vyžaduje článek 8 Listiny, a nebyla stanovena povinnost členských států zavést taková pravidla;
- nebyla zaručeno, aby poskytovatelé přijali technická a organizační opatření za účelem dosažení vysoké úrovně ochrany a bezpečnosti;
- nebyla zaručena likvidace údajů po skončení doby jejich uchovávání.

Z výše uvedeného přehledu nedostatků směrnice 2006/24/ES vyplývá, že nebyla stanovena jasná a přesná pravidla pro rozsah zásahu do základních práv na ochranu osobních údajů a soukromí a že směrnice představovala rozsáhlý a zvlášť závažný zásah do základních práv v unijním právním řádu, aniž by takový zásah byl omezen na nezbytné minimum. Přijetím směrnice 2006/24/ES byly tedy překročeny meze, jež ukládá požadavek na dodržování zásady proporcionality z hlediska článků 7 a 8 a čl. 52 odst. 1 Listiny, což vedlo k závěru o neplatnosti posuzované směrnice. Důvody neplatnosti směrnice by přirozeně měly být zváženy i při posuzování vnitrostátních právních předpisů členských států EU, které byly přijaty na jejím základě.[25]

[25] Návrh Ústavního soudu Pl. ÚS 45/17 na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, návrh na zrušení § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, návrh na zrušení § 88a zákona č. 141/1961 Sb., trestního řádu, ve znění pozdějších předpisů, návrh na zrušení vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

Legislativa

Vláda získala důvěru 12. července 2018 a legislativní proces se tím vrátil do standardní podoby. Stále se však spíše upřednostňují novely před věcnými záměry a novými zákony. Názvy novel jsou v řadě případů formální, místo toho, aby vyjadřovaly, čeho se týkají. Vláda požádala Úřad o stanovisko k iniciativním, obvykle poslaneckým, návrhům zákonů spíše ojediněle. Rada Evropské unie v roce 2018 zpřístupnila celkem 284 dokumentů týkajících se ochrany osobních údajů z 15 836 celkem.

Vyhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

(DPIA) je povinnou součástí důvodových zpráv nebo odůvodnění od 1. ledna 2013, což se aktualizuje článkem 35 obecného nařízení. Přes nové požadavky na kvalitu DPIA dané v obecném nařízení[26] bohužel ani po pěti letech stále ještě není jeho podoba optimální. Úřad proto připravil návod, v němž vysvětluje, jak má DPIA v legislativě vypadat.[27] Kladně lze hodnotit zpravidla ta vyhodnocení, kde si předkladatel přizval k jejich tvorbě svého pověřence pro ochranu osobních údajů.

Implementace nového unijního regulačního rámce

V roce 2018 se Úřad věnoval rovněž implementaci nového unijního regulačního rámce ochrany osobních údajů (obecné nařízení, JHAD[28] & PNRD[29]). Návrh

[26] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

[27] https://www.uoou.cz/navod-k-posouzeni-vlivu-na-ochranu-osobnich-udaju-u-navrhu-pravnich-predpisu-dpia/ds-5344

[28] 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.

[29] 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.

zákona o zpracování osobních údajů a doprovodného zákona byl značně opožděn. Teprve 21. března 2018 jej schválila vláda a od té doby jej celý zbytek roku projednávala poslanecká sněmovna.

K iniciativnímu návrhu novely stávajícího zákona o zpracování osobních údajů poskytl Úřad vládě obsáhlé stanovisko, v němž především upozornil na nesystémovost vynětí celé územní samosprávy ze správního trestání obecného nařízení. Poslanci posléze návrh stáhli z projednávání.

Elektronická veřejná správa

Největší aktualitou bylo praktické naplňování eIDAS[30] a zákona č. 250/2017 Sb., o elektronické identifikaci. To se promítlo jako spuštění NIA (https://www.eidentita.cz) a Portálu občana (https://obcan.portal.gov.cz). Úřad podpořil ukončení uvádění rodných čísel na občanských průkazech. Ministerstvo vnitra chce e-government rozvíjet koncepcí Registry 2.0.

Otázku elektronické identifikace Úřad řešil rovněž s Českým úřadem zeměměřickým a katastrálním a ministerstvem zdravotnictví. Již od počátku roku 2018 Státní ústav pro kontrolu léčiv umožňuje každému pacientovi nahlédnout na svůj lékový záznam. Návrh zákona jej zpřístupňuje též lékařům se zárukami ochrany osobních údajů.

Zásadní změnu zdravotnictví má přinést návrh věcného záměru zákona o elektronickém zdravotnictví (angl. *eHealth*). Jeho podstatou je indexace zdravotnické dokumentace a reforma registrů NZIS.

Soukromé právo

Ministerstvo spravedlnosti připravilo návrh novely nového občanského zákoníku, která má umožnit změnu pohlaví bez chirurgického zákroku. Úřad ji odmítl jako celek pro předčasnost a nepromyšlenost. Ministerstvo spravedlnosti rovněž navrhlo rozsáhlou změnu zákona o obchodních korporacích, která byla v roce 2018 projednávána jako sněmovní tisk 207.

Transparentnost

Vláda požádala Úřad o vyjádření k iniciativnímu návrhu na částečnou transpozici 4. AML[31] směrnice ve znění 5AMLD[32], jímž se mají zveřejnit koncoví vlastníci – sněmovní tisk 318. Úřad vládě doporučil s návrhem nesouhlasit, zejména pro nedostatečné DPIA a absenci více záruk ochrany soukromí z preambule 5AMLD; tedy nedostatečnou ochranu osobních údajů. Vláda k němu zaujala neutrální stanovisko.

Soukromí v elektronických komunikacích

Návrh nařízení o respektování soukromého života a ochrany osobních údajů v elektronických komunikacích (CELEX[33]: 52017PC0010) by měl nahradit stávající směrnici 2002/58/ES. Nejspornějšími otázkami tohoto návrhu jsou zadržování údajů, zpracování metadat a obsahu

---

30 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

31 Praní špinavých peněz.

32 SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU.

33 Communitatis Europeae Lex

elektronických komunikací, *cookie walls*, nastavení prohlížečů či vztah k obecnému nařízení. Vzhledem k politicky citlivému obsahu a dopadu tohoto návrhu na další sektory se rakouské předsednictví EU rozhodlo, že nepokročí do další fáze, trialogu s Evropským parlamentem a Evropskou komisí. Na prosincové Radě pro telekomunikace byla schválena pouze zpráva o pokroku. Kvůli mnoha nevyřešeným otázkám se nepředpokládá, že by návrh byl schválen do konce volebního období Evropského parlamentu.

K vývoji rovněž dochází na poli umělé inteligence a blockchainu, tedy technologií, které mají dopad na základní lidská práva, jako je ochrana soukromí a ochrana osobních údajů.

Dezinformační kampaň

Návrh nařízení Evropského parlamentu a Rady EU, kterým se mění nařízení (EU, Euratom) č. 1141/2014, pokud jde o postup ověřování v případě porušení pravidel ochrany osobních údajů v souvislosti s volbami do Evropského parlamentu, má za cíl zlepšit ochranu před kybernetickými bezpečnostními incidenty a v boji proti dezinformačním kampaním v souvislosti s volbami do Evropského parlamentu v květnu roku 2019.

Směrnice Evropského parlamentu a Rady EU 2013/40/EU harmonizovala definici trestných činů a upravila minimální a maximální výši sankcí v souvislosti s útoky proti informačním systémům. V této souvislosti stanovila, že útoky proti informačním systémům jsou zvlášť přitěžující okolností.

Evropská komise zároveň doporučuje, aby každý členský stát zřídil vnitrostátní volební síť. Ta by zahrnovala veškeré orgány, jež se věnují monitorování on-line činností. Takové opatření by usnadnilo výměnu informací a zároveň umožnilo sdílet poznatky a prosazovat pravidla. V závěru roku byl Úřad osloven s žádostí o účast na činnosti této sítě.

Volný tok neosobních dat

Po obecném přístupu Rady EU schválil na začátku října 2018 Evropský parlament nařízení o volném pohybu neosobních dat. To má pomoci vytvořit konkurenceschopnou ekonomiku, založenou na datech v rámci jednotného digitálního trhu. Zároveň také zajistí volný pohyb údajů přes hranice. Členské státy budou mít povinnost oznámit Evropské komisi veškerá zbývající nebo plánovaná omezení týkající se lokalizace dat v rámci vymezených konkrétních situací při zpracování údajů veřejnými úřady. Toto nařízení bude doplňovat obecné nařízení s cílem umožnit volný pohyb veškerých údajů (osobních i jiných) a tím vytvořit jednotný evropský datový prostor.

Vyřizování stížností podle § 175 správního řádu

Správní řád umožňuje těm, kteří nejsou spokojeni s výstupy správních orgánů včetně Úřadu pro ochranu osobních údajů, podat stížnost podle § 175 správního řádu.[34] Konkrétně se mohou dotčené osoby obracet na správní orgány se stížnostmi proti nevhodnému chování úředních osob nebo proti postupu správního orgánu. Takovou možnost mají stěžovatelé v případě, neposkytuje-li jim správní řád jiné prostředky ochrany, tj. zejména odvolání nebo další řádné či mimořádné opravné prostředky.

Úřad se v roce 2018 zabýval celkem dvanácti stížnostmi podanými na základě § 175 zákona č. 500/2004 Sb. Ve většině případů byli stěžovatelé nespokojeni s vyřízením jejich předchozího podnětu týkajícího se možného porušení právních předpisů v oblasti ochrany osobních údajů. V loňském roce byly z celkového počtu dvanácti stížností pouze dvě posouzeny jako důvodné a sedm bylo shledáno bezdůvodnými. Třemi stížnostmi, které Úřad obdržel na konci roku 2018, se bude zabývat v roce 2019.

I přes skutečnost, že v souvislosti s účinností obecného nařízení Úřad celkově zaznamenal výrazný nárůst počtu stížností směřovaných proti správcům či zpracovatelům osobních údajů, počet stížností podle § 175 oproti minulému roku klesl.

Pokud se budeme jednotlivými stížnostmi zabývat podrobněji, v deseti případech stížnosti směřovaly proti postupu odboru konzultačních agend, který metodicky řídí stížnostní a konzultační agendu. Stěžovatelé podali převážnou většinu stížností z důvodu jejich nesouhlasu s vyřízením předchozího podnětu, který odbor konzultačních agend odložil bez dalších opatření. V těchto případech byl prošetřen způsob vyřízení předchozího podnětu stěžovatele. V jednom případě stěžovatel opětovně nesouhlasil s vyřízením stížnosti a obrátil se na předsedkyni Úřadu. I v tomto případě byl předchozí postup Úřadu shledán oprávněným a stížnost byla vyhodnocena jako bezdůvodná. V situaci, kdy po přezkoumání podnětu stěžovatele bylo shledáno podezření z porušení zákona

[34] Zákon č. 500/2004 Sb. ze dne 24. června 2004, správní řád.

č. 101/2000 Sb. či obecného nařízení, následovalo postoupení podnětu buď inspektorovi Úřadu k provedení kontroly, nebo kontrolnímu odboru k zahájení správního řízení pro podezření ze spáchání správního deliktu či přestupku. Ve dvou případech se stěžovatelé obrátili na Úřad se stížností proti závěrům jeho kontrolních postupů nebo postupu při vedení kontroly inspektory Úřadu. V obou případech byly tyto stížnosti vyhodnoceny jako bezdůvodné.

Ve všech výše uvedených případech byl stěžovatel informován o výsledku šetření. Rovněž příslušný odbor Úřadu byl informován o vyřízení stížnosti.

Z počtu dvanácti podnětů, které Úřad obdržel od stěžovatelů, žádný nesměřoval proti nevhodnému chování úředních osob. Celkově lze konstatovat, že Úřad při výkonu svěřené činnosti postupuje profesionálně, zodpovědně a v souladu s principy dobré správy.

Zahraniční spolupráce

Během posledních let se postupně rozšiřoval akční záběr Úřadu na poli dnes už bývalé pracovní skupiny WP29. V uplynulém roce se tento trend skokově prohloubil a podíl na činnosti nově ustaveného Evropského sboru pro ochranu osobních údajů (dříve WP29) doznal kvalitativní změny. Pracovníci Úřadu se ve čtyřech případech stali členy návrhové skupiny, konkrétně u těchto úkolů:

- Analýza seznamů podle článku 35(4) předaných Sboru – seznamy druhů operací zpracování podléhajících požadavku na posouzení vlivu na ochranu osobních údajů.

Na základě článku 35 obecného nařízení[35] připravil Úřad návrh seznamu druhů operací, které podléhají posouzení vlivu na ochranu osobních údajů. V únoru a březnu roku 2018 proběhla veřejná diskuse k navrženému seznamu a v červnu byl návrh seznamu zaslán Evropskému sboru pro ochranu osobních údajů. Zároveň se Úřad přihlásil ke spolupráci na analýze seznamů zaslaných jednotlivými členskými státy.

Analýza prvních 23 seznamů probíhala v červenci a srpnu a výsledkem byl návrh stanovisek připravený pro plenární zasedání Sboru v září 2018. Sbor na svém zasedání stanoviska schválil a předložil je v rámci zajištění mechanismu jednotnosti k vypořádání jednotlivým členským státům. Hodnocení dalších seznamů (včetně Norska a Lichtenštejnska, které jsou členy EHS) probíhalo ještě v říjnu a listopadu roku 2018. Úřad připravil vypořádání připomínek a návrhů uvedených v rámci stanoviska k jím připravenému seznamu a zaslal upravený dokument zpět Sboru s tím, že předběžný návrh stanoviska ukazuje na dostatečnost provedených úprav, a seznam je tedy vyhovující. Po definitivním schválení Sborem se předpokládá zveřejnění seznamu na webových stránkách Úřadu.

- Příprava pokynů ke kamerovému sledování.

Evropský sbor pro ochranu osobních údajů přistoupil k práci na dalším z řady pokynů zaměřených na praktický a tematicky zaměřený výklad ustanovení obecného nařízení, tentokrát v oblasti monitorování prostřednictvím kamerových systémů. Úřad se stal členem řešitelského týmu. Vedle teoretických

[35] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

východisek, tj. vysvětlení rozsahu aplikace obecného nařízení a právního základu, bude dokument zaměřen prakticky pro potřeby zejména uživatelů kamerových systémů, ale také pro informaci jednotlivcům coby subjektům údajů. Na sérii příkladů z praktického života budou vysvětleny důležité aspekty jako předávání záznamů třetím stranám, transparentnost a informační povinnost, doba uchovávání záznamů a povinnost jejich výmazu, technická opatření nebo zpracování zvláštních kategorií osobních údajů.

- Příprava stanoviska k návrhu rozhodnutí Komise o odpovídající ochraně osobních údajů v Japonsku.

Evropská komise požádala Evropský sbor pro ochranu osobních údajů o stanovisko k chystanému rozhodnutí konstatujícímu, že Japonsko poskytuje ochranu osobních dat na úrovni odpovídající současnému standardu EU. Úřad se přihlásil ke spolupráci na formulaci tohoto stanoviska, zúčastnil se konzultací se zástupci Komise, se zástupci japonského dozorového úřadu pro ochranu osobních údajů a mnoha osobních setkání a telekonferencí úzkého pracovního týmu. Úkol vypracovat takové stanovisko vyplývá z čl. 70 odst. 1 písm. s) obecného nařízení. V případě Japonska šlo přitom o úkol o to zodpovědnější, neboť se jednalo o první takové rozhodnutí Komise v režimu obecného nařízení, které nastaví standardy v aplikaci čl. 45 obecného nařízení nejen pro práci Komise a pro hodnocení dozorových úřadů, ale i pro přístup třetích zemí, jež projeví zájem o konvergenci s evropským systémem ochrany osobních údajů.

- Posouzení dokumentu Otázky a odpovědi ohledně vzájemného vztahu mezi nařízením o klinických hodnoceních (EU 536/2014) a obecným nařízením.

Evropská komise požádala Sbor o odborný posudek a radu v zájmu konzistentního přístupu k ochraně osobních údajů v této oblasti. Celkem má Úřad přímé pracovní zastoupení v šesti podskupinách Sboru:

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

V roce 2019 Úřad plánuje vysílat delegáty do dalších dvou podskupin se zaměřením na finanční tematiku, respektive na otázky praktického prosazování práva (kontrolní a dozorová činnost).

Účinnost obecného nařízení se promítla také do dalších oblastí činnosti. Došlo například k nárůstu počtu případů s mezistátním přesahem, které Úřad řeší většinou v roli dotčeného dozorového úřadu, ale i v postavení vedoucího dozorového úřadu.

Úřad začal přijímat a evidovat oznámení o porušení zabezpečení osobních údajů podle článku 33 obecného nařízení. Podrobnější informace jsou k dispozici v kapitole „Stížnosti, ohlašování porušení zabezpečení a konzultace".

Pracovníci Úřadu vycestovali na každoročně pořádané konference a semináře, např. na tzv. jarní konferenci komisařů ochrany dat (s celoevropskou účastí) nebo na mezinárodní konferenci komisařů ochrany dat a soukromí (s celosvětovou účastí). Účast na jiných konferencích a seminářích byla omezena ve prospěch cest na zasedání pracovních formací Sboru.

• KODEXY CHOVÁNÍ

Obecné nařízení[36] v článcích 40 a 41 upravuje problematiku přípravy a monitorování kodexů chování, jakožto nového samoregulačního mechanismu. Ten poskytuje subjektům v daném odvětví příležitost dohodnout se společně na konkrétních a praktických pravidlech při zpracování osobních údajů v daném odvětví, která budou splňovat požadavky nařízení.

Kodex chování by měl definovat základní zásady, organizaci, postupy a požadavky na zpracování osobních údajů natolik konkrétně a jednoznačně, aby se podle něj mohl řídit daný správce či zpracovatel. Zároveň by podle něj mohl dělat svoji práci i subjekt provádějící monitorování kodexu chování.

PRVNÍ ZKUŠENOSTI A POZNATKY ÚŘADU

V roce 2018 zaznamenal Úřad ze strany správců a zpracovatelů velký zájem řešit shodu s obecným nařízením právě prostřednictvím kodexů chování. Narůstající zájem z různých odvětví i předčasné zasílání návrhů kodexů chování k posouzení vedl Úřad k vydání metodiky ke kodexům zveřejněné na webových stránkách Úřadu, ve které jsou široké veřejnosti poskytnuty základní informace a postupy pro zpracovatele kodexu.

Úřad v roce 2018 obdržel osm návrhů kodexů chování nebo poskytl konzultaci k jejich přípravě či monitorování. Jeden ze subjektů se dokonce rozhodl svůj „kodex chování" uveřejnit na svých webových stránkách. Na základě výzvy daného subjektu se k němu přihlásilo přibližně 50 dalších, a to přesto, že nebyl Úřadem schválen a není akreditován žádný subjekt určený pro jeho monitorování, tedy nebyly splněny základní požadavky, aby kodex mohl sloužit k prokázání souladu s obecným nařízením. Úřad upozornil daný subjekt, že takový postup je v rozporu s obecným nařízením a vyzval ho dopisem k nápravě.

Základní poznatky z jednání s předkladateli kodexů lze zobecnit následovně:

- návrh kodexu je cílen na malou skupinu správců (problematické monitorování, resp. ekonomické parametry takové činnosti) a někdy ignoruje další správce s obdobným nebo totožným charakterem zpracování osobních údajů,
- návrh kodexu obsahuje ve velké většině přepis ustanovení obecného nařízení, má tedy zanedbatelnou přidanou hodnotu vůči obecnému nařízení, čímž nesplňuje požadavky kodexu,
- zpracovatel kodexu (a jeho správce) požaduje po správcích činnosti, na které nemá dle nařízení právo,
- chybí dostatečná analýza a zdůvodnění přípravy a obsahu kodexu,
- chybí doložení proběhlých jednání nezbytných před zahájením tvorby kodexu, která dokládají, že na zpracování kodexu, jeho obsahu a jeho zpracovateli panuje širší shoda v rámci daného odvětví.

[36] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

ROLE EVROPSKÉHO SBORU

Významná úloha při uplatňování obecného nařízení v oblasti kodexů chování připadá Evropskému sboru pro ochranu osobních údajů, který připravuje metodické návody (Guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679) a také koordinuje zajištění jednotného výkladu (schvalování akreditačních kritérií a některých kodexů chování). Proto je nutné vyčkat na dokončení výše uvedených návodů a až poté začít zakládat celý systém přípravy a monitorování kodexů. Sladění s připravovanými vodítky je nezbytně nutné, aby nedocházelo k vytváření návrhů, které nemohou být schváleny, a k nežádoucím změnám v podmínkách akreditací subjektů pro monitorování kodexů a struktuře kodexů chování.

MONITOROVÁNÍ SCHVÁLENÝCH KODEXŮ CHOVÁNÍ

Každý kodex musí být před svým publikováním nejdříve nejen schválen ze strany Úřadu, ale musí být navíc opatřený závazkem subjektu (správce nebo zpracovatele) k dodržování v kodexu popsaných postupů a závazkem podrobení se monitorování dodržování kodexu ze strany nezávislého subjektu. Obecné nařízení počítá s tím, že dodržování kodexu chování bude monitorováno dozorovým úřadem, případně subjektem akreditovaným dozorovým úřadem.

Příprava požadavků pro akreditaci subjektů pro monitorování kodexů chování není krátkodobý proces. Obecně lze předpokládat, že kromě obecných požadavků (nestrannost, kvalita, bezdlužnost, čistý trestní rejstřík), požadavků na odbornost v oblasti bezpečnosti a ochrany osobních údajů, budou formulovány i požadavky na odbornost týkající se činnosti dané skupiny správců či zpracovatelů (znalost právních předpisů např. v oblasti zdravotnictví apod.). Systém monitorování schválených kodexů chování bude jistě ještě předmětem debat v rámci Evropy. Do té doby nelze prozatím žádat Úřad o akreditaci.

ÚKOLY ÚŘADU

Úkoly Úřadu spojené s agendou kodexů chování zahrnují dvě základní roviny:

- Úřad provádí schvalování kodexů chování – čl. 40 nařízení.
- Úřad musí zajistit monitorování kodexů (buď ve vlastní režii, nebo prostřednictvím třetího subjektu, který pro tuto činnost Úřad akredituje) – čl. 41 nařízení.

Úkoly související se zaváděním nového institutu kodexů do praxe jsou poměrně rozsáhlé. Budou vyžadovat i velké nároky na čas, finanční prostředky a na odbornou erudici posuzujících zaměstnanců Úřadu. Předpokládá vytvoření odborného zázemí pro provádění činností spojených s akreditacemi (zpracování akreditačních kritérií, komunikace se Sborem, vlastní akreditace, kontrola akreditovaných subjektů) a některých činností souvisejících se zpracováním kodexů chování (konzultace, vydání stanoviska ke kodexu, schválení kodexu, uveřejnění kodexu, zaslání kodexu Sboru ve stanovených případech).

Sdělovací prostředky a komunikační nástroje

Mediálně představovalo v roce 2018 ústřední komunikační bod květnové nabytí účinnosti obecného nařízení o ochraně osobních údajů.[37] Kromě tohoto byla pozornost médií zaměřena na legislativní proces týkající se příslušné adaptační legislativy, resp. zákona o zpracování osobních údajů.

Novináři se ve stále vyšší míře dotazovali na témata spojená s možnými sankcemi plynoucími z obecného nařízení, ale také na případné omezení vlastní činnosti, které bez příslušné adaptační legislativy podle nich mělo nastat.

V menší míře s ohledem na téma obecného nařízení sklidil pozornost mezinárodní Den ochrany osobních údajů, v jehož rámci poskytli několik mediálních výstupů zástupci Úřadu.

Stejně jako o rok dříve se i v roce 2018 Úřad připojil k oslavám Dne bezpečnějšího internetu s jednoznačným cílem podpory bezpečnějšího internetu a odpovědnějšího chování na síti.

V průběhu roku pokračoval Úřad ve své informační činnosti s cílem zvýšit povědomí a zájem o oblast ochrany osobních údajů. Obdobně se soustředil na témata spojená s účinností obecného nařízení. I nadále vytvářel a uveřejňoval své vlastní neoficiální překlady materiálů skupiny WP29 s cílem veřejnosti přiblížit jednotlivé části nařízení. V průběhu roku vypracoval nové informační materiály pro laickou veřejnost ke zmíněnému tématu. Ve výrazně zvýšené míře poskytoval konzultační činnost ať již přímo v sídle Úřadu, elektronicky či prostřednictvím speciálně vytvořené GDPR telefonní linky, která byla k dispozici od pondělí do pátku.

V rámci informační kampaně přednášeli odborníci Úřadu v roce 2018 na téměř 90 akcích, odborných konferencích a seminářích. Úřad navíc uspořádal

[37] Obecné nařízení o ochraně osobních údajů, též GDPR z anglických slov General Data Protection Regulation (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).

ve svých prostorách sedm setkání s pověřenci, jejichž účelem bylo předat účastníkům nejnovější poznatky z praxe.

Celkově lze konstatovat, že rok 2018 se mediálně výrazně lišil od předchozích let. Novinářská obec se vyjma obecného nařízení zajímala ve zvýšené míře zejména o kauzy typu uniklých dat klientů internetového obchodního domu Mall či Českou poštou chybně odeslané výzvy k zaplacení pokut za dopravní přestupky. Úřad také musel často reagovat na některé zavádějící až chybné informace, které se v médiích neustále opakovaly v souvislosti s obecným nařízením.

Úřad se v roce 2018 plně zapojil do příprav a průběhu Středoškolské soutěže ČR v kybernetické bezpečnosti, jejímž cílem bylo prověřit znalosti a dovednosti studentů v oblasti bezpečnosti v kyberprostoru. Do soutěže se přihlásilo téměř devět desítek středních škol a zúčastnilo se jí tři tisíce studentů.

MEDIÁLNÍ OBRAZ

Novináři ve svých článcích a reportážích nebyli vůči Úřadu nijak zásadně vymezeni a omezili se většinou na konstatování, že subjekty porušující obecné nařízení mohou dostat i novou maximální možnou sankci.

I v roce 2018 Úřad opakovaně médiím zdůrazňoval, že je nutné ctít zásadu, kdy se každý může přiměřeným způsobem domoci svého práva, pokud bylo zasaženo do jeho zákonem chráněných zájmů. Novináři již tento přístup Úřadu plně akceptovali a pravidelně jej připomínají ve svých výstupech u jednotlivých zveřejněných případů.

KNIHOVNA

Knihovna Úřadu disponuje 2500 svazky, což činí meziroční nárůst o 100 svazků ve srovnání s rokem 2017, z toho šest bylo obdrženo darem. Knihovna i přes obtížnější situaci způsobenou naplánovanou rekonstrukcí plnila svou standardní funkci skládající se ze dvou pilířů – zázemí pro zaměstnance a zdroj odborné literatury pro veřejnost. Dle schváleného plánu byla přesunuta knihovna do samostatných více vyhovujících prostor v přízemí.

WEBOVÉ STRÁNKY

Webové stránky představují i nadále primární komunikační kanál, prostřednictvím kterého může Úřad nejefektivněji informovat o své činnosti a novinkách z oblasti ochrany osobních údajů. Dominujícím tématem na webu Úřadu bylo v roce 2018 vcelku očekávaně obecné nařízení. Úřad výrazně zasáhl do struktury webu, přidal některé rubriky a celkově zvýšil přehlednost své internetové prezentace tak, aby se k nejdůležitějším informacím návštěvník dostal co nejrychleji. Rubriku GDPR (obecné nařízení), která byla umístěna na první pozici v navigačním menu, zpřístupnil v podobě jednotlivých rubrik také v pravém navigačním sloupci. V návaznosti na zmíněné vytvořil také speciální webovou mikrostránku o obecném nařízení pro širokou laickou veřejnost, která má zájem dozvědět se více o obecném nařízení. Na titulní stranu hlavního webu byl rovněž umístěn odkaz na GDPR linku s cílem více propagovat tento nový komunikační kanál.

Informační systém ORG

Systém ORG, který provozuje a udržuje Úřad, je součástí systému základních registrů. Od července 2012 systém základních registrů shromažďuje a uchovává základní informace o fyzických osobách. Základní registry veřejné správy představují jeden z klíčových pilířů rozvíjejícího se českého e-governmentu, tj. procesu elektronizace a efektivizace veřejné správy. Orgány veřejné moci, občané a další subjekty již v současné době berou systém základních registrů České republiky jako součást moderního fungování veřejné správy.

Základní registry obsahují mimo jiné referenční údaje o občanech, právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci a zjednodušují tak komunikaci občanů s úřady.

V roce 2014 byl přijat zákon č. 181/2014 Sb., o kybernetické bezpečnosti a informační systém ORG, coby součást e-governmentu, byl označen jako informační systém kritické infrastruktury. Správce takového informačního systému je povinen plnit technická opatření stanovená ve vyhlášce 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.

Informační systém ORG je naprosto nezbytnou bezpečnostně-technickou komponentou základních registrů. Dá se říct, že jednotlivé systémy základních registrů jsou od sebe odděleny, ale přes informační systém ORG je lze propojit. Každý den je využíván státní správou. Porucha nebo dlouhodobá odstávka by znamenala značné omezení chodu mnoha úřadů a organizací. Jednotlivé registry by se staly, v případě nečinnosti ORG, pouze seznamy s nic neříkajícím obsahem. Další financování informačního systému ORG vyplývá z usnesení vlády č. 411 ze dne 31. května 2017.

Vyhovět požadavkům kladeným na systém kritické infrastruktury vyžaduje neustálé zdokonalování a zavádění nových ochranných prvků, jak v propojení jednotlivých částí systému, tak v neustálém dohledu nad chodem systému. Zdokonalována je i ochrana samotného pracoviště zaměstnanců Úřadu, kteří dozor nad chodem systému provádějí.

Od roku 2012 byl systém po stránce HW udržován pouze formou výměny poškozených částí (disky, zdroje apod.) za nové. Dnes se ukazuje, že je již

technicky i morálně překonaný a zastaralý. Proto je třeba uvažovat nad jeho obměnou. Podobně i SW potřebuje instalovat například nové verze zabezpečení či databáze.

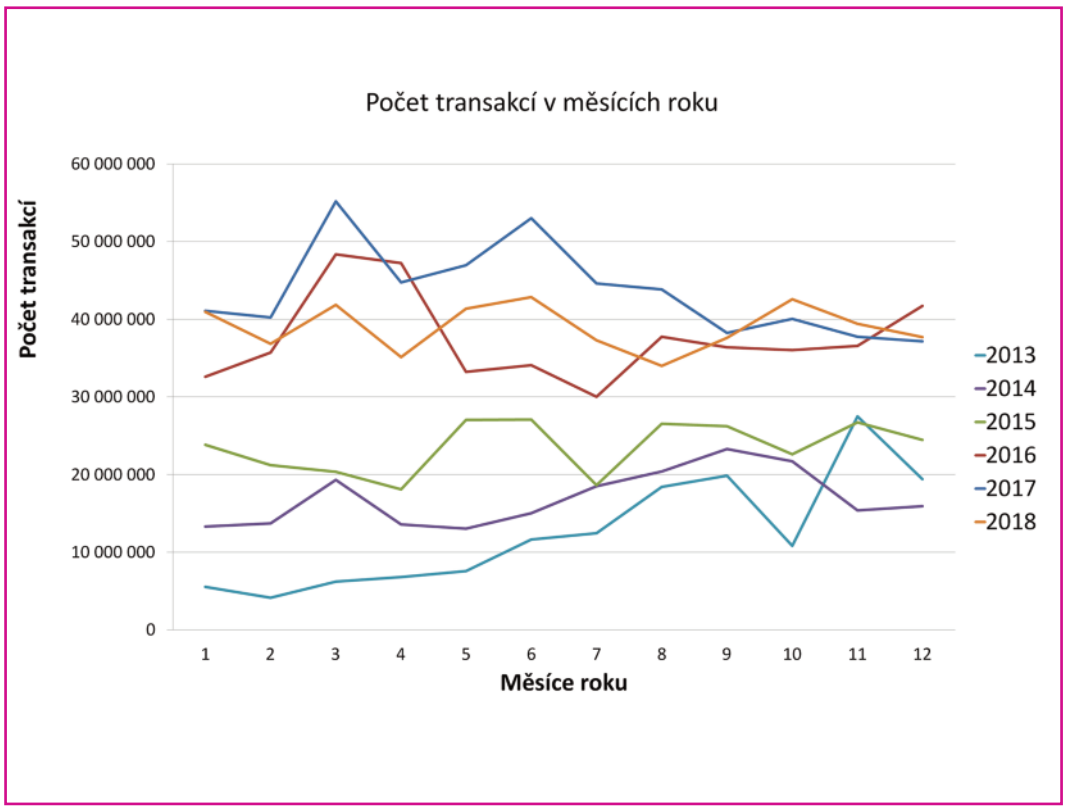
Vznik systému a jeho provoz během prvních pěti let byl částečně financován z prostředků poskytnutých EU v rámci podpory „Rozvoj informační společnosti ve veřejné správě".

Pro zajištění nutného chodu a rozvoje v nejbližší budoucnosti předpokládáme zajištění těchto podmínek:

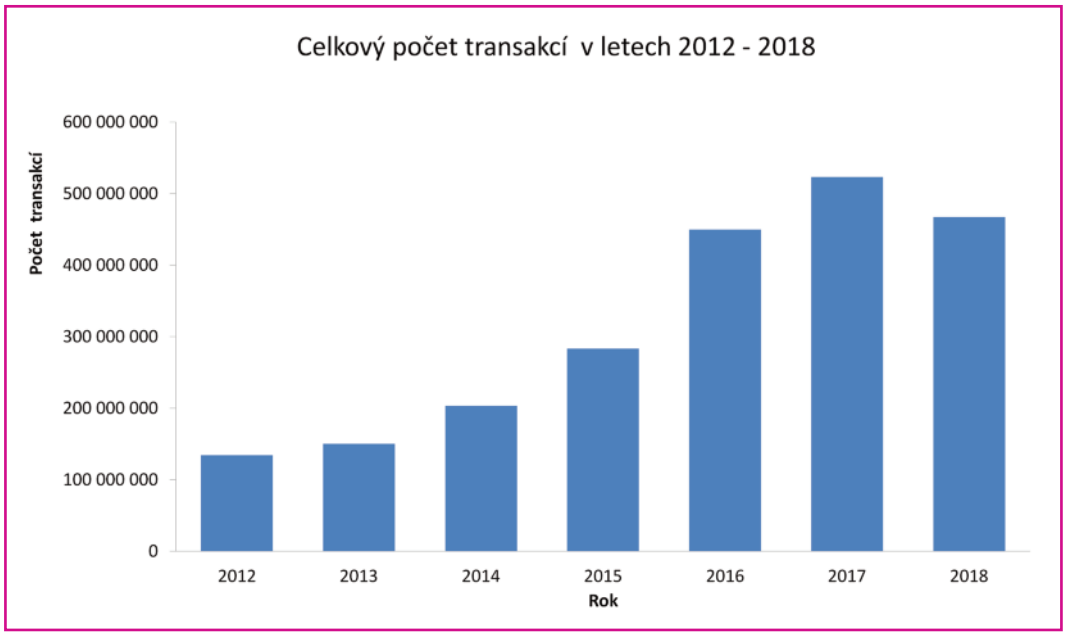
- pokračování transformačního projektu řešícího obnovu a rozvoj základních registrů veřejné správy a návazných systémů,
- provoz ZR za stávajících úrovní poskytovaných služeb (SLA),
- provoz ZR pouze na výrobcem certifikovaném HW a SW,
- roční 20% nárůst zatížení ZR do roku 2021.

Další výzvou bude také zajištění kybernetické bezpečnosti – v původním konceptu projektu základních registrů totiž nebylo počítáno se zákonem o kybernetické bezpečnosti.

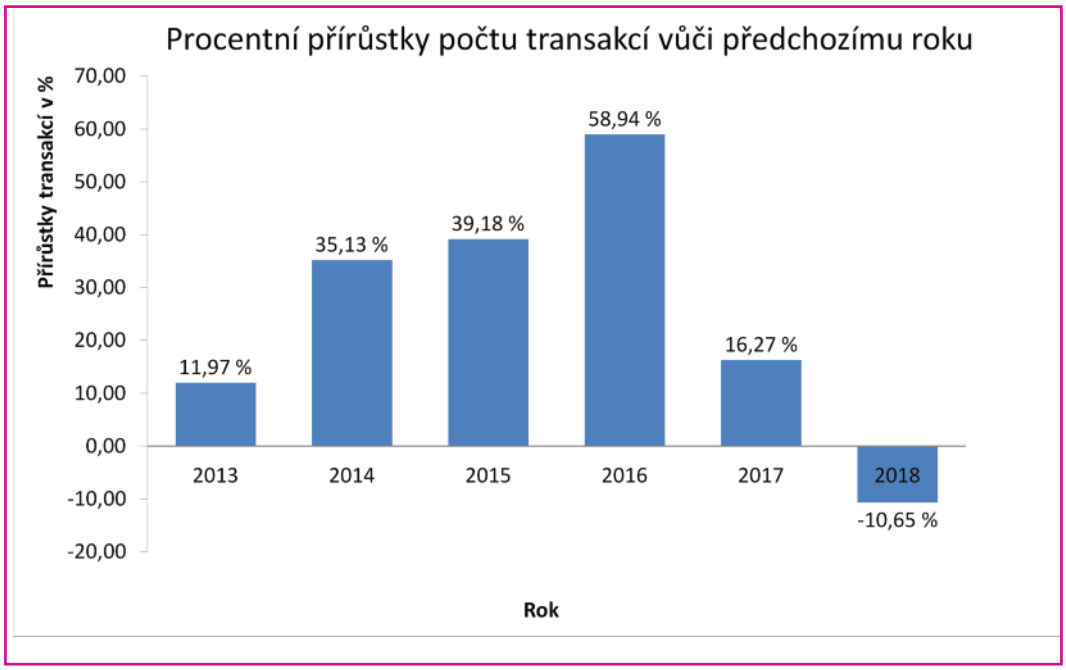
Graf „Počet transakcí v měsících roku" zobrazuje průběh počtu transakcí v jednotlivých letech a měsících od roku 2013.



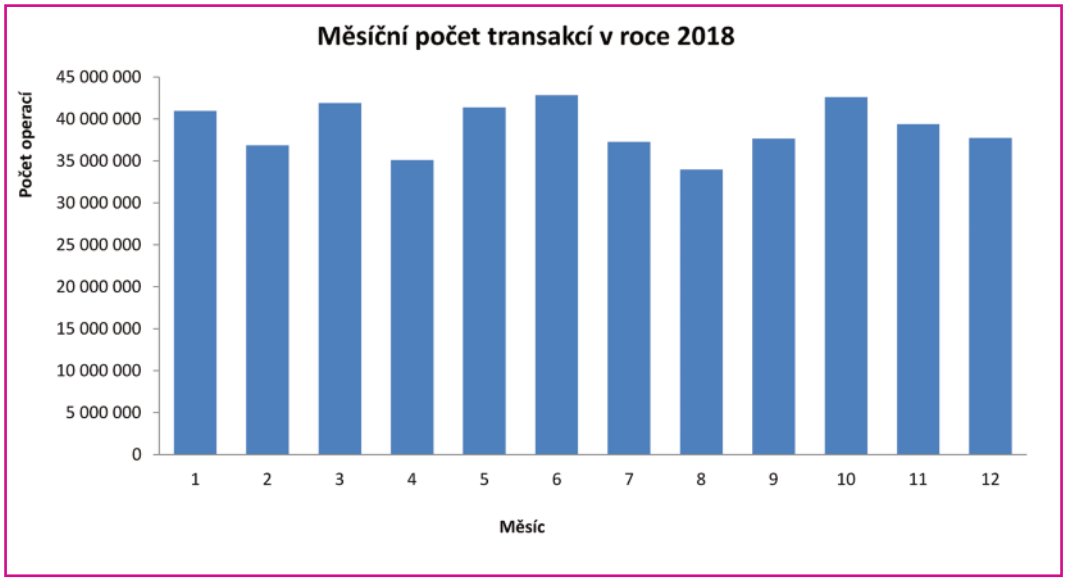
Přehled počtu transakcí v jednotlivých letech od spuštění systému v roce 2012



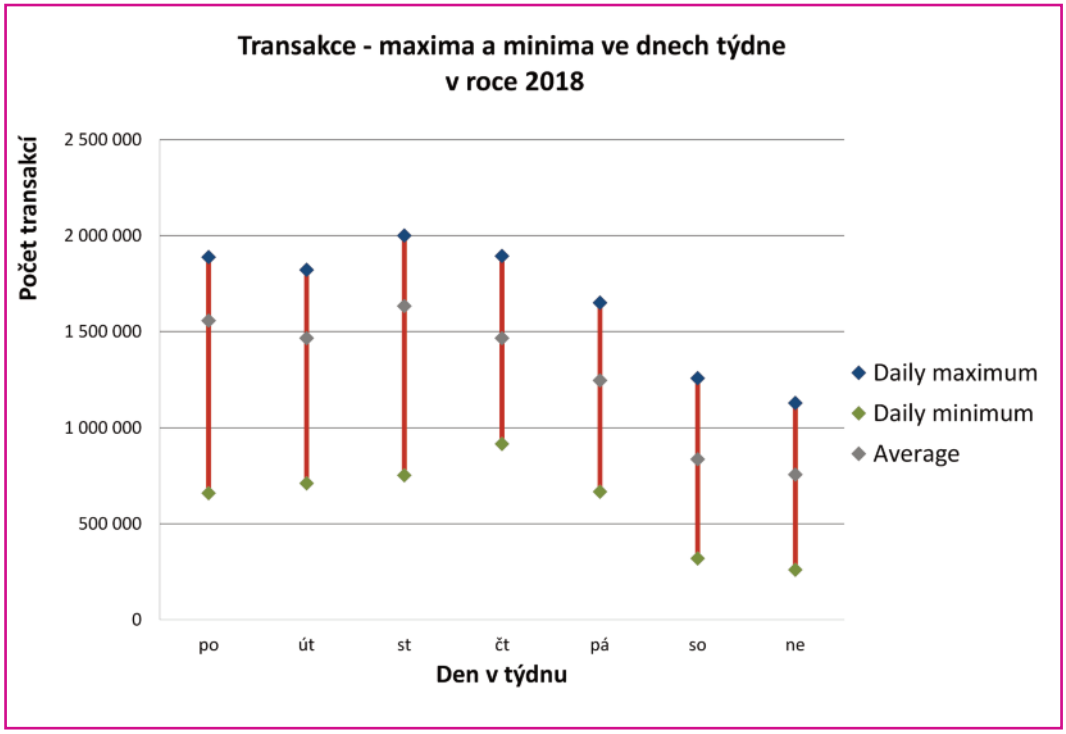
Zobrazení nárůstu počtu transakcí proti předchozímu roku v procentech je na grafu „Procentní přírůstky počtu transakcí vůči předchozímu roku".



Rozložení požadavků na systém základních registrů v průběhu roku je zobrazen v grafu „Měsíční počet transakcí v roce 2018“. Maximální zatížení bylo zaznamenáno 2. července 2018 s počtem transakcí 2 000 795, což je o 1 572 817 méně než v roce 2017. Minimální zatížení bylo zaznamenáno 5. června 2018 s počtem 260 631.



Další graf zobrazuje vytížení systému během týdne. Jsou v něm uvedeny maximální a minimální hodnoty počtu transakcí v jednotlivých dnech týdne. Maximální zatížení bylo zaznamenáno ve středu.



Personální obsazení

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

V roce 2018 činil celkový počet systemizovaných míst 109.

Fluktuace zaměstnanců se v roce 2018 v meziročním srovnání s předchozím rokem snížila z 16,6 % na 9 %.

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

Počátkem roku 2018 bylo provedeno služební hodnocení státních zaměstnanců zařazených k výkonu služby v Úřadu. Na základě těchto hodnocení bylo 29 státních zaměstnanců hodnoceno jako vynikajících a 26 jako dobrých. Žádný státní zaměstnanec nebyl hodnocen jako nevyhovující.

Do služebního poměru bylo nově přijato 10 zaměstnanců a 6 zaměstnanců služební poměr ukončilo. Do pracovního poměru pak byli přijati 4 zaměstnanci, přičemž 3 zaměstnanci pracovní poměr ukončili.

V rámci Úřadem zajišťované zvláštní části úřednické zkoušky pro obor služby „ochrana osobních údajů" bylo vyzkoušeno celkem 25 žadatelů, z nichž 21 žadatelů složilo zkoušku úspěšně a 4 žadatelé byli hodnoceni jako neúspěšní. Navýšení počtu zkoušených žadatelů oproti předchozím létům je důsledkem zřízení pozic pověřenců pro ochranu osobních údajů v jednotlivých resortech státní správy a nutnosti jejich přezkoušení v souladu se zákonem o státní službě.

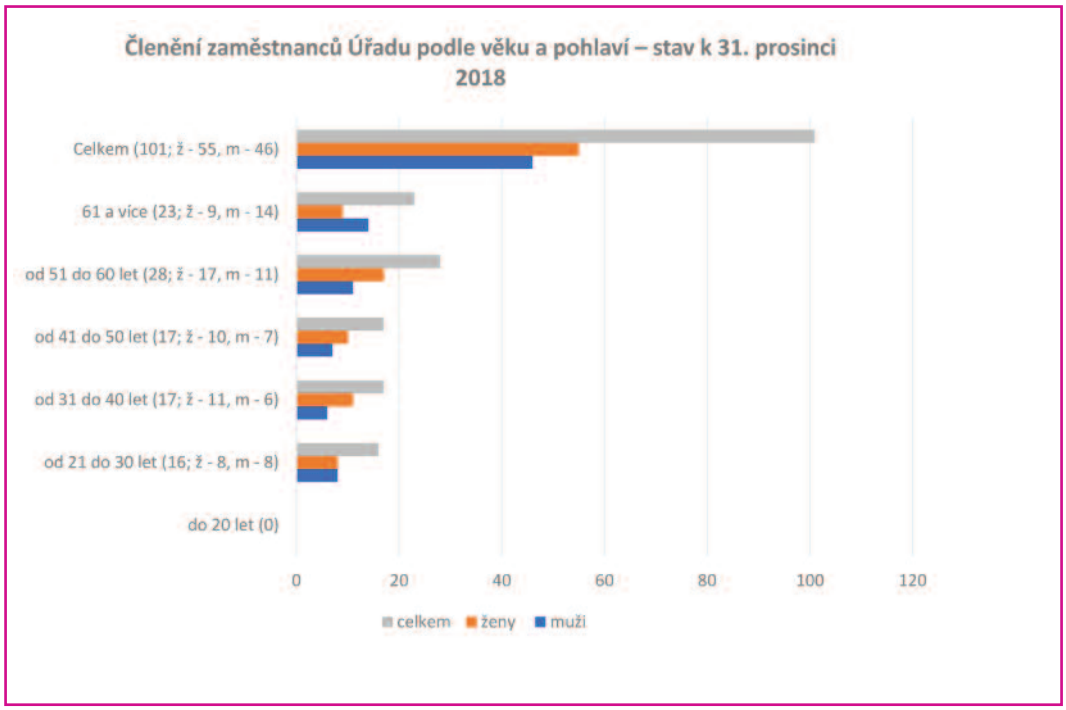
K 1. lednu 2018 bylo v Úřadu v evidenčním stavu 97 zaměstnanců, k 31. prosinci 2018 byl pak jejich počet 101.

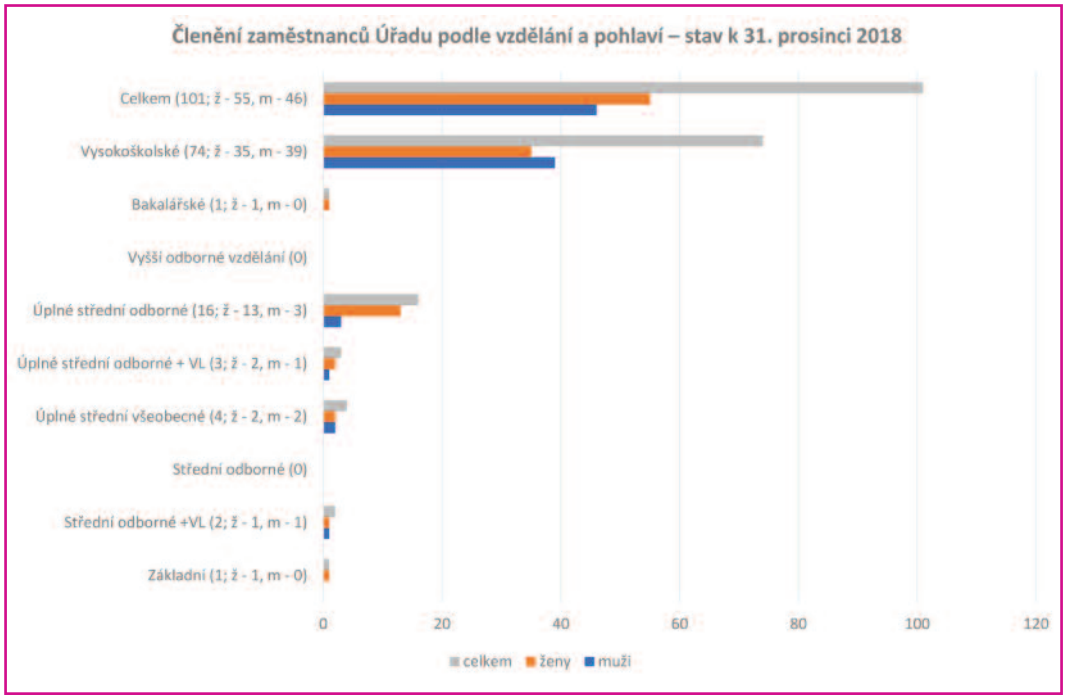
Průměrný evidenční přepočtený počet zaměstnanců za rok 2018 činil 99,10.

Dalších 37 osob vykonávalo v Úřadu činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr.

Z tabulky „Členění zaměstnanců Úřadu 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. Řada z nich působí v Úřadu dlouhou dobu 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 kurzů anglického, německého a francouzského jazyka. Tyto jazykové znalosti pak mohou zaměstnanci uplatnit při výkonu práce nebo služby, kdy s novým evropským pojetím ochrany dat a soukromí získává jazyková vybavenost zaměstnanců stále více na významu. Studentům středních a vysokých škol Úřad poskytuje možnost absolvovat odbornou praxi. Tím podporuje jejich zájem o problematiku ochrany osobních údajů a zároveň tak vyhledává nové potenciální zaměstnance.





Hospodaření

Rozpočet Úřadu byl schválen zákonem č. 474/2017 Sb., o státním rozpočtu České republiky na rok 2018.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

	v tisících Kč
Souhrnné ukazatele	
Příjmy celkem	3 056,89
Výdaje celkem	158 534,20
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	056,89
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	0,00
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	3056,89
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	158 534,20
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	65 650,92
Povinné pojistné placené zaměstnavatelem*)	22 101,10
Převod fondu kulturních a sociálních potřeb	1 271,71
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	12 553,16
Platy zaměstnanců na služebních místech podle zákona o státní službě	40 084,79
Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	11 007,49
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	9 940,09

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

1. Příjmy

Příjmy pro rok 2018 nebyly schváleným rozpočtem stanoveny.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částkou 3 056,89 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 2017 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2017).

2. Výdaje

Čerpání výdajů ve výši 158 534,20 tisíc Kč zahrnuje:

- veškeré náklady na platy a související výdaje,
- kapitálové výdaje, spojené s objektem Úřadu, obnovou informačních systémů, jak samotného Úřadu, tak i informačního systému ORG v systému základních registrů,
- 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 Úřadu.

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

Čerpání rozpočtu na platy zaměstnanců, ostatních výdajů za provedenou práci a souvisejících výdajů, vč. FKSP, a náhrad v době nemoci, ve výši **89 169,69** tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. prosinci 2018 byl **101 zaměstnanců**.

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

V souladu se schválenou dokumentací programu 043V10 „Rozvoj a obnova materiálně technické základny Úřadu pro ochranu osobních údajů od r. 2017" bylo celkem vyčerpáno **9 940,09 tisíc Kč**.

Přehled čerpání rozpočtu v roce 2018

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2018 v tis. Kč	Konečný rozpočet 2018 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2018 v tis. Kč	Skutečný konečný rozpočet v %
2211, 2212, 2324, 3113, 4132	Ostatní nedaňové příjmy	0,00	0,00	3 056,89	
	Příjmy celkem	**0,00**	**0,00**	**3 056,89**	
501	Platy	62 944,81	64 764,73	63 645,44	98,27
5011	Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	12 041,28	12 711,53	12 553,16	98,75
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	39 834,73	40 284,79	40 084,79	99,50
5014	Platy zaměst. odvozov. od platů úst. činitelů	11 068,80	11 768,41	11 007,49	93,53
502	Ostatní platby za provedenou práci	1 890,91	2 005,48	2 005,48	100,00
5021	Ostatní osobní výdaje	1 890,91	2 005,48	2 005,48	100,00
5024	Odstupné	0,00	0,00	0,00	0,00
503	Povin. pojist. plac. zaměstnavatelem	22 044,15	23 559,00	22 101,10	93,81
5031	Povin. pojist. na sociál. zabezpečení	16 208,93	17 343,74	16 206,63	93,44
5032	Povin. pojist. na veřej.	5 835,22	6 215,26	5 894,47	94,84
512	Výdaje na některé úpravy hm. věcí a pořízení a poř. některých práv k hm. věcem	0,00	80,00	3,29	4,11
513	Nákup materiálu	1 522,00	4 324,12	4 150,76	95,99
514	Úroky a ost. fin. výdaje	50,00	30,00	28,35	94,51
515	Nákup vody, paliv a energie	2 025,00	1 646,12	1 482,61	90,07
516	Nákup služeb	12 068,63	54 272,75	47 918,16	88,29

517	Ostatní nákupy	38 885,86	5 250,84	2 816,82	53,65
518	Poskyt. zálohy, jistiny, záruky a vládní úvěry	485,00	485,00	0,00	0,00
519	Výdaje souvis. s neinv. nákupy, příspěvky, náhrady a věcné dary	3 164,70	3 408,65	3 015,32	88,46
534	Převody vlastním fondům a ve vztahu k útv. bez plné práv. subjektivity	1 266,80	1 271,71	1 271,71	100,00
5342	Převody fondu kulturních a soc. potřeb a soc. fondů obcí a krajů	1 266,80	1 271,71	1 271,71	100,00
536	Ost. neinv. transf. jin. veřej. rozp. platby daní a další povinné platby	22,00	22,00	9,10	41,36
542	Náhrady plac. obyvatelstvu	200,00	200,00	145,97	72,99
5424	Náhrady v době nemoci	200,00	200,00	145,97	72,99
	Běžné výdaje celkem	**146 569,86**	**161 320,40**	**148 594,10**	**92,11**
611	Pořízení dlouh. nehmot. majetku	7 600,00	7 931,77	3 600,28	45,39
612	Pořízení dlouh. hmot. majetku	11 300,00	19 420,18	6 339,81	32,65
	Kapitálové výdaje celkem	**18 900,00**	**27 351,95**	**9 940,09**	**36,34**
	VÝDAJE CELKEM	**165 469,86**	**188 672,36**	**158 534,20**	**84,03**

Číselné údaje jsou použity z výkazů zpracovaných k 31. prosinci 2018.

INTERNÍ AUDIT

Základními právními a regulatorními normami upravujícími činnost interního auditu v roce 2018 byly:

- zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole),
- vyhláška č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb.,
- *Mezinárodní rámec profesní praxe interního auditu*,
- vnitřní směrnice Úřadu, které se pravidelně aktualizují.

Interní audit je organizačně oddělen od řídicích a výkonných struktur, funkčně nezávislý a podřízen přímo předsedkyni Úřadu.

Roční plán interního auditu na rok 2018 byl předsedkyní Úřadu schválen 15. března 2018. Hlavním podkladem pro jeho vypracování byla souhrnná analýza rizik Úřadu, včetně rizik identifikovaných při výkonu interního auditu. Roční plán vycházel také ze střednědobého plánu interního auditu na období let 2019 až 2021, z výsledků předchozích interních auditů, z požadavků vedoucích zaměstnanců Úřadu, z plnění povinností vyplývajících ze zákona o finanční kontrole (interní audit by měl prověřit nejméně jednou ročně např. účinnost vnitřního kontrolního systému na základě ustanovení § 30 odst. 7 zákona č. 320/2001 Sb.) a z kapacitních možností interního auditu.

Interní audit na základě schváleného ročního plánu na rok 2018 realizoval celkem čtyři audity. Při sestavování programů jednotlivých auditů a při výběru šetřeného vzorku operací k testování se zaměřil především na nastavení řídicích a kontrolních mechanismů a na stav plnění opatření, která byla přijata k nedostatkům zjištěným provedenými interními audity a k možným rizikům v auditovaných oblastech a jejich potenciálním dopadům.

Interní audity byly zaměřeny na prověření:

- strážní služby,
- funkčnosti a účinnosti vnitřního kontrolního systému,
- autoprovozu,
- nákupu služeb informačního systému a informační techniky.

Výsledky auditů ukončených v roce 2018 byly projednány s vedoucími zaměstnanci auditovaných útvarů, subjekty a s předsedkyní Úřadu. Svými zjištěními přinesly přidanou hodnotu k účinnějšímu fungování finančního řízení, dodržování obecně závazných právních a vnitřních předpisů. Ukázaly také nastavení a funkčnost vybraných auditovaných systémů.

Z hlediska provedených interních auditů nic nenasvědčuje tomu, že by účetní závěrka Úřadu neposkytovala věrný a poctivý obraz předmětu účetnictví.

Ke všem nedostatkům zjištěným při výkonu auditu byla přijata adresná, konkrétní a termínovaná opatření. Plnění přijatých opatření je pravidelně interním auditem sledováno a vyhodnocováno.

Při výkonu interních auditů nebyla identifikována žádná závažná zjištění ve smyslu ustanovení § 22 odst. 6 zákona o finanční kontrole. Nebyly zaznamenány možnosti vzniku korupce ani podvodu.

Interní audit rovněž v roce 2018:

1. zajišťoval konzultační činnost a metodickou činnost především v oblasti:
- řízení rizik,
- vnitřních předpisů,
- majetkové evidence,
- realizace plnění opatření.

2. organizoval:
- vzdělávání interního auditora.

Na základě výsledku auditních šetření lze poskytnout ujištění, že v auditovaném období ve vybraných dílčích oblastech vnitřního provozního a finančního řízení je nastavení řídicích a kontrolních mechanismů přiměřené a účinné s výjimkou nedostatků střední a nízké významnosti. Tyto zjištěné nedostatky však nebyly takového charakteru, aby zásadním způsobem ovlivnily výkon finančního řízení a funkčnost nastaveného vnitřního kontrolního systému. Jsou však

podporou pro zvýšení kvality kontrolního prostředí, aktualizaci a dodržování vnitřních předpisů, vzdělávání zaměstnanců i ochranu oprávněných práv a zájmů Úřadu.

ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2018 a informace o jejím předání proběhne v řádném termínu do 31. července 2019 dle Přílohy č. 4 vyhlášky č. 383/2009 Sb., o účetních záznamech v technické formě vybraných účetních jednotek a jejich předávání do centrálního systému účetních informací státu a o požadavcích na technické a smíšené formy účetních záznamů (technická vyhláška o účetních záznamech). V souladu se sdělením Ministerstva financí k aplikaci některých ustanovení zákona č. 221/2015 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, a v návaznosti na zákon č. 101/2000 Sb., nemá Úřad povinnost schvalovat účetní závěrku auditorem.

Poskytování informací podle zákona o svobodném přístupu k informacím

Úřadu bylo v roce 2018 adresováno celkem 56 žádostí o poskytnutí informací vztahujících se k jeho působnosti, což bylo o 26 více než v předchozím roce. Důvodem byla především celková medializace ochrany osobních údajů v souvislosti s obecným nařízením.

V plném rozsahu byla informace poskytnuta v 45 případech. Ve dvou případech Úřad odmítl informaci poskytnout a v sedmi případech žádost o informace odmítl částečně. Důvodem byla především ochrana osobních údajů osob, které byly obsaženy v požadovaných dokumentech, anebo skutečnost, že šlo o požadavek na informace, k nimž omezuje přístup § 11 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Ve dvou případech žadatelé nezaplatili požadovanou úhradu za mimořádně rozsáhlé vyhledávání informací.

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). Předmětem zájmu, s ohledem na účinnost obecného nařízení, byly i informace vztahující se k počtu přijatých podnětů, stížností za určitá období, počet udělených správních sankcí nebo týkající se pověřenců pro ochranu osobních údajů.

Poskytnuté informace byly zveřejněny způsobem umožňujícím dálkový přístup.

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2018
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 2019 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, 2019

ISBN 978-80-210-9224-2