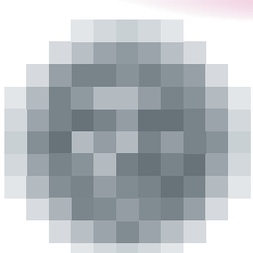
Výroční zpráva 2019



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-9548-9 (brožováno)
ISBN 978-80-210-9549-6 (online; pdf)

Úvodní slovo předsedkyně

Dámy a pánové,
výroční zpráva, kterou jste právě otevřeli, obsahuje témata, jimiž se Úřad pro ochranu osobních údajů zabýval k plnění svých povinností. Jsou dána zákony, ale promítají se v nich – byť mnohdy zprostředkovaně – vlastně všechny aktuální otázky, jimiž společnost žije.

Rok 2019 tak byl druhým rokem, v němž se problematika ochrany osobních údajů těšila širší pozornosti veřejnosti nejen v souvislosti s nabytím účinnosti obecného nařízení, ale také v souvislosti s nekorektním využíváním osobních údajů jiných lidí v kontextu dezinformování a snah o manipulaci s lidmi či v souvislosti s kybernetickými útoky.

Dobrá tradice ochrany osobních údajů v České republice a fakt, že ústavně zakotvené právo lze poměrně účinně vymáhat, přispěly k tomu, že požadavky lidí, kteří se cítí dotčeni na svém právu na ochranu osobních údajů, byl Úřad schopen zvládnout. Znamenalo to pro nás – na rozdíl od některých jiných členských zemí EU – pouze zvýšení objemu práce, nikoli zavedení nových služeb a nových procesů.

Základem činnosti Úřadu je dozorová činnost v ochraně osobních údajů v užším slova smyslu. Ta byla výrazně poznamenána čekáním na adaptační

zákony a na to navazující vyrovnání se s důsledky opožděné a v průběhu projednávání nikoli nepodstatně měněné vnitrostátní legislativy. V tomto světle je třeba číst čísla a závěry z jednotlivých případů kontroly správního trestání.

Nezbývá mi než konstatovat, že se v nich promítá jak několikaměsíční nejistota, tak snížení tlaku na dodržování pravidel veřejnými subjekty při zacházení s osobními údaji. A také postup podle různých předpisů, které nebyly adekvátně aktualizovány. To znamenalo, že byla prováděna dozorová činnost také v oblastech, které stále nemají stanovena přesnější pravidla zpracování osobních údajů, předpokládaná obecným nařízením. Úřad například upozornil ministerstvo práce a sociálních věcí na vzrůstající trend zpracování biometrických údajů zaměstnanců. Problém představuje také použití biometrických technologií soukromými správci či obecní policií.

V konzultační a poradenské činnosti jednoznačně preferujeme odborné akce, které mají širší dosah, a individuální konzultace pro subjekty údajů a správce.

Zásadně širší účinek má rovněž naše zapojení do přípravy nových právních předpisů. Obecné nařízení umožňuje, aby povinnost posoudit před zahájením nového zpracování jeho vliv na práva a svobody fyzických osob byla předsunuta právě do fáze přípravy předpisu, který ukládá povinnost osobní údaje zpracovávat. Úřad o řádné provedení posouzení důrazně usiluje v meziresortním připomínkovém řízení. Jen tak totiž nemusí tato rizika posuzovat každý, kdo k naplňování zákonné povinnosti nějaké osobní údaje zpracovává, případně se může omezit na rizika plynoucí ze začleňování takového zpracování do komplexnějšího informačního systému. Je to pomoc o to účinnější, oč nenápadnější.

Beze změn a tradičně naprosto spolehlivě plnil Úřad své úkoly podle zákona o základních registrech. Provozování kritického informačního systému poskytujícího základní a agendové identifikátory fyzických osob představuje druhý pilíř naší činnosti. Činnost je to relativně skrytá a veřejnost je hladkým fungováním tohoto systému ovlivňována zprostředkovaně přes orgány veřejné správy.

Absolutní novinkou v naší činnosti byla příprava na novou působnost (iniciovanou dolní Poslaneckou sněmovnou), která se začala zčásti naplňovat před koncem roku 2019 jako třetí pilíř. V oblasti práva na informace Úřad od ledna 2020 provádí přezkum rozhodnutí odvolacího orgánu. Je i nadřízeným orgánem některých povinných subjektů a řeší i případy nečinnosti podle zákona o svobodném přístupu k informacím.

Dámy a pánové,
tato zpráva je poslední zprávou, kterou předkládám v rámci svého (stávajícího) mandátu. Jsem přesvědčena, že z této perspektivy v ní lze nalézt i potvrzení trendů, o něž jsem po celou dobu usilovala. Jsou jimi aktivní přístup a neokázalá profesionalita. Zvnějšku jsou doufám patrné například na zapojení do spolupráce v Evropském sboru pro ochranu osobních údajů, kdy k práci Sboru přispívá Úřad kromě jiného též sdíleným zpravodajstvím v několika expertních skupinách komunikujících výhradně v angličtině; každý z deseti odborníků, kteří tyto úkoly plní, vykonává souběžně svoji základní agendu v Úřadu. Ale především jsou patrné na rozhodovací praxi Úřadu. Ze 120 mých druhoinstančních rozhodnutí bylo napadeno žalobou 23. Ve všech 11 případech, o nichž soud již rozhodl, totiž bylo mé rozhodnutí potvrzeno.

JUDr. Ivana Janů
předsedkyně Úřadu pro ochranu osobních údajů

Obsah

Úřad v číslech 2019

Dotazy a konzultace	dotazů celkem	1836
	telefonní konzultační GDPR linka	2667
	předchozí konzultace ve smyslu článku 36 GDPR	0
Podání a stížnosti	přijaté podněty	2482
	vyřízeno upozorněním správce na možné porušení	560
	předáno ke kontrole nebo jinému řízení	145
	ohlášení porušení zabezpečení osobních údajů ve smyslu článku 33 GDPR	416
	poskytnutí součinnosti orgánům činným v trestním řízení	31
	vyřízeno jiným způsobem	1677
Kontrolní činnost (vyjma kontrol týkajících se obchodních sdělení)	zahájeno	63
	ukončeno	75
	z toho z předchozích let	32
	uložená opatření k nápravě	19
	napadeno námitkami	12
	námitkám vyhověno	1
	nevyhověno	10
	částečně vyhověno	1
	pokuty za neposkytnutí součinnosti v kontrole	4
Obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	2007
	zahájených kontrol	5
	ukončených kontrol	17
	z toho z předchozích let	13

	napadeno námitkami	4
	námitkám vyhověno	0
	nevyhověno	4
	částečně vyhověno	0
	řízení o sankci	28
	pokuty za neposkytnutí součinnosti v kontrole	11
	vyřízeno bez zahájení kontroly upozorněním subjektu na možné porušení povinností	390
Správní trestání (s výjimkou řízení týkajících se nevyžádaných obchodních sdělení)	řízení o sankci vedená s právnickými osobami a fyzickými osobami podnikajícími	24
	řízení o sankci s fyzickými osobami	8
	upuštění od uložení pokuty podle § 40a zákona č. 101/2000 Sb., resp. § 65 zákona č. 110/2019 Sb	25
	napomenutí	4
	upuštěno od uložení správního trestu z důvodu nemožnosti trestání orgánů veřejné moci a veřejných subjektů	7
Rozhodování předsedkyně Úřadu	rozklady napadená rozhodnutí	15
	zamítnutých rozkladů	14
	zrušeno a vráceno k novému projednání	6
	zrušených rozhodnutí a zastaveno řízení	1
	změna rozhodnutí	4
Soudní přezkum (Pozn.: * *celkem od r. 2001*)	podaných žalob k soudu	10 (165)*
	zamítnutých žalob soudem	6
	zrušených rozhodnutí soudem	1
	ukončených/neukončených soudních řízení od roku 2001	141/24
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí	1
	rozhodnutí o povolení předávání	1
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	0
Stížnosti podle § 175 správního řádu	přijatých stížností	30
	vyřízených jako důvodné	4
	vyřízených jako částečně důvodné	0
	vyřízených jako bezdůvodné	19
	dosud nevyřízeno	7

Žádosti podle zákona o svobodném přístupu k informacím	přijatých žádostí	90
	zcela vyhověno	63
	částečně odmítnuto	24
	zcela odmítnuto	3
	požadavek na úhradu nákladů za mimořádné vyhledávání informací	6
	z toho uhrazených	3
Připomínkované návrhy	věcné záměry zákonů	3
	zákony	80
	prováděcí předpisy	43
	návrhy nařízení vlády	16
	návrhy vyhlášek	27
	nelegislativní dokumenty	41

Dozorová činnost

• STÍŽNOSTI A PODNĚTY

Na základě porovnání počtu 2482 stížností a podnětů obdržených v roce 2019, směřujících proti postupu správců osobních údajů, lze z hlediska zastoupení soukromého a veřejného sektoru konstatovat, že převažovaly podněty a stížnosti směřující proti zpracování osobních údajů v oblasti soukromoprávních vztahů. To lze přičítat nejen vyššímu početnímu zastoupení správců v tomto sektoru, ale i povinnému jmenování pověřenců pro ochranu osobních údajů u všech orgánů veřejné moci a veřejných subjektů, u kterých pověřenci za necelé dva roky svého působení kultivovali prováděné zpracování osobních údajů.

V oblasti veřejného sektoru se Úřad zabýval například stížnostmi směřujícími proti zveřejňování adresních údajů žadatelů při zveřejnění poskytnuté informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, kdy zejména obce neprovedly na zveřejněném dokumentu o poskytnutí informace anonymizaci žadatele, případně ji provedly nedostatečně.

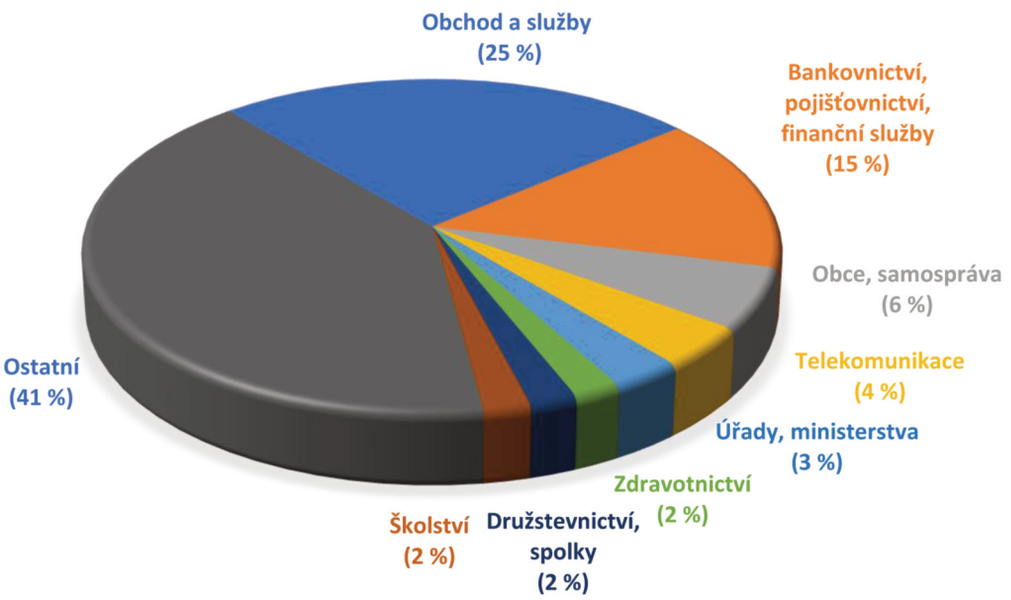
Opakovaným předmětem stížností bylo zveřejnění záznamů (případně zápisů) z jednání zastupitelstva obce nebo rady města na internetu. Stalo se tak bez nezbytné anonymizace osobních údajů občanů či třetích osob, které mohou být v záznamu obsaženy v souvislosti s jejich soukromými záležitostmi (tj. těch, kteří nevystupovali v souvislosti s věcí veřejného zájmu).

ÚOOÚ se ve veřejnoprávní oblasti rovněž zabýval stížnostmi na nahlížení úředníků do základních registrů, aniž by k tomu měli právní důvod.

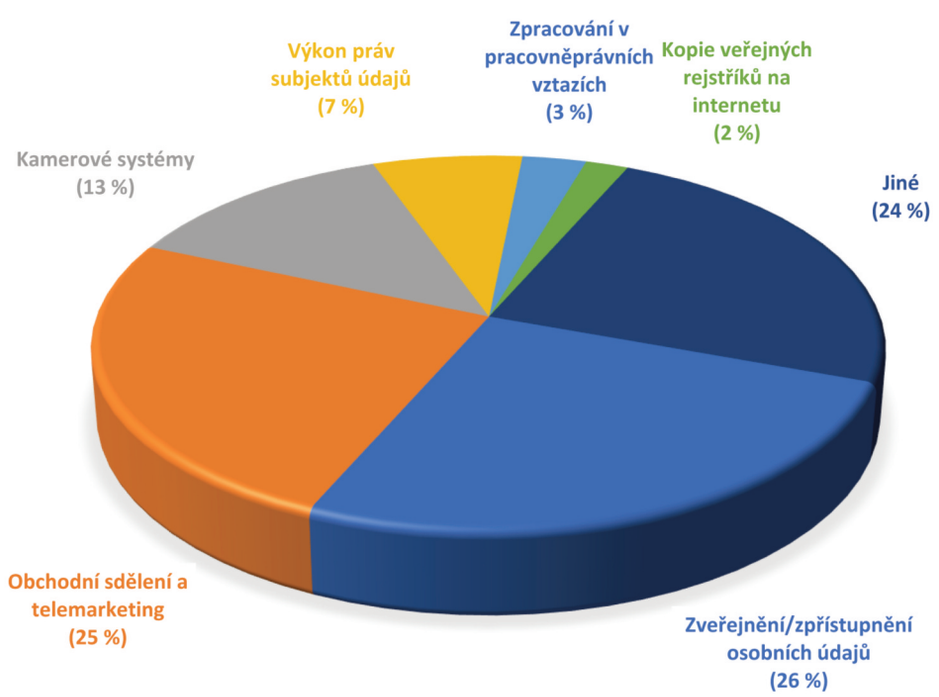
V soukromém sektoru tvořily velkou část agendy stížnosti na zpracování osobních údajů pro marketingové účely. Do této oblasti lze zařadit stížnosti na zasílání obchodních sdělení v listinné podobě poštou[1], aniž by osoba dotčená zpracováním (subjekt údajů) znala zdroj, od kterého správce získal její osobní údaje. Patří sem i stížnosti na získávání souhlasu se zpracováním osobních údajů za účelem marketingu, které někdy hraničily s nemožností získat danou službu bez poskytnutí takového souhlasu.

1 K dozorové činnosti Úřadu ve vztahu k šíření obchodních sdělení elektronickými prostředky viz strana 42.

PODNĚTY/STÍŽNOSTI PODLE OBLASTI ČINNOSTI SPRÁVCE (SEKTORU)



NA CO SI LIDÉ NEJČASTĚJI STĚŽUJÍ



Podatelé se často obraceli na Úřad i poté, co již uplatnili u příslušných společností právo, které jim obecné nařízení přiznává (např. odvolali souhlas, uplatnili právo na výmaz či vznesli námitku nebo se dotazovali na původ jejich osobních údajů v databázi správce), a přesto správce pokračoval ve zpracování jejich dat pro marketingové účely, a dále je oslovoval s obchodními sděleními, elektronicky nebo poštou.

Značná část stížností na zpracování údajů pro marketingové účely se týkala telemarketingových hovorů, které dotčené osoby vnímaly jako nejvíce obtěžující. Z obsahu těchto stížností bylo zřejmé, že podatelům často nebyla známa identita subjektu (správce), jehož jménem jim bylo voláno, a nebyl jim znám ani zdroj, z kterého správce jejich kontaktní, případně další osobní údaje získal. V návaznosti na to ÚOOÚ v únoru 2019 zveřejnil na svých webových stránkách materiál k obraně proti nevyžádaným marketingovým hovorům, které jsou uskutečňovány bez vazby na předchozí vztah mezi volaným a volajícím. Tento materiál, nazvaný Jak se bránit nevyžádanému telemarketingu, informuje mimo jiné i o tom, jak může adresát nevyžádaného telemarketingového hovoru uplatnit svá práva.

Také v období, které uplynulo od posílení ochrany práv subjektů údajů obecným nařízením, docházelo k nerespektování práv subjektů údajů ze strany mnoha správců. Zpravidla se jednalo o případy, kdy subjektu údajů na jeho žádost správce neposkytl adekvátní informaci o zpracování údajů, případně jeho žádost zůstala bez reakce správce, aniž by subjekt údajů byl informován o důvodech, pro které správce jeho žádosti nevyhověl.

Nadále ze strany některých správců docházelo ke znesnadňování přístupu subjektu údajů k jeho údajům neadekvátními požadavky na ověření jeho identity, přestože ta byla zjevná v kontextu dosavadní komunikace s ním. Důvodná pochybnost správce o identitě žadatele tak nebyla na místě. Závažnější nerespektování práv subjektů údajů Úřad dále řešil v rámci svěřených dozorových pravomocí.

Také v roce 2019 se ÚOOÚ potýkal s případy, kdy na žádost subjektu údajů o poskytnutí kopie zpracovávaných osobních údajů správce odmítl poskytnout kopii nahrávky hovoru (příp. jejího přepisu), na jehož základě měl být smluvní vztah se subjektem údajů uzavřen, nebo ujednána změna smluvního vztahu, případně dokumentován průběh plnění smlouvy. Úřad seznal stížnosti na neposkytnutí kopie nahrávky hovoru (popř. jejího přepisu) důvodnými, neboť záznam hovoru je klíčovým nejen pro určení, zda došlo ke vzniku či změně smluvního vztahu, ve kterých je subjekt údajů jednou ze smluvních stran, ale i pro určení, zda a jakým právním titulem správce pro dané zpracování údajů disponoval.

Součástí stížnostní agendy byly v roce 2019 i stížnosti na podmínění poskytnutí služby pořízením kopie dokladu totožnosti (občanského průkazu, cestovního pasu). Jednalo se o situace, kdy k tomu správci nebyla stanovena povinnost právním předpisem. Úřad při posouzení těchto stížností vycházel z hodnocení, zda v daném případě správci svědčil právní důvod k pořízení kopie dokladu totožnosti a zdali v případě, že právním důvodem byl souhlas, byl tento udělen svobodně, a v neposlední řadě zdali správce dodržel zásadu minimalizace údajů. Identifikace osoby totiž standardně spočívá v zaznamenání nezbytných identifikačních údajů z předloženého průkazu totožnosti, nikoli v pořízení a uchování jeho kopie.

Obdobně, především z hlediska existence právního titulu pro zpracování a zásady minimalizace údajů, ÚOOÚ posuzoval stížnosti na zpracování rodného čísla veřejnoprávními i soukromoprávními subjekty, například spolky.

Často se podatelé obraceli na Úřad též s podněty na neplnění nebo nedostatečné plnění informační povinnosti správce o zpracování osobních údajů (např. v rámci obchodních podmínek), případně poukazovali na skutečnost, že správce zaměňuje informační povinnost se získáváním souhlasu, a zpracování vnímali jako netransparentní.

Úřad se také setkával se stížnostmi, které nasvědčovaly zpracování osobních údajů s podvodným úmyslem. Jednalo se například o vymáhání plateb po registraci na webovém portále (např. dražby, aukce) nebo e-shopu, přičemž registrující netušil, že provedením „registrace" správce rozumí uzavření smluvního vztahu (např. o zprostředkování služby inzerce). Následně byla subjektu údajů fakturována neobjednaná služba, případně vymáhána pokuta za porušení „obchodních podmínek". Tyto podněty a stížnosti Úřad postoupil Policii České republiky s podezřením ze spáchání trestného činu podvodu či vydírání ze strany těchto subjektů.

O zpracování údajů s podvodným úmyslem svědčily i případy, kdy správce shromažďoval a zveřejňoval identifikační osobní údaje fyzických osob podnikajících z veřejného rejstříku, aniž podnikatel tušil, že je někde inzerován (v inzertním katalogu). Posléze byl subjekt údajů správcem telefonicky kontaktován a po určité manipulaci (např. výzvě k aktualizaci dat) uzavřel bez svého vědomí smlouvu na dálku (po telefonu). Následně byl vyzván k úhradě ceny za službu, přičemž je při jejím neuhrazení dále vymáhána smluvní pokuta.

Často se ÚOOÚ v roce 2019 zabýval také stížnostmi týkajícími se podvodného jednání osob jednajících jménem prodejců energií. Tito buď již disponovali osobními údaji osob, které kontaktovali prostřednictvím telemarketingových hovorů, aniž je informovali o skutečném zdroji získání údajů, anebo přímo podvodným způsobem získali osobní údaje subjektu údajů. Většinou se (v případě podomního prodeje) vydávali za zaměstnance stávajícího dodavatele energie a požádali jej o předložení dokladů a smluv.

Úřad zaznamenal i případy, kdy se osoby jednající jménem prodejce energií měly dopustit krádeže identity, tj. zfalšováním podpisu na smlouvě nebo dokonce zfalšováním následného verifikačního telefonického rozhovoru.

Také v uplynulém roce se na ÚOOÚ obracely fyzické osoby dotčené zpracováním svých osobních údajů zveřejněním na internetu, a to jak pro novinářský účel, případně v rámci příspěvků a diskusí na sociálních sítích a webových stránkách.

Při posouzení těchto stížností Úřad vycházel nejprve ze zhodnocení, zdali na dané zveřejnění obecné nařízení dopadá. Hodnotil tak, zda se jednalo o zveřejnění výlučně v rámci osobních činností (např. v osobním profilu na sociální síti, v rámci diskuse, blogu na sociální síti nebo na zájmové webové stránce) a zdali se jednalo o zpracování, tzn. zdali byl naplněn prvek systematičnosti pro dané zveřejnění (jednalo-li se o výstup z evidence nebo o data vkládaná do evidence).

V případech ad hoc zveřejnění informací o fyzické osobě, na které věcná působnost obecného nařízení nedopadá, a kdy se nejednalo o zpracování údajů ve smyslu obecného nařízení, Úřad informoval podatele o možnosti využít ustanovení zákona č. 89/2012 Sb., občanského zákoníku, upravujících ochranu osobnosti, a to v rámci občanskoprávního řízení. Podatel byl v takovém případě informován i o tom, že kromě občanskoprávní odpovědnosti osoby, která informace na internetu o něm šíří, může být dána i odpovědnost poskytovatelů internetových služeb (např. vyhledávačů) podle zákona č. 480/2004 Sb., o některých službách informační společnosti, i s odkazem na doporučení zveřejněné na webu Úřadu, jak v tomto případě postupovat.

V případech, kdy se jednalo o zveřejnění osobních údajů pro novinářský účel, Úřad věc posuzoval po nabytí účinnosti zákona o zpracování osobních údajů, i se zřetelem na ta jeho ustanovení, která upravují výjimku z práva na výmaz, a to ve vztahu ke zpracování údajů pro novinářské účely. Další postup Úřadu při vyřízení stížnosti se odvíjel v závislosti na hodnocení vztahu práva na informace a na soukromí, zejména zdali stanovený účel zpracování trvá, ale i s ohledem na statut správce. Zkoumáno bylo v tomto kontextu především, zdali se vzhledem k předmětu činnosti správce jedná o novinářskou licenci, resp. o vydávání periodického tisku.

Rovněž v roce 2019 ÚOOÚ obdržel a dále řešil stížnosti proti postupu soukromých subjektů, provozujících kopie veřejných rejstříků na internetu, které po uplatnění práv dotčenou osobou nevyhověly její námitce proti zpracování, resp. její žádosti o výmaz osobních údajů. Takové případy byly zpravidla následně ze strany oddělení podnětů a stížností postupovány k dalším dozorovým opatřením.

Úřad ani v roce 2019 nezaznamenal pokles stížností týkajících se provozování kamer, ať již v rámci sousedských (občanskoprávních) sporů, případně soukromoprávními i veřejnoprávními subjekty k ochraně majetku. Děje se tak i přesto, že v této oblasti dlouhodobě šíří osvětu na svých internetových stránkách.

V případě stížností směřujících proti zpracování osobních údajů zaměstnavateli byly vedle stížností týkajících se sledování zaměstnanců (kdy posouzení je v působnosti Státního úřadu inspekce práce) ÚOOÚ doručeny i stížnosti (bývalých) zaměstnanců na neposkytnutí přístupu ke zpracovávaným osobním údajům.

Stejně jako v předchozích letech, v případě méně závažných porušení povinností ze strany správce nebo v případě, kdy lze porušení povinností správce snadno a rychle napravit, pokračoval Úřad v osvědčeném informování správců o možném porušení pravidel ochrany osobních údajů, aniž by bylo nutné využívat jiných správních postupů. Tento přístup Úřadu vychází z uplatňování zásady subsidiarity trestně správní represe, která brání nadužívání správního trestání, a též z pokračující osvěty správců ve vztahu k obecnému nařízení.

Při posuzování bagatelních pochybení, ke kterým dochází zejména u malých správců, ÚOOÚ nezahajoval řízení z moci úřední a zvolil primárně takový postup, v němž bagatelně chybujícímu správci připomněl jeho povinnosti a vyzval jej k nápravě vadného zpracování. Tento postup se Úřadu ve většině případů osvědčil, neboť zajistil, že správce provedl změny své dosavadní praxe v souvislosti s jím prováděným zpracováním osobních údajů.

V uplynulém roce ÚOOÚ tento přístup uplatnil ve více než pěti stovkách případů, kdy tímto způsobem byla zajištěna rychlá a efektivní náprava. Našli se však správci, kteří na zaslaný informativní dopis nereagovali, či reagovali nedostatečným způsobem. V takových případech bylo nutné danou věc následně řešit buď formou zahájení kontroly, či jiného správního postupu.

• OHLAŠOVÁNÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

V roce 2019 obdržel Úřad celkem 416 ohlášení porušení zabezpečení osobních údajů. Ta se lišila jak v ohlašovaném riziku bezpečnostního incidentu ve vztahu k subjektům údajům, tak i splněním formálních požadavků, které na ohlášení dozorovému úřadu klade obecné nařízení v článku 33 odst. 3.

Právě za účelem co nejvíce ulehčit správcům provedení ohlášení porušení zabezpečení osobních údajů byl na internetových stránkách ÚOOÚ v průběhu roku 2019 zpřístupněn formulář pro ohlašování porušení zabezpečení osobních údajů. Ačkoli se nejednalo o povinnou formu ohlašování, začal být záhy využíván správci z celého spektra zpracování osobních údajů.

Porušení zabezpečení osobních údajů, která byla ohlašována Úřadu, se vyskytovala jak v soukromém, tak veřejném sektoru. Stejně jako v předchozím roce byla společným jmenovatelem pro oba sektory ohlášení týkající se kybernetického incidentu, který zasáhl též zpracovávané osobní údaje. Situace měla nejčastěji podobu napadení škodlivým programem (tzv. ransomware), který zašifroval údaje v informačních systémech, a následně k odblokování vyžadoval zaplacení výkupného. Ohlášení takových bezpečnostních incidentů Úřad během roku obdržel několik desítek.

ÚOOÚ ke zmírnění rizika ztráty dostupnosti dat správcům v reakci často zdůrazňoval nezbytnost pravidelného zálohování informací, které z velké části pomůže zmírnit následky takového protiprávního jednání.

Vzhledem k tomu, že valná část nákaz informačních systémů byla způsobena phishingovým útokem[2], ukazuje se jako nezbytnost také důkladná osvěta zaměstnanců.

Předmětem ohlášení byla též jednorázová nedbalostní pochybení zaměstnanců spočívající například v mylném zaslání osobních údajů jiným než zamýšleným adresátům, zaslání e-mailové komunikace adresátům v „neskrytých kopiích" nebo ztrátě zařízení, obsahujícího osobní údaje.

V oblasti zpracování osobních údajů v listinné podobě byla nejčastěji ohlašována jejich ztráta (dokumentů, zásilek apod.) nebo jejich odcizení bývalým nebo i současným zaměstnancem, zpravidla ve snaze poškodit zaměstnavatele.

Přijatá ohlášení Úřad řešil i s ohledem na účel této povinnosti stanovené v obecném nařízení, což primárně neznamená udílení peněžitých sankcí nebo zahájení kontroly. Dle závažnosti přijatých ohlášení ÚOOÚ některá ohlášení odkládal bez dalších opatření, komunikoval se správci a poskytoval jim doporučení nebo v některých případech i odůvodnění, že dané ohlášení nepředstavuje riziko pro subjekty údajů.

Některé případy byly dále řešeny v rámci dozorové činnosti. Ta byla uplatněna například u případu v souvislosti se žádostí České televize a Českého rozhlasu o zaslání seznamu osob, které odebírají elektřinu. Správce – energetická společnost, však nezajistila, aby vytvořená databáze, která byla následně těmto dvěma subjektům předána, neobsahovala osobní údaje přibližně 40 tisíc zákazníků odebírajících nikoliv elektřinu, ale pouze plyn. U fyzických osob se jednalo o osobní údaje v rozsahu jméno, příjmení, datum narození, adresa trvalého bydliště, adresa odběrného místa a dále u fyzických osob podnikajících o osobní údaje v rozsahu jméno,

[2] Phishing je forma počítačové kriminality, jejímž cílem je neoprávněně získat přístupové údaje k informačnímu systému, např. od zaměstnanců.

příjmení, příp. obchodní firma, IČO, adresa sídla a adresa odběrného místa. Některé z těchto osob byly následně bezdůvodně konfrontovány s informací o nutnosti uhradit televizní a rozhlasový poplatek. Úřad konstatoval porušení čl. 32 odst. 1 obecného nařízení, tedy povinnosti správce provést vhodná technická a organizační opatření, a uložil mu pokutu ve výši 40 000 Kč.

Zobecněné poznatky z ohlašování porušení zabezpečení osobních údajů Úřad prezentoval na svých internetových stránkách a též při vhodných příležitostech, jako byly například semináře pro pověřence.

• KONTROLNÍ ČINNOST

Kontroly zahajované Úřadem v roce 2019 byly již vykonávány podle obecného nařízení o ochraně osobních údajů, přičemž kontroly byly zahajovány jak z poznatků ze stížnostní agendy, tak na základě vypracovaného kontrolního plánu pro rok 2019.

V souvislosti s přijetím zákona č. 110/2019 Sb., o zpracování osobních údajů, a jeho účinností od 24. dubna 2019, který nově upravil ÚOOÚ a jeho organizaci, došlo s účinností od 1. července 2019 k reorganizaci odboru dozoru. Jeho struktura nyní odpovídá předpokladům zákona o zpracování osobních údajů a umožňuje provádět kontroly co nejefektivnějším způsobem. Vznikají tak kontrolní týmy v rámci specializovaných oddělení, které doplní dosavadní inspektory. Ti podle přechodného ustanovení § 66 odst. 3 zákona o zpracování osobních údajů takto dokončí svá funkční období.

K 1. červenci 2019 tak dosavadní čtyři inspektoráty nahradila dvě oddělení, přičemž každé z nich se věnuje výlučně kontrolní a související dozorové činnosti v soukromém[3], resp. veřejném[4] sektoru. Další oddělení poskytuje součinnost inspektorům při jimi vedených kontrolách, a též samostatně provádí kontrolní činnost. To umožní lépe diverzifikovat a plánovat kontrolní činnost, a to i ve vztahu k potřebným odborným znalostem v jednotlivých sektorech.

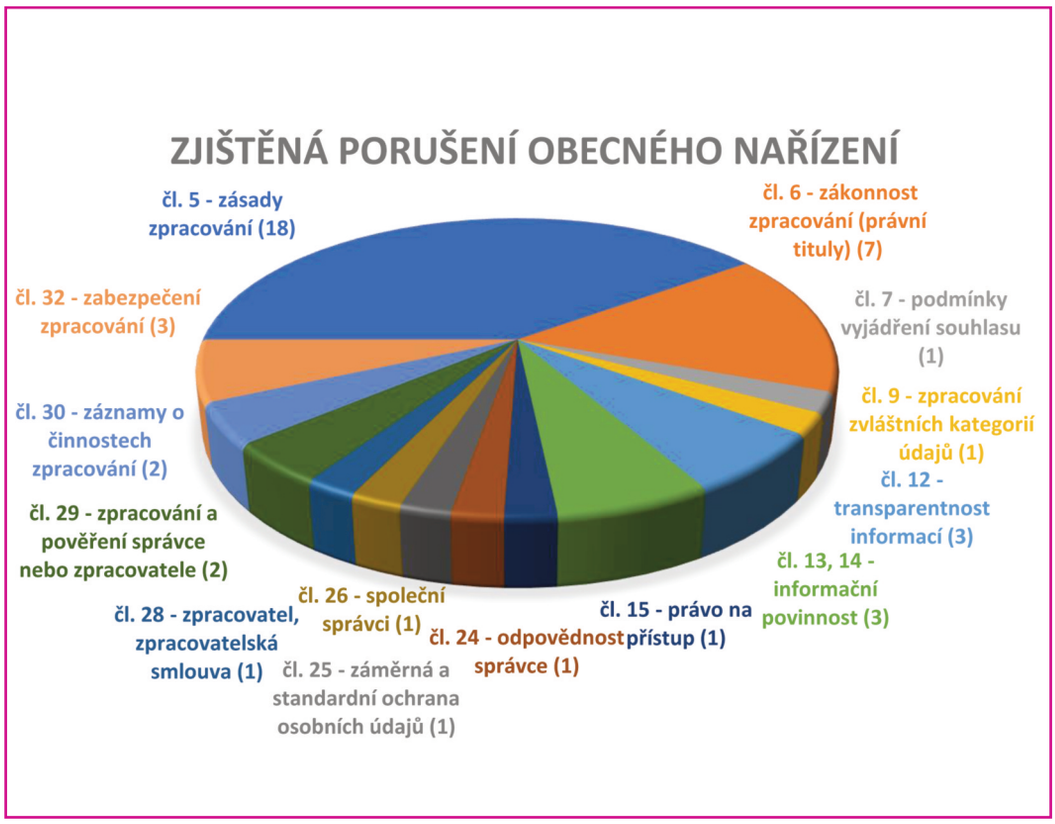
Předmětem kontrolní činnosti v roce 2019 bylo celé spektrum povinností vyplývajících z obecného nařízení, resp. zákona č. 110/2019 Sb., o zpracování osobních údajů. Bližší přehled kontrolně zjištěných porušení obecného nařízení poskytuje graf na následující straně.

Nejčastěji kontrolující konstatovali nedodržení základních zásad zpracování a absenci právního důvodu pro zpracování osobních údajů. Další porušení, která kontrolující zjistili, se týkala práv subjektu údajů. Často se jednalo o porušení transparentnosti informací ve smyslu článku 12 nebo poskytování informací dle článku 13 GDPR. Porušení byla též shledána v některých případech u zabezpečení osobních údajů.

Účinnost obecného nařízení se v roce 2019 projevila též v rámci vzájemné evropské spolupráce dozorových úřadů v oblasti ochrany osobních údajů. Ve čtyřech kontrolních případech Úřad vystupoval v roce 2019 jako tzv. vedoucí dozorový úřad. To přinášelo nutnost postupovat dle příslušných ustanovení obecného nařízení o spolupráci mezi dozorovými úřady, přičemž za tímto účelem ÚOOÚ využíval systém Evropské komise pro výměnu informací o vnitřním trhu (tzv. IMI). V prvním případě se jednalo o kontrolu na základě podnětu postoupeného Úřadu britským dozorovým úřadem – Information Commissioner's Office. Předmětem kontroly bylo uplatňování

[3] Oddělení kontroly soukromého sektoru.

[4] Oddělení kontroly veřejného sektoru.



práv subjektu údajů. Na základě provedené kontroly Úřad konstatoval, že kontrolovaná osoba porušila povinnost uvedenou v čl. 15 odst. 1 písm. c) GDPR.

Další kontrolou Úřadu v pozici vedoucího dozorového úřadu byla kontrola společnosti poskytující antivirový program, přičemž kontrola byla zaměřena na zpracování osobních údajů uživatelů antivirového programu. Předmětem stížnosti byla nemožnost deaktivovat přednastavené možnosti ochrany soukromí v bezplatné verzi antivirového softwaru.

Podrobná informace o těchto dvou kontrolách byla zveřejněna v průběhu roku na internetových stránkách ÚOOÚ.

Jiná kontrola, v níž Úřad vystupoval jako vedoucí dozorový úřad, se týkala zpracování osobních údajů převzatých z veřejných rejstříků či zveřejněných jiným způsobem. Tato kontrola, s ohledem na její komplexnost, bude dokončena v roce 2020.

I v roce 2019 se Úřad v rámci kontrolní činnosti setkával s nespolupracujícími subjekty, přičemž v 11 případech musel přistoupit k uložení pokuty za neposkytnutí součinnosti dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád).

• KONTROLNÍ PLÁN

Kontrolní plán Úřadu pro rok 2019 byl sestaven jak na základě poznatků ze stížnostní agendy, tak v návaznosti na motivaci Úřadu provést kontrolu vybraných ucelených oblastí činností, v nichž jsou využívány některé moderní technologie a prostředky, s nimiž se více či méně setkává v životě každý.

Z tohoto důvodu byly do kontrolního plánu zařazeny kontroly využívání souborů cookies v soukromém sektoru, a to hned u tří společností. Cílem bylo zjistit, jakým způsobem jsou tyto soubory v praxi ve vztahu k uživatelům využívány, a zhodnotit toto využívání s ohledem na příslušnou právní úpravu.

ÚOOÚ se v rámci kontrolního plánu zaměřil též na kontrolu nového fenoménu posledních let – zpracování biometrických údajů, tj. údajů, které nesou fyziologické znaky fyzické osoby nebo znaky jejího chování, umožňující její jedinečnou identifikaci. Do plánu kontrol proto zařadil kontrolu dvou kasin využívajících otisky prstů pro identifikaci hráčů při provozování hazardních her.

Úřad také na základě kontrolního plánu provedl u jednoho bankovního a jednoho nebankovního subjektu kontrolu zpracování osobních údajů žadatelů o uzavření smlouvy o úvěru při jejím sjednávání online, a to s důrazem na výkon práv subjektů.

Další ucelenou oblastí, které se ÚOOÚ v roce 2019 na základě kontrolního plánu věnoval, byla oblast zdravotnictví. V ní se zaměřil na kontrolu tzv. novorozeneckého laboratorního screeningu, což je aktivní vyhledávání chorob u narozených dětí na území České republiky. Jeho účelem je plošná diagnostika a léčba zjištěných chorob dříve, než se stačí projevit a způsobit dítěti nevratné poškození zdraví.

V rámci zdravotnictví zařadil Úřad do kontrolního plánu pro rok 2019 též kontrolu dvou společností zabývajících se testováním genetických údajů (DNA). Kontrola byla zařazena do plánu kontrol na základě poznatků z jednání Evropského sboru pro ochranu osobních údajů za účelem vyhodnocení zjištěných poznatků i pro evropské srovnání.

ÚOOÚ v kontrolním plánu neopominul ani aktuální téma voleb do Evropského parlamentu. Proto do něj zařadil kontrolu dvou politických stran s cílem zkontrolovat zpracování osobních údajů jak v rámci členské základny, tak i případné zpracování osobních údajů mimo ní.

Kontrola zpracování osobních údajů ve veřejném sektoru byla v kontrolním plánu dále zastoupena kontrolou České správy sociálního zabezpečení, jejímž předmětem byla komplexní kontrola zpracování osobních údajů prostřednictvím ePortálu. Úřad se v rámci kontrolního plánu zaměřil též na Generální finanční ředitelství, u něhož komplexně zkontroloval Daňový portál. O vybraných zmíněných kontrolách blíže pojednává kapitola Poznatky z kontrolní činnosti.

Tak jako v předchozích letech, ani v roce 2019 nebyly některé kontroly z kontrolního plánu ukončeny, byť byly v tomto roce všechny zahájeny. O výsledku těchto kontrol bude ÚOOÚ informovat obvyklým způsobem prostřednictvím svých internetových stránek.

• POZNATKY Z KONTROLNÍ ČINNOSTI

Inspektorka Jana Rybínová

Zpracování osobních údajů v rámci poskytování informací ze zdravotnické dokumentace (Psychiatrická nemocnice Bohnice)

Kontrola Psychiatrické nemocnice Bohnice (dále také „kontrolovaná osoba“) byla zahájena na základě podnětu, který Úřadu postoupila Policie ČR ve věci podezření z neoprávněného zpřístupnění osobních údajů poškozené Z. F. odsouzenému pachateli trestné činnosti J. K. Stalo se tak prostřednictvím předané kopie dokumentu Přípis pro věznice a pro zdravotnické zařízení (dále také „Přípis“), zaslaného kontrolované osobě obvodním soudem.

Z hlediska ochrany osobních údajů byla kontrolovaná osoba podezřelá z porušení zabezpečení osobních údajů poškozené Z. F. Ta v přípravném řízení, jenž vyústilo v rozsudek obvodního soudu ve spojení s usnesením Městského soudu v Praze, jimiž byl odsouzený J. K. uznán vinným přečinem nebezpečného pronásledování dle § 354 odst. 1 písm. b) trestního zákoníku a bylo mu nařízeno mimo jiné ochranné psychiatrické léčení v ústavní formě, požádala dle § 158 odst. 6 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), o utajení svých osobních údajů v podobě data narození, rodného čísla, bydliště a doručovací adresy ve smyslu § 55 odst. 1 písm. c) trestního řádu, a aby byla informována o propuštění odsouzeného J. K. na svobodu.

Kontrolovaná osoba byla o žádosti poškozené informována prostřednictvím Přípisu pro věznice a pro zdravotnické zařízení. Uvedený Přípis i s osobními údaji poškozené však byl zaměstnankyní kontrolované osoby odsouzenému J. K. v kopii zpřístupněn.

Předmětem kontroly bylo dodržování povinností stanovených obecným nařízením v souvislosti se zpracováním osobních údajů v rámci poskytování informací ze zdravotnické dokumentace, resp. z její administrativní části. S tím souvisela kontrola vnitřních předpisů upravujících technicko-organizační zabezpečení osobních údajů a postupů zdravotnických pracovníků, zaměřená zejména na dodržování povinností správce osobních údajů ve smyslu čl. 30 a 32 obecného nařízení.

Skutek v části podání žádosti poškozené po jeho vyřízení příslušným soudem až po předání kontrolované osobě je upraven zákonem č. 40/2009 Sb., trestní zákoník, a zákonem č. 45/2013 Sb., o obětech trestných činů, tedy předpisů aplikujících Směrnici Evropského parlamentu a Rady (EU) 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, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/97/SVV ze dne 27. dubna 2016.

Bylo zjištěno, že kontrolovaná osoba zpracovává údaje, které jsou osobními údaji subjektu údajů Z. F. ve smyslu čl. 4 bodu 1 obecného nařízení. Kontrolovaná osoba na základě plnění právní povinnosti stanovené zákonem č. 141/1961 Sb. a zákonem č. 45/2013 Sb. určila účel a prostředky zpracování osobních údajů. Je tedy správcem osobních údajů dle čl. 4 bodu 7 obecného nařízení a za toto zpracování odpovídá. Kontrolovaná osoba osobní údaje poškozené Z. F. ve smyslu čl. 4 bodu 3 GDPR shromáždila, uložila ve zdravotnické dokumentaci, tyto ve smyslu čl. 4 bodu 2 obecného nařízení ve zdravotnické dokumentaci zpracovává a neposledně je ve smyslu čl. 4 bodu 9 obecného nařízení zpřístupnila pacientovi J. K.

Úřad dále zjistil, že kontrolovaná osoba tím, že nepřijala ve smyslu čl. 24 bodu 1 obecného nařízení dostatečná technicko-organizační opatření a prostřednictvím své zaměstnankyně zpřístupnila v rámci nahlížení do zdravotnické dokumentace osobní údaje Z. F. odsouzenému, porušila zásadu zpracování osobních údajů vyjádřenou v čl. 5 bodu 1 písm. f) GDPR.

Kontrolovaná osoba prostřednictvím zaměstnankyně zpřístupnila odsouzenému J. K. Přípis s osobními údaji poškozené Z. F. neoprávněně. Kontrolující konstatovali, že kontrolovaná osoba dostatečně nevyhodnotila rizika související se založením Přípisu s osobními údaji Z. F. do zdravotnické dokumentace J. K., ke které má ve smyslu § 65 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), přístup. Uvedený Přípis s ohledem na informace, které obsahoval, neměl být součástí zdravotnické dokumentace. Uvedené porušení nebylo možno zhojit ani argumentací kontrolované osoby, že postupuje v souladu s ustanovením § 2 písm. e), resp. § 1 odst. 1 písm. g) vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci, neboť údaje Z. F. nejsou údaji souvisejícími s průběhem a výsledkem poskytovaných zdravotních služeb.

Kontrolovaná osoba tím, že nepřijala ve smyslu čl. 24 bodu 1 obecného nařízení dostatečná technicko-organizační opatření pro zajištění ochrany osobních údajů Z. F., důsledkem čehož došlo k systémovému porušení zásady zpracování osobních údajů ve smyslu čl. 32 bodu 1 a 4 obecného nařízení, nezajistila dostatečnou úroveň zabezpečení osobních údajů odpovídající danému riziku. Současně nezajistila ani dostatečné předpisy a pokyny pro postup svých zaměstnanců při zpracování osobních údajů poškozených osob, které požádaly o informaci dle § 55 odst. 1 písm. c) a § 103a zákona č. 141/1961 Sb., o vyrozumění, kdy pacient ukončí výkon ochranného léčení. Porušila tak zásadu zpracování osobních údajů vyjádřenou v čl. 5 bodu 1 písm. f) obecného nařízení.

Kontrolovaná osoba podala proti zjištěním uvedeným v protokolu o kontrole námitky, které předsedkyně Úřadu svým rozhodnutím zamítla. Následně byl ve věci vystaven a doručen Příkaz, kterým bylo kontrolované osobě uloženo přijmout příslušná technicko-organizační opatření. Kontrolovaná osoba tuto povinnost splnila.

Uloženou pokutu ve výši 10 000 Kč kontrolovaná osoba uhradila.

Zpracování osobních údajů v rámci novorozeneckého laboratorního screeningu

Kontrola byla realizována na základě kontrolního plánu Úřadu a probíhala ve čtyřech nemocnicích – v Nemocnici Mělník, Fakultní nemocnici Brno, Fakultní nemocnici Královské Vinohrady a Nemocnici Havlíčkův Brod (dále také „kontrolované osoby"), a to v návaznosti na kontroly provedené ÚOOÚ v roce 2015. Tehdy bylo zjištěno, že kontrolované osoby uchovávají vzorky tzv. suché kapky krve novorozenců, tj. vzorky krve odebrané za účelem novorozeneckého laboratorního screeningu, po neúměrně dlouhou dobu, která neodpovídá účelu zpracování.

Novorozenecký laboratorní screening (dále také „NLS") je součástí preventivní péče ve smyslu § 5 odst. 2 písm. a) zákona č. 372/2011 Sb., tj. je *„prováděn za účelem včasného vyhledávání faktorů, které jsou v příčinné souvislosti se vznikem nemoci nebo zhoršením zdravotního stavu, a provádění opatření směřujících k odstraňování nebo minimalizaci vlivu těchto faktorů a předcházení jejich vzniku"*, cílem je rychlá diagnostika a včasná léčba novorozenců se vzácnými onemocněními – v souladu s usneseními vlády ČR č. 466/2010 (Národní strategie pro vzácná onemocnění) a č. 76/2015 (Národní akční plán pro vzácná onemocnění). Vyhledávána jsou onemocnění endokrinní (2), dědičné poruchy metabolismu (15) a cystická fibróza. Novorozenecký laboratorní screening je založen na analýze krve odebrané novorozenci.

Kontrola u všech kontrolovaných osob byla zaměřena na dodržování povinností stanovených obecným nařízením v souvislosti se zpracováním osobních údajů v rámci novorozeneckého laboratorního screeningu (včetně krevních vzorků), na dobu uchování odebraných vzorků a jejich likvidaci a na plnění dalších povinností stanovených obecným nařízením, týkajících se práv subjektů údajů, zejména čl. 5, 6, 9 a čl. 12 až 23 obecného nařízení.

V rámci kontrol byly prověřovány veškeré postupy při zpracování (nakládání) s odebranými vzorky, tedy odběr kapky krve, její uchování a zabezpečení u kontrolovaných osob, které provedly odběr, předávání, zabezpečení a likvidace v laboratořích kontrolovaných osob, které provádějí analýzu vzorku krve. V současné době je NLS prováděn na základě Metodického návodu k zajištění novorozeneckého laboratorního screeningu a přílohy (Věstník ministerstva zdravotnictví – ročník 2016, částka 6, vydáno 31. května 2016).

V rámci novorozeneckého laboratorního screeningu jsou shromažďovány a zpracovávány osobní údaje novorozenců a jejich matek a příslušných dětských lékařů, které jsou osobními údaji ve smyslu čl. 4 bodu 1 obecného nařízení. Zpracování osobních údajů prováděné v rámci novorozeneckého laboratorního screeningu (osobních údajů uváděných na screeningových kartičkách – žádankách) je tak zákonné, neboť je prováděno v souladu s čl. 6 bodem 1 písm. a) obecného nařízení. Subjekt údajů (zákonný zástupce novorozence) zde udělil souhlas se zpracováním svých osobních údajů pro konkrétní účel (včetně souhlasu s uchováním suché kapky krve), přičemž souhlas poskytovaný subjektem údajů (zákonným zástupcem), je ve smyslu čl. 4 bodu 11 GDPR svobodným, konkrétním, informovaným a jednoznačným projevem vůle subjektu údajů (zákonného zástupce novorozence).

V rámci screeningu je zpracováván specifický údaj přiřazený fyzické osobě za účelem laboratorního vyšetření pro zdravotní účely. Znamená to, že zpracovávány jsou údaje o zdravotním stavu ve smyslu čl. 4 bodu 15 obecného nařízení, které jsou ve smyslu čl. 9 obecného nařízení zvláštními kategoriemi osobních údajů. Zpracovávání zvláštních kategorií osobních údajů je zákonné, probíhá na základě právního titulu vyplývajícího z čl. 9 bodu 2 písm. a) obecného nařízení, neboť subjekt údajů (zákonný zástupce novorozence) udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden účel, kterým je novorozenecký laboratorní screening,

přičemž souhlas poskytovaný subjektem údajů (zákonným zástupcem novorozence) je ve smyslu čl. 4 bodu 11 obecného nařízení svobodným, konkrétním, informovaným a jednoznačným projevem vůle subjektu údajů (zákonného zástupce novorozence).

Kontrolou nebylo zjištěno porušení povinností kontrolovaných osob uložených jim jako správcům osobních údajů čl. 30 bodu 1 obecného nařízení, neboť mají přesně stanovené postupy zpracování osobních, resp. zvláštních kategorií osobních údajů. Vedou navíc záznamy o činnostech zpracování, které obsahují informace dle bodu 1–5 čl. 30 obecného nařízení.

Kontrolující s přihlédnutím ke konkrétní povaze, rozsahu, kontextu, postupům a účelům zpracování, vč. zvážení rizika při zpracování, konstatovali, že přijatá technická a organizační opatření zajišťují dostatečnou úroveň zabezpečení ve smyslu čl. 32 obecného nařízení a zpracování je v souladu se zásadou vyjádřenou v čl. 5 bodu 1 písm. f) obecného nařízení.

Kontrolované osoby, které provádějí odběr krve, jsou ve smyslu čl. 4 bodu 7 GDPR správci osobních údajů (zvláštních kategorií osobních údajů) subjektů údajů zpracovávaných v rámci novorozeneckého laboratorního screeningu, a to od doby provedení odběru do doby, než screeningové kartičky předají k transportu do příslušné laboratoře, tedy zpracovávají osobní údaje v souladu se zásadou uvedenou v čl. 5 bodu 1 písm. e) obecného nařízení. Jednotlivé screeningové kartičky jsou totiž označeny jménem, příjmením, datem narození a dalšími informacemi, umožňujícími po přesně stanovenou dobu identifikaci subjektů údajů.

Kontrolované osoby, které provádějí laboratorní vyšetření, jsou ve smyslu čl. 4 bodu 7 GDPR správcem osobních údajů (zvláštních kategorií osobních údajů) zpracovávaných v rámci novorozeneckého laboratorního screeningu, a to od doby, kdy převezmou screeningové kartičky za účelem laboratorního vyšetření od „spádových" nemocnic. Tyto kartičky pak uchovávají po provedení laboratorního vyšetření po dobu 5 let v souladu s ustanovením bodu 15 písm. b) Přílohy č. 3 – Doby uchování zdravotnické dokumentace nebo jejích částí vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci. Kontrolované osoby zpracovávají osobní údaje ve smyslu čl. 4 bodu 2 obecného nařízení a prováděné zpracování je v souladu s ustanovením čl. 5 bodu 1 písm. e) obecného nařízení.

Inspektorka Božena Čajková

Zpracování osobních údajů v souvislosti s poskytováním elektronických služeb orgány veřejné správy při poskytování služeb prostřednictvím ePortálu provozovaného Českou správou sociálního zabezpečení

Kontrola byla provedena na základě kontrolního plánu Úřadu pro rok 2019. Zaměřila se na dodržování povinností stanovených obecným nařízením v souvislosti se zpracováním osobních údajů při poskytování služeb občanům orgány veřejné správy prostřednictvím ePortálu provozovaného Českou správou sociálního zabezpečení (dále také „kontrolovaná osoba" nebo „ČSSZ").

Úřad se u kontrolované osoby jako správce dle čl. 4 bodu 7 obecného nařízení zaměřil na dodržování zásad při zpracování osobních údajů (klientů a zaměstnanců) a plnění povinností. Zejména šlo o dodržování zásady legitimity a legality, minimalizaci údajů, přesnost a omezení uložení. Z povinností pak plnění informační povinnosti, povinnost při uplatnění práva subjektu údajů dle čl. 15–23 GDPR (práva na přístup k osobním údajům), povinnost uzavřít zpracovatelskou smlouvu dle čl. 28 obecného nařízení, povinnost vést záznamy o činnostech dle čl. 30 obecného nařízení, přijmout technicko-organizační opatření pro zabezpečení osobních údajů dle čl. 32 obecného nařízení a plnění opatření při ohlašování a oznamování případů porušování zabezpečení dle čl. 34 a 35 GDPR.

Kontrolovaná osoba je orgánem sociálního zabezpečení, jehož působnost je upravena zvláštními právními předpisy. Ve stanovených případech v rámci svého oprávnění poskytuje online elektronické služby formou aplikace ePortálu ČSSZ, umožňující klientovi obstarat si konkrétní informace a služby dálkově online formou přístupu z veřejné komunikační sítě internet. Současně poskytuje zabezpečené prohlížení vybraných údajů evidovaných v ČSSZ, umožňuje a nabízí k využití interaktivní tiskopisy a užitečné online služby, které klientům ČSSZ umožňují online komunikaci s ČSSZ, ale též s okresními správami sociálního zabezpečení. ePortál byl zaveden jako internetová samoobsluha, aplikace usnadňující klientům komunikaci s ČSSZ, předávání informací mezi klientem ČSSZ a samotnou ČSSZ, včetně osobních údajů klientů ePortálu.

Kromě úkolů uložených v § 5 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ČSSZ kontroluje plnění povinností subjektů sociálního zabezpečení, posuzuje zdravotní stav a pracovní schopnost občanů pro účely sociálního zabezpečení, vede evidenci práce neschopných občanů a v určených případech provádí nemocenské pojištění. Podle koordinačních nařízení EU je kontrolovaná osoba styčným orgánem vůči zahraničním institucím pro peněžité dávky v nemoci a mateřství, důchody a peněžité dávky v případě pracovních úrazů a nemocí z povolání. I další právní předpisy svěřují kontrolované osobě působnost a stanovují požadavky na výkon státní správy v oblasti sociálního a nemocenského zabezpečení, kterou má vykonávat (zákon č. 155/1995 Sb., o důchodovém pojištění, zákon č. 187/2006 Sb., o nemocenském pojištění, zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti).

Kontrolovaná osoba plní taktéž úkoly služebního orgánu podle zákona č. 234/2014 Sb., o státní službě, zaměstnavatele podle zákona č. 262/2006 Sb., zákoník práce, a správce kritické infrastruktury státu podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Kontrolovaná osoba jako správce zpracovává podle výše uvedených zvláštních právních předpisů potřebné osobní údaje klientů a zaměstnanců ČSSZ. Svědčí pro ni také několik zákonných legitimních oprávnění pro zpracování osobních údajů. Jako zaměstnavatel plní právní povinnosti pro splnění smlouvy v souladu s čl. 6 bodu 1 písm. b) obecného nařízení. Konkrétně se jedná o následující účely:

- zajišťování agendy sociálního zabezpečení (tj. pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, nemocenského pojištění, důchodového pojištění a agendy osob zdravotně znevýhodněných),
- zajišťování agendy lékařské posudkové služby (dále jen „LPS“) pro pojistný i nepojistný systém sociálního zabezpečení a oblast zaměstnanosti,
- správa údajové základny (správa registru pojištěnců, pojistných vztahů, nárokových podkladů důchodového pojištění a dávkových spisů důchodového pojištění),
- poskytování informací a dalších služeb oprávněným osobám v sociálním zabezpečení a v agendě LPS (včetně vzájemné komunikace a spolupráce),
- poskytování informací mimo sociální zabezpečení a LPS oprávněným osobám (včetně vzájemné komunikace a spolupráce),
- personální správy,
- zajišťování kontroly,

- zajišťování agendy bezpečnosti,
- zajišťování právní agendy a oblasti projektů,
- zajišťování vnitřní správy,
- zajišťování účetnictví (nedávkové i výplaty dávek),
- zajišťování agendy informačních a komunikačních technologií,
- poskytování informací oprávněným osobám mimo sociální zabezpečení a LPS oprávněným osobám (včetně vzájemné komunikace a spolupráce).

Kontrolovaná osoba zpracovává osobní údaje klientů ePortálu pro činnost nezbytnou k naplnění právní povinnosti, stanovené výše uvedenými zákony.

Vzhledem k předmětu kontroly se kontrolující zaměřili i na plnění informační povinnosti dle čl. 12 v rozsahu čl. 13 a 14 obecného nařízení na webovém portálu ČSSZ. Pro klienty je na webových stránkách ČSSZ uvedeno několik odkazů, týkajících se zpracování osobních údajů (GDPR – informace o zpracování osobních údajů, leták Informace o zpracování osobních údajů, Provozní řád ePortálu správy sociálního zabezpečení pro klienty ePortálu ČSSZ). V článku „GDPR – informace o zpracování osobních údajů" je uvedena kompletní informace o zpracování osobních údajů klientů. Kontrolovaná osoba přijala vhodná opatření, aby poskytla klientům veškeré informace dle čl. 13 a 14 obecného nařízení.

Kontrolující hodnotili rovněž splnění povinnosti stanovené v čl. 15 až 23 obecného nařízení. Podle těchto ustanovení má subjekt údajů právo na přístup k osobním údajům, tj. právo žádat a získat relevantní informace o zpracování jeho osobních údajů a rovněž právo vznést námitku. Věcně příslušnou osobou pro vyřizování žádostí o výkon práv subjektů údajů je pověřenec pro ochranu osobních údajů.

U kontrolované osoby se právo na výmaz osobních údajů neuplatní v případě, že je zpracování nezbytné pro plnění povinností, které vyžaduje právní řád České republiky, nebo pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci. Tou je pověřena ČSSZ. Na kontrolovanou osobu se v období od ledna do srpna 2019 obrátilo celkem 13 subjektů údajů s žádostí na výkon práv podle čl. 15 až 23 obecného nařízení.

Kontrolující dále ověřili plnění povinnosti, která kontrolované osobě vyplývá z čl. 30 odst. 1 obecného nařízení. Jedná se o povinnost vést záznamy o činnostech zpracování. Kontrolovaná osoba předložila směrnici, jejíž přílohou je i Seznam činností zpracování, Záznamy o činnostech zpracování správce a vymezení účelů zpracování. Záznamy jsou vedeny také v elektronické formě. Postupy při vedení záznamů o činnostech jsou obsaženy ve zmiňované směrnici. Kontrolovaná osoba zpracovává tzv. mapovací dotazníky, které jsou podkladem (evidenčním nástrojem) pro vedení záznamů o činnostech zpracování osobních údajů.

Úřad s ohledem na předmět kontroly také hodnotil, zda a do jaké míry kontrolovaná osoba plní povinnosti týkající se zabezpečení osobních údajů v souvislosti s poskytováním online elektronických služeb ePortálu, jak je její povinností podle čl. 25 a 32 GDPR.

Bylo zjištěno, že aplikace ePortál je součástí Informačního systému kritické informační infrastruktury, který je chráněn záměrnou ochranou osobních dat. Ta zavádí a provádí vhodná technická a organizační opatření s cílem chránit práva subjektů údajů. Standardní ochrana osobních údajů je zajištěna na základě právních předpisů upravujících kybernetickou bezpečnost.

Zabezpečení osobních údajů je tak na úrovni kritické informační infrastruktury. Kontrolovaná osoba dále zavedla a provádí režimová opatření, opatření fyzické bezpečnosti pro ePortál.

Veškerá online komunikace uživatele ePortálu ČSSZ je zabezpečena šifrováním, pro ePortál ČSSZ existuje informační a komunikační ochranné zabezpečení. Základním předpokladem je ověření identity, je zajištěna integrita dat proti zneužití, jejich ztrátě apod.

Kontrola nezjistila žádné porušení povinností.

Zpracování osobních údajů společností TOPlist s.r.o. při používání cookies pro měření návštěvnosti webových stránek

Kontrola byla zahájena na základě kontrolního plánu Úřadu pro rok 2019. Tam byla zařazena s ohledem na dosavadní poznatky ÚOOÚ a také v návaznosti na „Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018", zveřejněného Úřadem dne 22. května 2018. Kontrolovaným subjektem byla společnost TOPlist s.r.o. (dále také „kontrolovaná osoba").

Kontrolovaná osoba poskytuje službu TOPlist, jejíž nedílnou součástí je i zpracování osobních údajů návštěvníků webových stránek jednotlivým uživatelům (provozovatelům webových stránek) na základě jejich registrace.

Účelem zpracování osobních údajů je měření návštěvnosti webových stránek. Tento účel určují jednotliví uživatelé, přičemž služba TOPlist představuje jimi zvolený prostředek k dosažení tohoto cíle. Uživatelé jsou tedy v tomto případě v postavení správce osobních údajů dle čl. 4 bodu 7 obecného nařízení.

Kontrolovaná osoba provádí předmětné zpracování na základě smlouvy s uživatelem a dle jeho pokynů, tzn. dle údajů uvedených v registračním formuláři. V tom uživatel definuje, na kterých webových stránkách má být měření prováděno a zároveň, zda mají být informace o návštěvnosti zahrnuty do statistik na www.toplist.cz, příp. v jaké kategorii. Uživatel dále rozhoduje o tom, zda podrobnosti o návštěvnosti budou veřejně přístupné či nikoli.

Kontrolující konstatovali, že kontrolovaná osoba je v postavení zpracovatele osobních údajů dle čl. 4 bodu 8 obecného nařízení, neboť zpracovává osobní údaje pro správce.

Služba měření návštěvnosti webových stránek (dále jen „služba TOPlist") umožňuje uživateli této služby sledovat statistiky návštěvnosti stránky a zároveň je porovnávat s návštěvností jiných webových stránek registrovaných na www.toplist.cz (např. návštěvnost webových stránek konkurence v daném odvětví). Jedná se o bezplatnou službu poskytovanou na základě registrace na www.toplist.cz. Uživatel má dále možnost využít i rozšířenou placenou službu TOPlist Profi.

Základní měřenou veličinou v rámci služby TOPlist je počet návštěv dané webové stránky. Za návštěvu je považováno zobrazení stránky v prohlížeči (rozlišené pomocí IP adresy a cookie). Opakovaná návštěva dané webové stránky z téhož zařízení před uplynutím 30 minut se pak považuje za pouhé zhlédnutí. Naopak v případě, kdy se návštěvník vrátí ze stejného zařízení na webovou stránku po uplynutí 30 minut, je započítána nová návštěva.

K technickému rozlišení návštěvy od zhlédnutí se v rámci služby TOPlist používá anonymní cookie „ui". Jedná se o náhodné číslo mezi 1 až 65 000. Na straně návštěvníka měřené webové stránky se ukládá do prohlížeče s platností 30 dní, na straně serveru pak s platností 30 minut od posledního požadavku. Při vstupu návštěvníka na měřenou stránku se IP adresa zařízení a náhodná cookie na třicet minut uloží do paměťové databáze kontrolovaného subjektu. V této fázi je vyhodnoceno, zda se jedná o návštěvu, či zhlédnutí. IP adresy jsou ukládány po určitou dobu a přístup k nim má uživatel služby TOPlist.

K posouzení toho, zda kontrolovaná osoba zpracovává osobní údaje návštěvníků webových stránek uživatelů služby TOPlist (provozovatelů webových stránek), bylo nezbytné vyhodnotit, zda lze shromažďované informace přiřadit k identifikované nebo identifikovatelné fyzické osobě.

Identifikovanou je taková fyzická osoba, jejíž identitu lze na základě shromážděných informací přímo určit (tj. je k dispozici jedinečný identifikátor, jako např. rodné číslo anebo jedinečná kombinace identifikátorů, např. jméno, příjmení, adresa). Identifikovatelnou je pak ta fyzická osoba, u které shromážděné informace samy o sobě k přímému určení totožnosti nevedou, avšak na jejich základě (s využitím dalších dostupných informací a prostředků) je možné totožnost osoby určit. Jednoznačným určením fyzické osoby se přitom nerozumí pouze občanskoprávní identita fyzické osoby. Zejména v prostředí internetu může v určitých případech postačovat jednoznačná individualizace uživatele na základě určitého prvku. V souladu s recitálem 26 obecného nařízení je pro identifikovatelnost určité osoby postačující například výběr vyčleněním. Individualizace tak může být učiněna spojením údajů s individuálními identifikátory, například s IP adresou, MAC adresou, případně jiným identifikátorem zařízení, zpravidla používaným fyzickými osobami.

V této souvislosti bylo také nezbytné zdůraznit, že v čl. 4 bodu 1 GDPR se výslovně uvádí, že fyzická osoba je identifikovatelná například odkazem na síťový identifikátor. Ačkoli je IP adresa jako síťový identifikátor primárně technickým údajem zařízení, je zpravidla nezbytné ji považovat za osobní údaj. To platí zejména v případě, je-li pravděpodobné, že dané zařízení je ve vlastnictví konkrétní fyzické osoby.

V případě, že určitá IP adresa sama o sobě neposkytuje trvalou identifikaci zařízení připojeného k síti, je v souladu s recitálem 26 obecného nařízení nutno vzít v úvahu všechny rozumně předpokládatelné prostředky použitelné správcem či třetí osobou. IP adresa je osobním údajem pro každého, kdo má či může reálně předpokládat, že existuje legální a reálná možnost jejího přiřazení ke konkrétním osobám, a to bez ohledu na to, kým je takové přiřazení provedeno.

Není tedy rozhodující, zda je tato identifikovatelnost přímá, tj. že správce spojení údajů provede sám na základě informací, kterými disponuje nebo které může získat, nebo nepřímá, tj. že pro ztotožnění osoby je nutno využít součinnosti více subjektů. K těmto závěrům dospěl ostatně Soudní dvůr Evropské unie (dále jen „SDEU“) již ve vztahu ke směrnici 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. Konkrétně v rozsudku ze dne 24. listopadu 2011 ve věci C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL a v rozsudku ze dne 19. října 2016 ve věci C-582/14, Breyer v. Bundesrepublik Deutschland.

Kontrolující na základě výše uvedeného konstatovali, že kontrolovaný subjekt zpracovává osobní údaje ve smyslu čl. 4 bodu 1 a čl. 4 bodu 2 obecného nařízení.

V průběhu kontroly upravil kontrolovaný subjekt službu TOPlist tak, že všechny získané IP adresy jsou automaticky anonymizovány. Anonymizace je prováděna před jakýmkoliv dalším statistickým zpracováním dat, a to tak, aby zpětná identifikace subjektu údajů nebyla (s přihlédnutím k dostupné technologii) možná.

Kontrolou bylo zjištěno, že technická a organizační opatření, přijatá za účelem zajištění bezpečnosti zpracovávaných osobních údajů návštěvníků webových stránek, kontrolovaná osoba zdokumentovala v Interních pravidlech pro nakládání s osobními údaji. Tato opatření byla popsána i v záznamech o činnostech zpracování vedených společností jako zpracovatelem osobních údajů dle čl. 30 bodu 2 obecného nařízení. Přijatá technická a organizační opatření byla

vyhodnocena jako odpovídající. Úřad v souvislosti s předmětným zpracováním osobních údajů nezjistil porušení GDPR.

Inspektor Daniel Rovan

Založení osobního běžného účtu bankou bez vědomí a žádosti klienta (UniCredit Bank, a.s.)

Kontrola byla provedena na základě stížnosti, ve které stěžovatel uvedl a doložil, že mu UniCredit Bank, a.s. (dále jen „kontrolovaná osoba") bez jeho žádosti a zájmu založila osobní běžný účet. Kontrolovaná osoba měla k dispozici jeho osobní údaje potřebné k založení účtu, protože figuroval jako disponent firemního účtu svého zaměstnavatele, vedeného kontrolovanou osobou.

Kontrolovaná osoba ke stížnosti uvedla, že byl stěžovateli na pobočce jeho bankéřkou založen běžný účet U konto s pojištěním U5 od AXA Pojišťovny, což doložila záznamem v kontaktní historii. Účet byl údajně zatížen exekucí, a proto se na něm neúčtovaly poplatky.

Kontrolovaná osoba během celé existence účtu klienta/stěžovatele opakovaně oslovovala s obchodními nabídkami, návrhy na změnu Obecných či Produktových obchodních podmínek, upozorňovala na zrušení pobočky, kde byl soukromý účet veden a na odstávky systémů do Online Banking. Komunikace částečně souvisela také s firemním účtem, neboť banka používá Online Banking jako komunikační kanál, nehledě na konkrétní produkty.

Založené pojištění U5 bylo dle vyjádření stěžovatele pro neplacení pojistného zrušeno od počátku, o čemž AXA Pojišťovna informovala klienta písemně. Poplatky se účtovaly od března 2018, jiné pohyby na účtu nebyly. Od 21. června 2017 do data změny bankovního systému dne 9. října 2017 neevidovala banka na účtu žádné transakce, proto se žádný výpis negeneroval. To kontrolovaná osoba doložila opisem obratů z období 6. října 2017 až 30. listopadu 2018, tedy do uzavření účtu.

Dne 9. října 2018 byl stěžovatel kontrolovanou osobou osloven v souvislosti s vymáháním nepovoleného debetu 1 456 Kč. Stěžovatel na základě zaslané upomínky podal stížnost. Vzhledem k tomu, že se kontrolované osobě nepodařilo smluvní dokumentaci dohledat ani v elektronickém, ani ve fyzickém archivu, v důsledku čehož nemohla prokázat, že byla s klientem smlouva o vedení účtu uzavřena, banka stížnost uznala jako oprávněnou. Účet byl zrušen k 20. listopadu 2018, debet vyrovnán a byly rovněž vymazány veškeré s tím související záznamy v příslušných registrech. Bylo zajištěno smazání záznamů v Bankovním registru klientských informací a Registru FO vedených v SOLUS. Bankéřka, které se toto pochybení týkalo, byla v době šetření stížnosti již ve výpovědní době.

Případ byl kontrolovanou osobou vyhodnocen jako neoprávněné a účelové založení konta. O výsledku šetření vyrozuměla kontrolovaná osoba stěžovatele dne 19. listopadu 2018, kdy mu bylo e-mailem sděleno: … *jak jsme ověřili, Účet byl založen chybně ze strany Banky. Na základě Vašeho upozornění jsme zajistili vrácení všech poplatků včetně debetních úroků a následně bude Účet uzavřen. Současně potvrzujeme, že jsme zajistili odstranění negativních záznamů z bankovního registru. Přijměte prosím naši upřímnou omluvu za vzniklé pochybení.*

Kontrolovaná osoba uvedla, že šetření stížnosti neodhalilo účast další osoby na tomto pochybení.

Dokumentace k založení běžného účtu byla v souladu s kompetenčními pravidly banky podepisována jedním pracovníkem. Účet založila oprávněná bankéřka, pracovní poměr této zaměstnankyně v bance skončil výpovědí pro porušení povinností vyplývajících z právních

předpisů vztahujících se k jí vykonávané práci zvlášť hrubým způsobem. Výpověď se týkala jiných pochybení bankéřky a se šetřenou stížností nesouvisela.

Z vyjádření kontrolované osoby tedy vyplynulo, že se nepodařilo smluvní dokumentaci dohledat ani v elektronickém, ani ve fyzickém archivu, v důsledku čehož nemohla prokázat, že byla s klientem smlouva o vedení účtu uzavřena. Sama banka stížnost uznala jako oprávněnou. Účet byl zrušen, debet vyrovnán a byly rovněž vymazány veškeré s tím související záznamy v příslušných registrech.

Kontrola konstatovala porušení:

- čl. 5 bodu 1 písm. a) obecného nařízení, neboť kontrolovaná osoba žádným způsobem neprokázala zákonné a korektní zpracování osobních údajů stěžovatele k danému účelu,
- čl. 5 bodu 1 písm. b) obecného nařízení, neboť shromažďovala a zpracovávala jeho osobní údaje i pro jiný než výslovně legitimní účel,
- čl. 5 bodu 1 písm. f) obecného nařízení, když neprokázala dodržení interních předpisů, popsaných v kontrolních zjištěních, čímž nezajistila dodržování zavedených technických a organizačních opatření,
- čl. 6 bodu 1 obecného nařízení, protože nebylo prokázáno, že v případě stěžovatele kontrolovaná osoba splnila některou z nutných podmínek zákonnosti zpracování osobních údajů uvedených v obecném nařízení.

Vzhledem k tomu, že tento závadný stav kontrolovaná osoba napravila před zahájením kontroly, Úřad věc odložil, aniž by zahájil řízení, protože s ohledem na uvedené nebylo zahájení správního řízení podle § 40 zákona č. 101/2000 Sb. důvodné.

Zpracování osobních údajů (prováděné přímo kontrolovaným nebo jeho jménem), se zaměřením na členskou základnu, čekatele na členství, zájemce o členství, příznivce a jiné oslovované osoby (potenciální voliči) SPD – Tomio Okamura

Kontrola byla provedena na základě kontrolního plánu Úřadu pro rok 2019, do kterého byla zařazena s ohledem na aktuální téma spravedlivé volby v rámci celé Evropské unie.

Předmětem bylo dodržování povinností stanovených kontrolované osobě obecným nařízením při zpracování osobních údajů prováděném buď přímo kontrolované osobě nebo jejím jménem, se zaměřením na členskou základnu, čekatele na členství, zájemce o členství, příznivce a jiné oslovované osoby (potenciální voliči) kontrolované osoby.

Kontrolovaná osoba zpracovává v rámci své činnosti čtyři různé databáze, pro které má vypracovány záznamy o zpracování. Dokumenty uvádí rozsah zpracovávaných osobních údajů, a to *jméno*, *příjmení*, *trvalé bydliště*, *doručovací adresa*, *datum narození*, *e-mailová adresa*, *telefonní číslo*, *vzdělání*, *podpis*, *profese a povolání*, *politické názory a trestní delikty*. Zákonným důvodem zpracování osobních údajů je splnění právní povinnosti a udělený souhlas subjektu údajů. Osobní údaje jsou uloženy elektronicky i analogově (v papírové formě).

Jako místo uložení je v dokumentu uvedeno cloudové úložiště (pro osobní údaje v elektronické podobě). Osobní údaje v papírové formě jsou uloženy v poslaneckém klubu strany v budově Parlamentu České republiky (kartotéka).

Lhůta pro výmaz osobních údajů je uvedena pět let po ukončení členství, resp. nepřijetí čekatele za člena. Lhůta pro výmaz osobních údajů u dárců je uvedena dva roky od uplynutí lhůty pro daňovou evidenci stanovenou daňovými předpisy.

K osobním údajům mají přístup pouze oprávněné osoby. Zpracování osobních údajů je manuální.

Dokumenty dále obsahují informaci o existenci 34 zpracovatelů osobních údajů, dokument uvádí jejich výčet. Osobní údaje nejsou předávány mimo Evropskou unii a v dokumentech jsou uvedena ochranná a bezpečnostní opatření.

Kontrolovaná osoba má schválenu *Interní směrnici o ochraně osobních údajů*, která upravuje povinnosti zaměstnanců při ochraně osobních údajů. Její nedodržení je vázáno smluvní pokutou a úhradou vzniklé škody. Směrnice uvádí mimo jiné výčet povinností odpovědných osob, a to např. 1x za rok provést interní audit dodržování postupů zpracování, bezpečnosti a uložení osobních údajů, seznámení a proškolení všech zaměstnanců se směrnicí.

Kontrolovaná osoba předložila Úřadu *smlouvy o zpracování osobních údajů*, které má uzavřeny s fyzickými osobami podnikajícími. Účelem smlouvy je *mzdová agenda*, *personální agenda a provozní agenda správce v souladu s příkazní smlouvou a s obecně závaznými právními předpisy*. Bod 2.3. smlouvy obsahuje ujednání: *Předmětem zpracování Osobních údajů na základě Smlouvy jsou citlivé údaje ve smyslu Nařízení*. K tomu kontrolovaná osoba uvedla, že *tento bod se týká zvláštní kategorie osobních údajů (citlivých údajů), a to politických názorů a trestních deliktů, jelikož členství v politickém hnutí je vázáno na trestní bezúhonnost a taktéž v politických názorech či neúčast v politických uskupeních, které by mohly být v kolizi se zákonem či politickými názory hnutí.*

Dále je ve smlouvě uvedeno, že zpracování osobních údajů bude bezplatné. Nalezneme zde ujednání o povinnosti zavedení *vhodných technických, organizačních, personálních a jiných vhodných opatření*, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům a k datovým nosičům. Obsahuje také mimo jiné ujednání o zachování mlčenlivosti.

Další zpracovatelskou *Smlouvu na zajištění služeb*, jejímž předmětem je *ke svému softwaru připojovat projekt pro klienta na ovlivňování veřejného mínění na sociálních sítích a v diskusních fórech na internetu a zároveň ho spravovat*, má kontrolovaná osoba uzavřenou na vyhodnocování zásahů v rámci sociálních sítí a určování strategie.

Kontrola prověřila plnění povinností správce osobních údajů stanovených zejména v čl. 5 (zásady zpracování osobních údajů), čl. 6 (zákonnost zpracování), čl. 9 (zvláštní kategorie osobních údajů) a čl. 32 obecného nařízení (zabezpečení).

Z kontrolních zjištění vyplynulo porušení čl. 5 bodu 1 písm. c), d), e), protože kontrolovaná osoba v rozporu s čl. 5 bodu 1 písm. c) GDPR zpracovává osobní údaje skupiny dárci nad rámec nutný k jednoznačné identifikaci smluvní strany.

Dále pak bylo zjištěno, že kontrolovaná osoba nezpracovávala přesné osobní údaje dle požadavku čl. 5 bodu 1 písm. d) obecného nařízení, což bylo ověřeno v případě konkrétního člena, a rovněž kontrolovaná osoba nastavila lhůtu pro výmaz osobních údajů nepřijatých zájemců o čekatelství a nepřijatých čekatelů v rozporu s čl. 5 bodu 1 písm. e) obecného nařízení. Totéž se přitom vztahuje i na skupinu dárců, kde byla lhůta stanovená právními předpisy kontrolovanou osobou nadbytečně prodloužena o dva roky.

Kontrolou bylo dále zjištěno porušení čl. 6 obecného nařízení, neboť kontrolovaná osoba nesprávně určila právní titul, na jehož základě osobní údaje zpracovává. Zpracování osobních údajů členů se neděje na základě právního titulu čl. 6 bodu 1 písm. c) , ale děje se tak na základě právního titulu dle čl. 6 bodu 1 písm. f) GDPR.

Vzhledem k předmětu kontroly, zda není v rámci zpracování osobních údajů použito nekorektních praktik ovlivňujících spravedlivou volbu, nebylo kontrolou učiněno žádné zjištění.

Inspektorka Jiřina Rippelová

Kontrola zpracování osobních údajů prováděného politickou stranou se zaměřením na členskou základnu i na osoby stojící mimo ni (tj. členové, čekatelé na členství, zájemci o členství, příznivci a jiní oslovovaní – potencionální voliči)

Úřad provedl v roce 2019 kontrolu politické strany TOP 09 (dále také „kontrolovaná osoba"). Kontrola byla zahájena a provedena na základě kontrolního plánu Úřadu pro rok 2019. Do kontrolního plánu byla zařazena s ohledem na aktuální téma spravedlivých voleb v rámci celé Evropské unie. Byla definována jako kontrola zpracování osobních údajů politickou stranou nebo hnutím se zaměřením na cílené oslovování jednotlivců pro politické účely v návaznosti na právní úpravu dle obecného nařízení.

V jejím rámci se kontrolující zaměřili na cílené oslovování jednotlivců (členů a uchazečů o členství, podporovatelů a příp. dalších oslovovaných – potencionálních voličů) pro politické účely, a to bez ohledu na to, zda oslovování provádí přímo kontrolovaný subjekt, nebo jiný subjekt jeho jménem.

Úřad zjistil, že kontrolovaná osoba shromažďuje informace o zájemcích o zasílání newsletteru, podporovatelích a členech politické strany, resp. uchazečích o členství.

Zájemci o zasílání newsletteru (registrují svoji e-mailovou adresu), podporovatelé (registrují se prostřednictvím webové stránky nebo portálu my.top09.cz) a členové strany, resp. zájemci o členství vyplňují přihlášku. Politická strana TOP 09 také využívá sociálních sítí (Facebook, Instagram, Twitter), kde má tzv. fanouškovskou stránku, resp. účet. Zpracovává tedy osobní údaje zájemců o zasílání newsletteru, podporovatelů, uchazečů o členství a členů a dále se podílí na zpracování osobních údajů uživatelů sociálních sítí, kteří navštívili její fanouškovské stránky.

Kontrolovaná osoba je tedy s ohledem na výše uvedené v postavení správce osobních údajů, resp. ve vztahu k osobám, které jsou oslovovány prostřednictvím kampaní zadaných na sociálních sítích, v postavení společného správce. Ve smyslu rozsudku velkého senátu Soudního dvora Evropské unie ze dne 5. června 2018 ve věci C-210/16 (Unabhangiges Landes zentrum fur Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH) je totiž za správce osobních údajů, resp. společné správce nutno považovat jak společnost Facebook Ireland Ltd. a Facebook Inc., tak i jednotlivé vlastníky fanouškovských stránek (profilů) na sociální síti Facebook.

Ačkoli tedy v tomto případě kontrolovaná osoba fakticky nedisponuje informacemi o identitě osob, které byly osloveny (tj. osobními údaji), je třeba ji jako vlastníka fanouškovské stránky považovat za společného správce spolu s uvedenými společnostmi, které tuto sociální síť provozují.

V souvislosti s předmětným zpracováním bylo kontrolou zjištěno, že kontrolovaná osoba využívá služeb zpracovatelů a spolupracuje s dalším společným správcem. Úřad přitom také zjistil, že uzavřela smlouvy vyhovující požadavkům čl. 26 bodu 1 a čl. 28 bodu 3 obecného nařízení. Předmětné zpracování je dle kontrolních zjištění založeno na souhlasu se zpracováním osobních údajů, resp. oprávněném zájmu správce a rovněž na plnění smlouvy.

Kontrolovaná osoba navíc poskytuje subjektům údajů, od nichž shromažďuje osobní údaje, informace v rozsahu a způsobem odpovídajícím požadavkům uvedeným v čl. 12 bodu 1 a bodu 13.

Porušení nebylo zjištěno ani v oblasti zabezpečení osobních údajů, tj. povinností vyplývajících z čl. 32 GDPR.

Kontrolující však odhalili porušení povinnosti podle čl. 30 obecného nařízení, neboť předložené záznamy o činnostech zpracování neobsahovaly veškeré požadované náležitosti. Jednu kategorii subjektů údajů (zájemce o zasílání newsletteru) neobsahovaly vůbec.

Vzhledem k tomu, že kontrolovaná osoba závadný stav neprodleně napravila, Úřad neuložil opatření k odstranění zjištěných nedostatků a od uložení pokuty upustil.

Kontrola dodržování povinností stanovených obecným nařízením při zpracování genetických údajů, jakožto zvláštních kategorií osobních údajů

ÚOOÚ na základě svého kontrolního plánu provedl kontrolu společnosti Forenzní DNA servis, s.r.o. (dále také „kontrolovaná osoba"), jejímž předmětem bylo zpracování osobních údajů u společnosti testující genetické údaje (DNA), tedy zvláštní kategorie osobních údajů.

Úřad zjistil, že kontrolovaná osoba poskytuje svým klientům službu v podobě určování paternity a genetické genealogie. Určování otcovství, popř. mateřství a příbuzenství představuje cca dvacet procent činnosti kontrolované osoby. Hlavním těžištěm činnosti je výzkum a vývoj, např. v oblasti kosterních pozůstatků či zvlášť ohrožených živočišných druhů. Uvedené procento představuje v praxi v průměru deset zájemců o test paternity a deset zájemců o test příbuzenství za měsíc. Každému testování, tj. analýze DNA, vždy předchází požadavek (objednávka) subjektu údajů (zákazníka). Objednávku lze učinit osobně, telefonicky, e-mailem, faxem či vyplněním elektronického objednávkového formuláře na webových stránkách kontrolované osoby, resp. na webových stránkách elektronického obchodu 4N6shop.cz. Poté je zákazníkům předán/odeslán požadovaný formulář, informace pro subjekty údajů o nakládání se vzorky DNA, odběrové soupravy v odpovídajícím množství a návod k použití odběrové soupravy.

Za účelem určování paternity a genetické genealogie, které kontrolovaná osoba poskytuje jako službu svým klientům (zákazníkům), shromažďuje a dále zpracovává identifikační a kontaktní údaje v rozsahu jméno a příjmení, e-mailová adresa, telefonní kontakt, kontaktní adresa pro zaslání tištěných výsledků analýz a podpis. Uvedenému rozsahu osobních údajů pak odpovídá i obsah formulářů, které kontrolovaná osoba pro shromažďování osobních údajů zákazníků používá.

Zpracovávány jsou též genetické údaje, konkrétně vzorky získané stěrem z ústní dutiny. Co se týče samotné analýzy DNA, kontrolovaná osoba testuje pouze nekódující část DNA, nepracuje tedy např. s informacemi o zdravotním stavu. Výsledek testu příbuzenského vztahu (například paternity) pak vždy vyjadřuje pouze určitou míru pravděpodobnosti, s jakou jsou srovnávané vzorky ve vzájemném poměru (používá se tzv. „paternitní index").

Právní titul pro předmětné zpracování osobních údajů byl v daném případě kontrolou shledán v čl. 6 bodu 1 písm. b) obecného nařízení (plnění smlouvy), v části, kdy dochází ke zpracování osobních údajů nezbytných pro plnění smlouvy, jejíž stranou je subjekt údajů (klient), a dále v čl. 6 bodu 1 písm. a) a čl. 9 bodu 1 písm. a) GDPR (souhlas, resp. výslovný souhlas). Jedná se konkrétně o vztah ke zpracování zvláštních kategorií údajů (informací ze vzorku DNA).

Kontrolující dále posoudili také plnění informační povinnosti. Zjistili, že informace o postupu při testování jsou dostupné prostřednictvím internetových stránek kontrolované osoby, resp. internetových stránek elektronického obchodu, jehož prostřednictvím kontrolovaná osoba své

služby nabízí. Před objednáním konkrétního typu testu se tak může klient seznámit s podrobným popisem postupu od podání žádosti přes provádění testů až po odeslání či předání výsledků a následné vymazání a likvidaci údajů a vzorků.

Klientům je k dispozici také formulář určený k uplatnění jejich práv. Kontrolovaná osoba tedy poskytuje veškeré relevantní informace o způsobu zpracování osobních údajů i o právech subjektů údajů.

Kontrolovaná osoba v průběhu kontroly předložila kontrolujícím sadu interních předpisů, v nichž jsou popsány všechny aspekty zpracování osobních údajů, definován jejich rozsah nezbytný pro plnění činností kontrolované osoby. Jsou zde uvedeny právní důvody pro zpracování a kontaktní údaje na kontrolovanou osobu, jakožto správce předmětných osobních údajů. Kontrolovaná osoba tím tak splnila mj. svoji povinnost dle čl. 30 obecného nařízení, a to vést záznamy o činnostech zpracování.

V rámci posouzení plnění povinnosti přijmout opatření k zajištění bezpečnosti zpracovávaných osobních údajů kontrolující hodnotili jak fyzické zabezpečení prostor, tak technická a organizační opatření. Dospěli k závěru, že kontrolovaná osoba neporušila povinnosti stanovené obecným nařízením.

Inspektor František Bartoš

Zpracování osobních údajů vlastníků průmyslových práv – fyzických osob, uváděných v rejstřících průmyslových práv (IPTR, s.r.o.)

Kontrola byla provedena na základě kontrolního plánu Úřadu pro rok 2019 a podnětu zaslaného Úřadem průmyslového vlastnictví (dále jen „ÚPV“).

Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených obecným nařízením při zpracování osobních údajů vlastníků průmyslových práv – fyzických osob, uváděných v rejstřících průmyslových práv kontrolovanou osobou.

ÚPV sdělil, že kontrolovaná osoba zasílá vlastníkům průmyslových práv komerční nabídky publikace (registrace) jejich průmyslových práv na svých webových stránkách. Jak však kontrolovaná osoba sama v písemném oslovení s nabídkou registrace přiznává, informace získává z rejstříků mezinárodních patentů publikovaných podle Smlouvy o patentové spolupráci nebo ochranných známek přihlášených dle Madridské dohody o mezinárodním zápisu továrních nebo obchodních známek a Protokolu k této dohodě u Světové organizace duševního vlastnictví, se sídlem Ženeva, Švýcarsko.

Osobní údaje uváděné v jednotlivých rejstřících průmyslových práv slouží pro informaci třetích osob a jejich účelem je vytvoření spolehlivého zdroje informací a poskytnutí právní jistoty, která je nezbytná pro ochranu zájmů vlastníků průmyslových práv, poctivost transakcí a správné fungování průmyslových práv na trhu. Z povahy průmyslových práv, která jsou nehmotnými statky, vyplývá, že údaje o nich vedené v jednotlivých rejstřících jsou jediným zdrojem informací, který umožňuje poskytnutí úplného obrazu konkrétního práva a umožňuje každé třetí osobě se s těmito informacemi seznámit. Ze stížností dotčených osob, držitelů autorských práv, je zřejmé, že obdržené nabídky kontrolované osoby obsahují také požadavek na úhradu částky za zveřejnění ve vlastním registru, a to ve výši 2 795 AUD, 1 954 EUR, 18 785 SEK nebo 2 356 USD.

Kontrolovaná osoba v průběhu kontroly opakovaně neposkytovala součinnost, za což jí byly v souladu s kontrolním řádem uloženy pravomocné pokuty v celkové výši 100 000 Kč, přičemž vymáhání pokut bylo předáno Celní správě.

Ze stížností, které Úřad obdržel prostřednictvím ÚPV od jednotlivých stěžovatelů, bylo možné dovodit, že jednotlivé subjekty údajů požadují od kontrolované osoby výmaz osobních údajů ve smyslu čl. 17, práva na omezení zpracování dle čl. 18, resp. vznesly námitku dle čl. 21 GDPR.

V rámci kontroly však kromě jedné e-mailové korespondence, která se týkala dvou stěžovatelů, kteří byli vyzváni k doplnění podnětu a kteří svým podpisem akceptovali navrženou smlouvu, nebyla zjištěna žádost dle článků 17, 18, resp. čl. 21 obecného nařízení.

S ohledem na

- způsob shromažďování a využívání osobních údajů adresátů nabídkových dopisů, včetně informace, kterou kontrolovaná osoba v rámci nabídkového dopisu adresátům sdělovala o zdroji jejich osobních údajů,
- stanovený účel, včetně právního základu (smluvní nabídka),
- skutečnost, že kontrolou nebylo možno potvrdit, zda využité adresní údaje kontrolovaná osoba dále zpracovává, tedy podezření, že došlo k porušení povinností správce dle čl. 14 obecného nařízení, v případě, že osobní údaje nebyly získány od subjektu údajů, nemohli kontrolující konstatovat porušení obecného nařízení.

Zpracování osobních údajů prostřednictvím webového portálu hlidacvyboru.cz (Open Data Company s.r.o.)

Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených obecným nařízením v souvislosti se zpracováním osobních údajů prostřednictvím webového portálu www.hlidacvyboru.cz, který Open Data Company s.r.o. (dále také „kontrolovaná osoba“) provozuje.

Stěžovatel ve svém podnětu uvedl, že na výše uvedených webových stránkách provozovatel zveřejňuje informace o členech výborů společenství vlastníků, a to včetně informace i o něm, jako o členu výboru Společenství vlastníků v Praze 8 (dále také „SVJ“). Jedná se o jméno, příjmení, titul, funkce v SVJ a informace o zdrojích dat. Stěžovatel uvedl, že jde o nepřiměřený zásah do jeho soukromého života s tím, že společnost, která webové stránky provozuje, nemá se společenstvím nic společného.

Stěžovatel dále doložil, že podal proti zpracování jeho osobních údajů námitku a požádal společnost o výmaz svých osobních údajů. Do doby, než bude námitka vyřešena, uplatnil právo na omezení zpracování podle čl. 18 obecného nařízení.

V provedené kontrole bylo zjištěno, že kontrolovaná osoba stěžovateli na jeho žádost o výmaz osobních údajů odpověděla. Podle ní jsou osobní údaje týkající se jeho osoby tzv. veřejnými neomezenými informacemi, tj. těmi, které veřejná správa zveřejňuje bez jakéhokoli omezení, a přístup má kdokoli ke všem informacím, bez dalších podmínek. V další části odpovědi kontrolovaná osoba stěžovateli sdělila, že jsou splněny předpoklady pro zpracování osobních údajů stěžovatele ve veřejném rejstříku na základě oprávněného zájmu, bez nutnosti získání souhlasu subjektů podle obecného nařízení.

Kontrolovaná osoba dále sdělila, že posoudila její oprávněný zájem ke zveřejnění osobních údajů stěžovatele, a po zdokumentování je připravena předložit tento závěr v souladu se zásadou odpovědnosti ÚOOÚ ke kontrole.

V rámci kontroly Úřad dále zjistil, že kontrolovaná osoba získává informace z veřejných registrů, a to z obchodního rejstříku – registr SVJ, z insolvenčního rejstříku a dalších, přičemž tuto činnost nabízela v rámci svého podnikání.

Stěžovatel opakovaně vznesl u správce námitku podle čl. 21 obecného nařízení a požádal o omezení zpracování podle čl. 18 obecného nařízení, dokud nebude o námitce rozhodnuto, a poté o výmaz z webové stránky hlidacvyboru.cz.

Ve svém vyjádření kontrolovaná osoba sdělila, že neakceptuje požadavek stěžovatele, neboť zpracovává osobní údaje na základě svého oprávněného zájmu, přičemž se opírá mimo jiné o balanční test. Z toho vyplynulo, že splňuje předpoklady pro zpracování osobních údajů získaných z veřejných rejstříků na základě oprávněného zájmu bez nutnosti získání souhlasu dotčených osob.

Kontrolou bylo konstatováno, že kontrolovaná osoba porušila svoji povinnost dle čl. 6 bodu 1 písm. a) obecného nařízení, tedy zpracovávala osobní údaje bez souhlasu stěžovatele, přičemž jí nenáleží žádný z jiných právních titulů.

Poté co stěžovatel vznesl námitku proti zpracování jeho osobních údajů ve smyslu čl. 21 bodu 1 GDPR, nemohla kontrolovaná osoba jeho osobní údaje na webových stránkách hlidac vyboru.cz dále zpracovávat, jelikož její odůvodnění oprávněných zájmů na zveřejnění osobních údajů stěžovatele jako člena výboru SVJ není v souladu s obecným nařízením. Kontrolovaná osoba také dostatečně neprokázala existenci jiných závažných důvodů pro zpracování osobních údajů stěžovatele na webových stránkách hlidacvyboru.cz, které by byly v souladu s obecným nařízením.

Tím, že kontrolovaná osoba nesplnila požadavek stěžovatele na výmaz jeho osobních údajů, porušila čl. 17 bod 1 písm. c) obecného nařízení.

Kontrolovaná osoba podala proti zjištěním uvedeným v protokolu o kontrole námitky, které byly předsedkyní Úřadu zamítnuty a protokol o kontrole potvrzen. V následném správním řízení byla kontrolované osobě uložena povinnost ukončit zpracování osobních údajů stěžovatele, zlikvidovat je a následně o tom stěžovatele informovat. Kontrolovaná osoba tuto povinnost splnila.

Inspektor Petr Krejčí

Zpracování osobních údajů vypovídajících o zdravotním stavu v rámci poskytování ubytovacích služeb (MERKURIA UNION, s.r.o.)

Na základě podnětu postoupeného Odborem sociálních věcí Krajského úřadu Pardubického kraje provedl Úřad kontrolu společnosti MERKURIA UNION, s.r.o., se sídlem Nová Ves u Litomyšle. Kontrola zjistila, že uvedená společnost poskytuje ve svém Domově seniorů „Pohodlí" i sociální služby na základě několika živnostenských oprávnění. Konkrétně se jednalo o hostinskou činnost, koupi zboží za účelem jeho dalšího prodeje a prodej, správu a údržbu nemovitostí a realitní činnost. Ubytovací zařízení poskytuje služby 55 osobám, které jsou v různém stupni závislé na pomoci druhé osoby a jsou jim vypláceny přiznané příspěvky na péči od Úřadu práce ČR podle stupně závislosti.

Přitom bylo zjištěno, že ubytovatel MERKURIA UNION, s.r.o., shromažďuje o ubytovaných osobách i citlivé údaje týkající se zdravotního stavu. Ve „Smlouvě o ubytování a stravování" ukládá ubytovaným povinnost, aby při nástupu do ubytovacího zařízení předložili lékařskou zprávu a údaje o kontaktní osobě, respektive příbuzném. Ve složkách ubytovaných osob byly také nalezeny dokumenty s názvem „Sociální šetření", kde je stručně zaznamenáno, v jakých oblastech potřebuje ubytovaná osoba pomoc druhé osoby, jsou zde uvedeny informace o zdravotním stavu a kontakt na osobu blízkou. V ubytovacím zařízení poskytuje pomoc ubytovaným osobám 12 asistentů sociální péče, kteří přicházejí do kontaktu s osobními údaji ubytovaných osob.

Vzhledem k tomu, že MERKURIA UNION, s.r.o., nemá oprávnění k poskytování zdravotní a sociální péče, bylo zde podezření, že dochází i k neoprávněnému shromažďování citlivých osobních údajů ze strany ubytovatele. Úřad byl proto požádán o prošetření výše uvedených podnětů.

Předmětem kontroly ÚOOÚ bylo dodržování povinností stanovených obecným nařízením a zákonem č. 110/2019 Sb., o zpracování osobních údajů, který s účinností od 24. 4. 2019 nahradil zákon č. 101/2000 Sb., při zpracování osobních údajů klientů ubytovaných a stravujících se v Domově seniorů „Pohodlí". Tam jsou jim poskytovány i zdravotní a sociální služby bez zákonného oprávnění ve smyslu ustanovení § 78 zákona č. 108/2006 Sb., o sociálních službách, včetně zpracování zvláštních kategorií osobních údajů, které by mělo být založeno na právním titulu dle čl. 9 bodu 2 písm. g) obecného nařízení, v rámci podnikatelské činnosti správce.

Jestliže kontrolovaná osoba poskytuje pro ubytované klienty ve svém zařízení kromě stravování také zdravotní a sociální služby bez oprávnění k jejich poskytování dle ustanovení § 11 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) a § 78 zákona č. 108/2006 Sb., o sociálních službách (ať už to bylo v zařízení Domova seniorů „Pohodlí" do června 2018 prostřednictvím zaměstnanců a poté jejich změnou na asistenty sociální péče, podnikající podle zvláštního zákona, a na tuto péči byly/jsou vypláceny přiznané příspěvky na péči od Úřadu práce ČR podle stupně závislosti na pomoci druhé osoby bez ohledu, zda na účet kontrolované osoby nebo nyní na účet jednoho z asistentů sociální péče, a má tak kontrolovaná osoba přístup zejména ke zvláštním kategoriím osobních údajů uvedených v listinách založených ve „zdravotnické dokumentaci pacienta" nebo ve „spise vedeném na klienta", přičemž tak nesplnila žádnou z podmínek uvedených v článku 6 bodu 1 písm. a) až f) GDPR a nesplnila ani žádnou z výjimek zákazu zpracování zvláštních kategorií osobních údajů uvedených v článku 9 bodu 2 písm. a) až j) obecného nařízení), porušila kontrolovaná osoba zákonnost zpracování osobních údajů subjektů údajů, resp. zákaz zpracování zvláštních kategorií osobních údajů subjektu údajů.

V daném případě nebyla kontrolovaná osoba oprávněna zpracovávat ani rodná čísla klientů. To za předpokladu, měla-li v rámci svého podnikání vydána pouze živnostenská oprávnění na ubytovací a stravovací služby a nesplnila tak rovněž podmínky zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel).

Pokud kontrolovaná osoba využívá své sídlo, v němž je umístěn Domov seniorů „Pohodlí", pro účely poskytování sociální péče a aktivně se i na této péči podílí, včetně prezentace své činnosti, je povinna dodržovat zákonnost zpracování osobních údajů. Jedná se o splnění povinností správce osobních údajů podle obecného nařízení, zákona č. 110/2019 Sb., ve spojení se zákonem č. 108/2006 Sb., o sociálních službách. Kontrolovaná osoba je povinna zajistit, aby tuto činnost vykonávala pouze osoba k tomu oprávněná, zejména podle zákona č. 108/2006 Sb. (§ 78) a zákona č. 372/2011 Sb. (§ 11), bez přístupu neoprávněných osob ke zdravotnické dokumentaci vedené o pacientovi a k osobním spisům klientů; včetně prokazatelného seznámení osob s postupy při nakládání s dokumenty a tím garantovat ochranu osobních údajů pacientů/klientů v těchto listinách uvedených.

Zejména ke zdravotnické dokumentaci vedené o pacientovi může mít přístup jen osoba ze zákona oprávněná, tj. rovněž ve smyslu ustanovení § 3 odst. 3 zákona č. 98/2012 Sb., o zdravotnické dokumentaci. Konkrétně tedy zdravotnický pracovník nebo jiný odborný pracovník, který pacientovi poskytl zdravotní službu a provedením zápisu do zdravotnické dokumentace zajistí jeho správnost svým podpisem.

Úřadem provedená kontrola podezření na nezákonné jednání kontrolované osoby potvrdila v plném rozsahu.

Inspektor zjistil závažná a dlouhodobě praktikovaná porušení výše uvedených zákonů, za která byla kontrolované osobě ve správním řízení udělena pokuta ve výši 50 000 Kč.

Zpracovávání osobních údajů osob přepravovaných v dopravních prostředcích (Dopravní podnik hl. m. Prahy, akciová společnost)

Kontrola v Dopravním podniku hl. m. Prahy, akciová společnost, (dále také „kontrolovaná osoba") byla zahájena na základě kontrolního plánu Úřadu pro rok 2019.

Kontrola byla zaměřena na to, jak si kontrolovaná osoba počínala při ochraně osobních údajů od poslední provedené kontroly v roce 2012 do současnosti.

Předmětem kontroly bylo dodržování povinností stanovených obecným nařízením ve spojení se zákonem č. 110/2019 Sb., o zpracování osobních údajů, při zpracování osobních údajů subjektů údajů v souvislosti s kontrolami jízdních dokladů a navazujícím zpracování osobních údajů a v souvislosti s nákupem časových jízdenek.

V souvislosti s vyplňováním osobních údajů zákazníka/cestujícího přímo do elektronické podoby a jeho nákupem jízdního dokladu/časové jízdenky v papírové formě u pracovníka za přepážkou režimového pracoviště, na němž proběhla fyzická kontrola, se do elektronických formulářů zapisují některé údaje. Jedná se o jméno, příjmení, datum narození, datum vystavení a datum platnosti, případně škola (IČO), školní rok, ročník u uplatněných slev studenta. Nevyplňují se předtištěné údaje o pohlaví, rodném čísle, PSČ a státu.

V průběhu kontroly byly tyto předtištěné údaje, které kontrolovaná osoba nezpracovává, z formuláře jako nadbytečné vymazány.

Obdobná režimová opatření týkající se ochrany osobních údajů jsou v souvislosti s vystavováním průkazek, sběrem žádostí o Lítačku, reklamacemi, vydáváním duplikátů průkazek s evidencí znehodnocených fundamentů, které jsou uložené na bezpečném místě (uzamčeny v cash boxech či trezorech) zavedena i na ostatních prodejních místech.

Podle provozního předpisu D 6 „Předpis pro činnost přepravní kontroly" s účinností od 1. července 2012 čl. 12 odst. 3 může přepravní kontrolor zjišťovat osobní údaje cestujících za účelem vymáhání zaplacení přirážky k jízdnému. Děje se tak z dokladu vydaného příslušným správním orgánem v rozsahu: jména, příjmení, data a místa narození, adresy pro doručování, druh a číslo dokladu, ze kterého byly osobní údaje zjištěny.

Z formuláře zápisu o provedené přepravní kontrole pořizovaném přepravním kontrolorem v souvislosti se zapsáním identifikačních údajů cestujícího, který se neprokázal platným jízdním dokladem a nezaplatil jízdné a přirážku k jízdnému, pro účel vymáhání pohledávky v soudním řízení, je zřejmé, že kontrolovaná osoba zpracovává osobní údaje. Těmi jsou číslo vydaného zápisu jako variabilní symbol pro platbu, datum, čas, linka, pověřená osoba/číslo odznaku, místo kontroly, přirážka, nesnížené jízdné, příjmení a jméno cestujícího/dlužníka, datum a místo narození, údaje zjištěné z dokladu, stát, adresa pro doručování – ulice, číslo domu, obec, tel. č./e-mail, zaškrtnutí popisu události, jízdní doklad č., zda byl odebrán, potvrzení správnosti údajů pro cestujícího, zda cestující stejnopis zápisu převzal – nepřevzal, podepsal – odmítl podepsat, služební záznam, datum podpisu cestujícího/dlužníka, podpis osoby pověřené dopravcem, jeho razítko, z druhé strany s informací pro cestující o možnostech úhrady a postupu dopravce.

Tiskopis „Prohlášení o převzetí dluhu“, který přepravní kontrolor vyplňuje ve stejném rozsahu jako u cestujícího/dlužníka, se používá v případě, že za cestujícího, který nemůže zaplatit uloženou přirážku v hotovosti na místě a nemá u sebe ani osobní doklad, dobrovolně převezme povinnost zaplatit tuto přirážku jiná osoba (neplatí pro zaplacení na místě). Musí se však jednat o osobu starší 18 let anebo v případě, že se jedná o nezletilou osobu v doprovodu zletilé osoby, s níž přepravní kontrola řeší převzetí dluhu za osobu nezletilou.

Dle formuláře zápisu o zjištění osobních údajů cestujícího, který vyplňuje Policie ČR (PČR) v případě neprokázání totožnosti cestujícího, který nezaplatil jízdné a přirážku k jízdnému přepravnímu kontrolorovi za jízdu bez platného jízdního dokladu, kontrolovaná osoba přebírá osobní údaje cestujícího v rozsahu: datum, čas, místo zjištění, příjmení, jméno, datum narození, lomítko r. č., údaje zjištěny z, trvalé bydliště – ulice č., PSČ, okres, poznámka, služební číslo a podpis, přičemž číslo za lomítkem u data narození slouží PČR pouze k ověření (pravosti) totožnosti cestujícího a kontrolovaná osoba dále v elektronické podobě tento údaj nezpracovává a v listinné podobě jej následně znečitelňuje jeho začerněním.

Je na zvážení, zda je účelné z hlediska zásady minimalizace a kontrolovanou osobou obhajitelné takovýto zavádějící údaj vůbec mít ve formuláři předepsaný, jestliže jej dále nezpracovává. Podle dokladu o zaplacení přirážky cestujícím, který při přepravní kontrole nepředložil platný jízdní doklad, zpracovává kontrolovaná osoba: číslo dokladu, datum, linku a čas, přičemž kontrolní útržek pro cestujícího obsahuje: číslo dokladu, linku, čas, číslo vozu, č. kontrolního odznaku, datum.

V souladu se zásadami zpracování osobních údajů uvedenými v článku 5 tak, jak byla kontrolovaná osoba schopna prokázat ve smyslu zásady odpovědnosti za dodržování všech pravidel stanovených obecným nařízením dle odst. 2 tohoto článku, což musí být schopna vždy doložit, neporušila zásady zpracování osobních údajů uvedených v článku 5 odst. 1. GDPR. S odkazem na článek 5 odst. 2 pak byla schopna unést odpovědnost za dodržení všech stanovených zásad přímo souvisejících s doložením zákonného zpracování osobních údajů, v souvislosti s uzavřením smlouvy se subjektem údajů o poskytnutí/poskytování služby spojené s využitím přepravy MHD a PID dopravcem, kterým je kontrolovaná osoba.

V souvislosti s aktivitami kontrolované osoby a provedením opatření již v průběhu kontroly nebylo kontrolujícími zjištěno porušení informační povinnosti vůči subjektům údajů uvedené v článku 12 odst. 1. obecného nařízení. Nebylo rovněž zjištěno porušení informační povinnosti na základě žádosti subjektu údajů podle článku 12 odst. 3 obecného nařízení.

Kontrolovaná osoba neporušila svoje povinnosti v rozsahu předmětu kontroly uvedené v článku 24 a článku 25 GDPR, jestliže garantovala, že zpracování provádí v souladu s těmito články a kontrolujícími nebylo zjištěno, že by z hlediska ochrany osobních údajů k porušení došlo.

Kontrolovaná osoba garantovala, že vede záznamy o všech činnostech zpracování ve smyslu článku 30 obecného nařízení, a v rozsahu předmětu kontroly, které se týkají zpracování osobních údajů cestujících, kterým byly vydány evidované průkazky, a týkající se zpracování osobních údajů cestujících, kteří se neprokázali platným jízdním dokladem, nezaplatili jízdné a přirážku k jízdnému a byli zaevidováni jako dlužníci, a v souvislosti s prodejem jízdních dokladů, reklamací apod., za něž odpovídá.

Kontrolovaná osoba má v současnosti nastavena svá pravidla a předpisy tak, že garantuje ve své působnosti respektování zákona č. 110/2019 Sb. i obecného nařízení.

Oddělení kontroly soukromého sektoru

Kontrola zpracování cookies u společnosti Velká Pecka s.r.o.

Na základě kontrolního plánu Úřadu pro rok 2019 provedlo oddělení kontroly soukromého sektoru kontrolu zpracování cookies[5] a jejich využití při remarketingu u společnosti Velká Pecka s.r.o. (dále také „kontrolovaná osoba").

V rámci kontroly se Úřad jako první zaměřil na právní rámec cookies. V rámci národní legislativy se jedná o § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, přičemž toto ustanovení bylo transpozicí čl. 5 odst. 3 směrnice 2002/58/ES. Na základě této směrnice byl pro cookies zaveden v národní legislativě princip opt-out, tj. uživatelé koncových zařízení museli být na ukládání cookies upozorněni, cookies byly do jejich zařízení uloženy a měla jim být dána možnost toto ukládání odmítnout. Tato směrnice byla v roce 2009 novelizována a nově byla vystavěna na principu opt-in tj., uživatelé mají nejdříve získat veškeré informace o zpracování cookies a toto zpracování následně povolit, než bude do jejich zařízení uložené.

Český zákonodárce tuto novelu do příslušného zákona č. 127/2005 Sb. sice zakotvil, nicméně nesprávným způsobem. Výsledným stavem tedy je, že národní legislativa (zákon č. 127/2005 Sb.) je v nesouladu s právním rámcem Evropské unie (směrnice 2002/58/ES), neboť na základě novelizace směrnice 2002/58/ES byl zaveden princip opt-in, avšak národní legislativa ve svém důsledku nedále pracuje s principem opt-out.

Kontrolující se tak museli vypořádat především s právní otázkou, která se týkala vztahu národního a unijního práva. Obecně je možné konstatovat, že judikatura Evropského soudního dvora zakotvuje princip přednosti unijního práva před právem národním, a to na základě judikátu Costa v. E.N.E.L., věc 6/64. Dalším právním principem je tzv. eurokonformní výklad, který vyplývá z judikátu von Colson, věc 14/83, který stanoví povinnost vykládat národní právo ve světle unijních předpisů. Kontrolující však shledali, že rozpor mezi národní a unijní legislativou je natolik závažný, že jej není možné eurokonformním výkladem překlenout.

Kontrola se zabývala také účinkem směrnic. Musela však vyhodnotit judikaturu Evropského soudního dvora (např. Marshall, C-152/84, Tullio Ratti, C-148/79 či Van Duyn, C-41/74).

Na základě těchto judikátů kontrolující konstatovali, že směrnice v zásadě nemůže mít na jednotlivce přímý účinek. Proto Úřad dospěl k závěru, že kontrola musí proběhnout ve světle národních právních předpisů.

Na základě výše uvedeného se tak kontrolující zaměřili na to, zda kontrolovaná osoba při nakládání s osobními údaji (cookies) v rámci remarketingu postupuje jak v souladu s obecným nařízením, tak v souladu se zákonem č. 127/2005 Sb.

Nejprve došli k závěru, že cookies lze podřadit pod pojem osobní údaje ve smyslu čl. 4 bod 1 obecného nařízení, a to ve spojení s recitálem 30 obecného nařízení, který uvádí, že fyzickým osobám mohou být přiřazeny identifikátory cookies. Tyto identifikátory však zanechávají takové stopy, které ve spojení s dalšími informacemi, které servery získávají, mohou vést k jednoznačnému určení konkrétní fyzické osoby a sloužit k jejímu profilování.

---

[5] Cookies jsou malé textové soubory, které se při návštěvě internetové stránky ukládají do zařízení uživatele (počítač, telefon apod.) a jsou nosičem informací o tom, které stránky uživatel navštívil a jaké informace na nich hledal. Společnosti proto cookies často využívají za účelem cílení reklamy na konkrétního uživatele. Praktický dopad na subjekt údajů je tedy takový, že jím procházené internetové stránky (např. zpravodajské weby a jiné portály, na kterých je umístěn reklamní prostor) následně zobrazují cílenou nabídku dříve navštívených internetových stránek.

Další zkoumanou otázkou bylo, zda se kontrolovaná osoba nachází v postavení správce osobních údajů ve smyslu čl. 4 bod 7 obecného nařízení. Kontrolující vyhodnotili, že kontrolovaná osoba se v postavení správce osobních údajů nachází, neboť určila účel a prostředky zpracování osobních údajů. Účelem je zde personalizace zobrazovaných reklam a přednostní nabízení zboží a prostředkem zpracování osobních údajů jsou jednotlivé služby, které kontrolovaná osoba využívá (např. Doubleclick, Custom Audiences a Lookalike Audiences).

Kontrolující v závěru svého šetření konstatovali, že kontrolovaná osoba získává osobní údaje v souladu s parametry, které jsou stanoveny § 89 odst. 3 zákona č. 127/2005 Sb., neboť poskytuje subjektům údajů informace v souladu s požadavky citovaného ustanovení. Řádně zároveň plní informační povinnost ve smyslu čl. 12–14 obecného nařízení a informuje subjekty údajů především o rozsahu a účelu zpracování osobních údajů, přičemž jim zároveň umožňuje takové zpracování odmítnout.

Proti kontrolním závěrům nepodala kontrolovaná osoba námitky.

Oddělení podpory

Kontrola dodavatele zajišťujícího dodávku elektřiny (ČEZ Prodej, a.s.)

Úřad na základě nahlášeného porušení zabezpečení osobních údajů provedl a ukončil kontrolu dodavatele elektřiny.

Předmětem kontroly bylo dodržování povinností stanovených kontrolované osobě ČEZ Prodej, a.s., obecným nařízením v souvislosti s předáním osobních údajů o odběratelích plynu (kteří zároveň nejsou odběrateli elektřiny), poskytnutých na základě § 8 odst. 10 zákona č. 348/2005 Sb., o rozhlasovém a televizním vysílání. Podle tohoto dokumentu je dodavatel zajišťující dodávku elektřiny odběratelům povinen na požádání sdělit provozovateli vysílání ze zákona, se kterými odběrateli uzavřel smlouvu o dodávce elektřiny.

Dodavatel zajišťující dodávku elektřiny odběratelům předá do 30 dnů ode dne doručení žádosti vedle adresy odběrného místa určité osobní údaje. Jedná se o jméno, popřípadě jména a příjmení, datum narození a adresu trvalého pobytu, u cizinců popřípadě dlouhodobého pobytu odběratele, jenž je fyzickou osobou, jméno, příjmení, popřípadě obchodní firmu, místo podnikání a identifikační číslo odběratele, který je fyzickou osobou – podnikatelem, obchodní firmu nebo název, právní formu, sídlo a identifikační číslo odběratele, jenž je právnickou osobou, název, sídlo a identifikační číslo odběratele, který je organizační složkou státu nebo územního samosprávného celku.

Dodavatel zajišťující dodávku elektřiny odběratelům je ze zákona oprávněn požadovat po provozovateli vysílání úhradu účelně vynaložených nákladů, které mu vznikly v přímé souvislosti se splněním jeho žádosti.

Kontrolovaná osoba zjistila incident až na základě stížnosti zákaznice, kterou kontaktoval Český rozhlas v souvislosti s placením koncesionářského poplatku. Vlastní provedenou analýzou bylo zjištěno, že zaměstnanec kontrolované osoby nesprávně pracoval s databázemi zákazníků odebírajících elektřinu i plyn.

Předáním databáze, která obsahovala osobní údaje o odběratelích plynu Českému rozhlasu a České televizi, došlo k nezákonnému způsobu zpracování osobních údajů, neboť pro předání osobních údajů o odběratelích plynu nedisponuje kontrolovaná osoba žádným právním titulem.

Kontrolovaná osoba na postup při vyřizování uvedené povinnosti neměla zpracován samostatný řídicí dokument pro jednotlivé exporty dat, práce s daty se přitom řídí obecnými postupy

stanovenými v řídicí dokumentaci pro ochranu osobních údajů a pro informační a kybernetickou bezpečnost.

Přijatá (obecná) opatření a pokyny pro zaměstnance do doby zjištění porušení vedla k porušení postupu zaměstnance při vytváření předmětné databáze a tím i k porušení ustanovení obecného nařízení.

Bezodkladně po zjištění nesprávně vygenerované databáze byl vydán pokyn nadřízeného stanovující postup zaměstnanců při vytváření uvedených databází. Kontrolovaná osoba zároveň provedla školení zaměstnanců. Dále byli bezodkladně telefonicky i písemně informováni zástupci České televize a Českého rozhlasu, kdy byli požádáni o součinnost, výmaz/anonymizaci osobních údajů, zastavení procesu upomínání a vymáhání koncesionářských poplatků ve vztahu k neoprávněně předaným osobním údajům.

Úřad zjistil, že kontrolovaná osoba výše uvedeným jednáním porušila povinnosti stanovené čl. 6 bodem 1 obecného nařízení (zákonnost zpracování) a čl. 29 obecného nařízení (zpracovávání pouze na pokyn správce).

Vzhledem k tomu, že kontrolovaná osoba závadný stav neprodleně napravila, neuložil ÚOOÚ opatření k odstranění zjištěných nedostatků a uložil pokutu ve výši 40 000 Kč.

• DOZOROVÁ ČINNOST V OBLASTI OBCHODNÍCH SDĚLENÍ

V roce 2019 obdržel Úřad celkem 2007 stížností na zasílání nevyžádaných obchodních sdělení, ať už podaných prostřednictvím formuláře, který je na jeho webových stránkách k tomuto účelu zřízen, nebo prostřednictvím elektronické podatelny.

Na tomto místě je třeba uvést, že pro podání stížnosti je velice důležité, aby byl podatelem (stěžovatelem) vyplněn zdrojový kód e-mailové zprávy (formulář pro podávání stížností na zasílání nevyžádaných obchodních sdělení obsahuje podrobné návody, kde tento zdrojový kód e-mailové zprávy najít a jak jej do formuláře vložit), a také aby byl přiložen též samotný text obdrženého e-mailu, nebo aby byl vložen printscreen obdržené nevyžádané SMS zprávy. Tyto údaje pak slouží jako důkaz.

Pokud je stížnost podávána prostřednictvím elektronické podatelny Úřadu (posta@uoou.cz), měl by stěžovatel zaslat celý e-mail (celé sdělení, které obdržel), a to ve formátu .msg nebo .eml (v těchto formátech je pak uložena celá zpráva, tedy včetně textu a též zdrojového kódu e-mailové zprávy). V samotném podání je vhodné uvést i další informace, nejčastěji půjde například o informace ve vztahu k odmítání dalšího zasílání obchodních sdělení, včetně doložení této skutečnosti, informace o vztahu k odesílateli apod.

Pakliže je stížnost podána prostřednictvím webového formuláře, může stěžovatel kdykoli zjistit stav vyřizování jeho stížnosti. Tento stav se mění pokaždé, kdy její vyřízení přejde do další fáze (např. analýza, upozornění subjektu na možné porušení, kontrola, její vyřízení.

Stížnosti, u kterých bylo zjištěno, že odesílatelem je zahraniční subjekt v rámci EU, byly předávány příslušným zahraničním dozorovým úřadům na základě přeshraniční spolupráce. K tomuto účelu byl nařízením Evropského parlamentu a Rady (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele (nařízení o spolupráci v oblasti ochrany spotřebitele)[6] vytvořen systém CPC (Consumer Protection Cooperation). V některých případech oddělení obchodních sdělení využilo možnost vznést dotaz či žádost o součinnost přes systém IMI (Internal Market Information System).

Oddělení obchodních sdělení v roce 2019 v rámci přeshraniční spolupráce žádalo příslušné dozorové úřady (v Polsku – 2 případy, ve Velké Británii – 2 případy, v Německu – 2 případy, v Irsku – 1 případ, v Litvě – 1 případ a v Maďarsku – 1 případ). Z hlediska provedení nezbytných donucovacích opatření k zamezení či zastavení šíření nevyžádaných obchodních sdělení společnostmi, které jsou usídlené v jejich státech, nelze tuto spolupráci prozatím náležitě zhodnotit. Tyto případy totiž nebyly do konce roku 2019 ještě uzavřeny nebo bylo zjištěno, že v daných zemích mají příslušní rozesílatelé své sídlo pouze evidováno, přičemž faktickou činnost zde buď neprovozují, nebo jsou nedostižitelní.

Řada stížností také směřovala k zahraničním subjektům usídleným mimo rámec EU. V některých případech se příslušného odesílatele nebo toho, v čí prospěch jsou obchodní sdělení zasílána,

[6] Dne 17. ledna 2020 nabývá účinnosti nařízení Evropského parlamentu a Rady (EU) 2017/2394 ze dne 12. prosince 2017 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování právních předpisů na ochranu zájmů spotřebitelů a o zrušení nařízení (ES) č. 2006/2004.

dohledat nepodařilo. Většinou se jednalo o případy podezřelých e-shopů, které na svých stránkách neuvádějí žádné kontaktní údaje a byly taktéž v hledáčku České obchodní inspekce nebo se jednalo právě o případy odesílatelů operujících mimo Evropskou unii.

Převážnou část své činnosti oddělení obchodních sdělení věnovalo v roce 2019 především kontrolní činnosti a ukládání sankcí. V případech malého počtu stížností byly subjekty pouze upozorňovány na možná porušení zákona při šíření obchodních sdělení. Zároveň bylo takovému subjektu náležitě vysvětleno, jak má postupovat, aby byla obchodní sdělení zasílána v souladu se zákonem. Pokud jsou však taková upozornění častější, je s příslušným subjektem zahájeno kontrolní řízení.

V roce 2019 se oddělení zabývalo celkem 18 kontrolními řízeními a s 28 subjekty vedlo správní řízení, jehož výsledkem bylo uložení sankce. Celková výše sankce, kterou oddělení za šíření nevyžádaných obchodních sdělení udělilo, byla 2 099 000 Kč. Ve 11 případech bylo vedeno rovněž správní řízení o uložení pořádkové pokuty za neposkytování součinnosti při kontrole, kde celková výše uložené sankce činila 475 000 Kč. Upozorněno na možné porušení zákona pak bylo v roce 2019 celkem 390 subjektů.

Oddělení obchodních sdělení poskytovalo též informace veřejnosti. Ty byly určeny jak případným adresátům obchodních sdělení, tak také společnostem, které si nevěděly rady, jak správně obchodní sdělení zasílat. Za tímto účelem Úřad v roce 2019 zrevidoval rubriku Často kladené otázky k zákonu č. 480/2004 Sb. a bylo vydáno několik zpráv vycházejících z dozorové praxe v oblasti šíření obchodních sdělení.

Kontrola společnosti GlobalAdvertisement s.r.o.

Kontrola byla zahájena na základě stížností na rozesílání nevyžádaných obchodních sdělení. Jejím předmětem bylo posouzení dodržování povinností vyplývajících ze zákona č. 480/2004 Sb., týkajících se rozesílání obchodních sdělení pomocí elektronických prostředků.

Stížnosti na zasílání nevyžádaných obchodních sdělení směřující k této společnosti byly podávány i v průběhu celého kontrolního řízení. Celkový počet podaných stížností byl nakonec 675.

V rámci kontrolního řízení společnost GlobalAdvertisement s.r.o. zpočátku spolupracovala a ke stížnostem se vyjadřovala alespoň v obecném rámci. Podle jejích slov předmětná obchodní sdělení odeslala, a to na e-mailové adresy jejích klientů. Sdělila, že databázi klientů získává například formou zábavné hry tzv. Kola štěstí, přičemž tito klienti jí udělili souhlas se zasíláním obchodních sdělení. Tento souhlas však kontrolovaná osoba žádným způsobem nedoložila, ani nedoložila podmínky či bližší informace ke hře „Kolo štěstí", byť k tomu byla kontrolujícími několikrát v průběhu kontroly vyzývána. Následně pak kontrolovaná osoba doplnila pouze informace týkající se tzv. affiliate programů, a to ve vztahu ke dvěma společnostem, v jejichž prospěch obchodní sdělení rozesílala.

K fungování affiliate programů je třeba uvést, že se jedná o provizní marketingový systém, který se uplatňuje u online reklamy. Tento program je postaven na provázanosti mezi webovými stránkami prodejce zboží či služeb a webovými stránkami osob, které toto zboží či služby doporučují (propagátoři). Tito propagátoři jsou placeni prodejcem, a to formou provize.

Fungování affiliate programů lze jednoduše popsat ve čtyřech krocích:

- zákazník přes stránky propagátora navštíví web prodejce nebo si přes propagátora objedná zboží či službu prodejce,
- prodejce následně kontaktuje zákazníka, ověří objednávku,

- zákazník zaplatí prodejci,
- prodejce zaplatí provizi propagátorovi (výše provize záleží na interní domluvě, může jít o pevnou částku, částku určenou procenty apod.).

Jak je z výše uvedeného patrné, affiliate programy jsou marketingové nástroje. Výhodou tohoto typu marketingu je snadná měřitelnost účinnosti reklamy, a to právě díky proklikům přes stránky propagátora. Další výhodou těchto programů je zacílení reklamy na danou cílovou skupinu zákazníků, čímž dochází k úspoře nákladů vynaložených na reklamu.

S narůstajícím počtem stížností, a tedy i dalších žádostí o doplnění vyjádření kontrolované osoby, však přestala kontrolovaná společnost s ÚOOÚ komunikovat.

Za neposkytování potřebné součinnosti byla následně Úřadem uložena sankce ve výši 300 000 Kč. Výše této sankce je především odrazem velkého počtu doručovaných stížností a dlouhým obdobím (několik měsíců), kdy součinnost kontrolovaná osoba neposkytovala, ačkoli jí všechny žádosti byly prokazatelně doručovány (přihlášením oprávněné osoby do datové schránky). Tuto situaci ztěžoval kontrolujícím i fakt, že kontrolovaná osoba zasílala obchodní sdělení týkající se nabídek zboží a služeb různých internetových obchodů. V rámci součinnosti tak Úřad vyzýval k vyjádření jednotlivé internetové obchody, v jejichž prospěch byla obchodní sdělení šířena.

ÚOOÚ se také obracel na poskytovatele hostingových služeb za účelem zjištění, komu jsou poskytovány hostingové služby vztahující se k doménám odchozích e-mailových adres, ze kterých byla obchodní sdělení šířena, a též k doménám webových stránek internetových obchodů, v jejichž prospěch byla obchodní sdělení zasílána. V neposlední řadě vycházel Úřad též ze samotných textů a především ze zdrojových kódů jednotlivých obchodních sdělení.

Úřad tak v rámci této kontroly zjistil spojitost a provázanost několika společností s tím, že se jedná o společnosti, které jsou zapojeny do některých z affiliate programů. Kontrolovaná osoba byla v šetřených případech v pozici rozesílatele obchodních sdělení. Ostatní společnosti (v jejichž prospěch byla obchodní sdělení kontrolovanou osobou zasílána) byly pak šiřiteli předmětných obchodních sdělení v postavení příkazce – zadavatele obchodních sdělení, neboť zapojením do affiliate programu šířily a iniciovaly zadání samotných rozesílek obchodních sdělení.

Jak je uvedeno výše, kontrolovaná osoba v průběhu kontroly nikterak nedoložila, resp. neprokázala souhlas (tedy právní titul) k zasílání obchodních sdělení na předmětné e-mailové adresy. Tvrzení kontrolované osoby, že e-mailové adresy pocházejí např. z tzv. „Kola štěstí", není v tomto případě možné považovat za prokazatelný souhlas k zasílání obchodních sdělení. Kontrolovaná osoba tak porušila povinnosti stanovené v § 7 odst. 2 zákona č. 480/2004 Sb., tedy povinnosti využít podrobnosti elektronického kontaktu za účelem šíření obchodních sdělení elektronickými prostředky pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.

ÚOOÚ dále dospěl k závěru, že došlo také k porušení § 7 odst. 4 písm. b) zákona č. 480/2004 Sb., neboť obchodní sdělení neobsahovala jednoznačné označení toho, jehož jménem se komunikace uskutečňuje. V této souvislosti též konstatoval, že porušení § 7 odst. 2 zákona č. 480/2004 Sb. se dopustily také společnosti, v jejichž prospěch byla obchodní sdělení šířena, a to proto, že byly šiřiteli obchodních sdělení v postavení příkazce – zadavatele.

Proti protokolu o kontrole nebyly kontrolovanou osobou námitky podány.

S ohledem na skutečnost, že společnost GlobalAdvertisement s.r.o. zanikla již 11. července 2019, nemohlo být příslušné správní řízení s ní již vedeno. Správní řízení tak bylo zahájeno jen se společnostmi, v jejichž prospěch byla předmětná obchodní sdělení šířena.

Z kontextu příslušných ustanovení zákona č. 480/2004 Sb., která se vztahují k zasílání obchodních sdělení, je třeba uvést, že veřejnoprávní odpovědnost za přestupek dle § 11 odst. 1 zákona č. 480/2004 Sb. je formulována jako objektivní odpovědnost (odpovědnost 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 (chránit soukromí v co nejširší možné míře) je třeba za šiřitele obchodních sdělení považovat také osoby, v jejichž prospěch jsou obchodní sdělení šířena.

Odpovědným subjektem za rozesílání obchodních sdělení jsou tak kromě faktického odesílatele (společnosti GlobalAdvertisement s.r.o.) také společnosti, v jejichž prospěch byla obchodní sdělení odesílána.

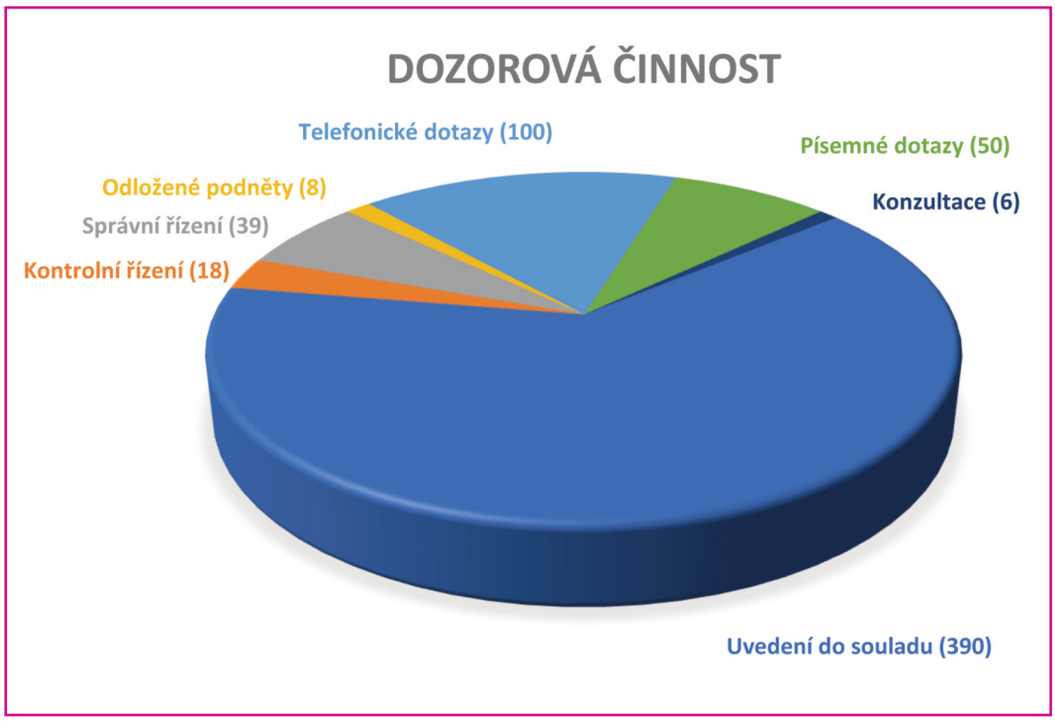
Šiřitelé obchodních sdělení, ať už jde o zadavatele (tedy toho, v čí prospěch jsou obchodní sdělení rozesílána) či faktické rozesílatele, by si měli vždy dostatečně prověřit, zda adresáti obchodních sdělení udělili souhlas pro takové zasílání, resp. v obecnosti, zda rozesílka probíhá zákonným způsobem.

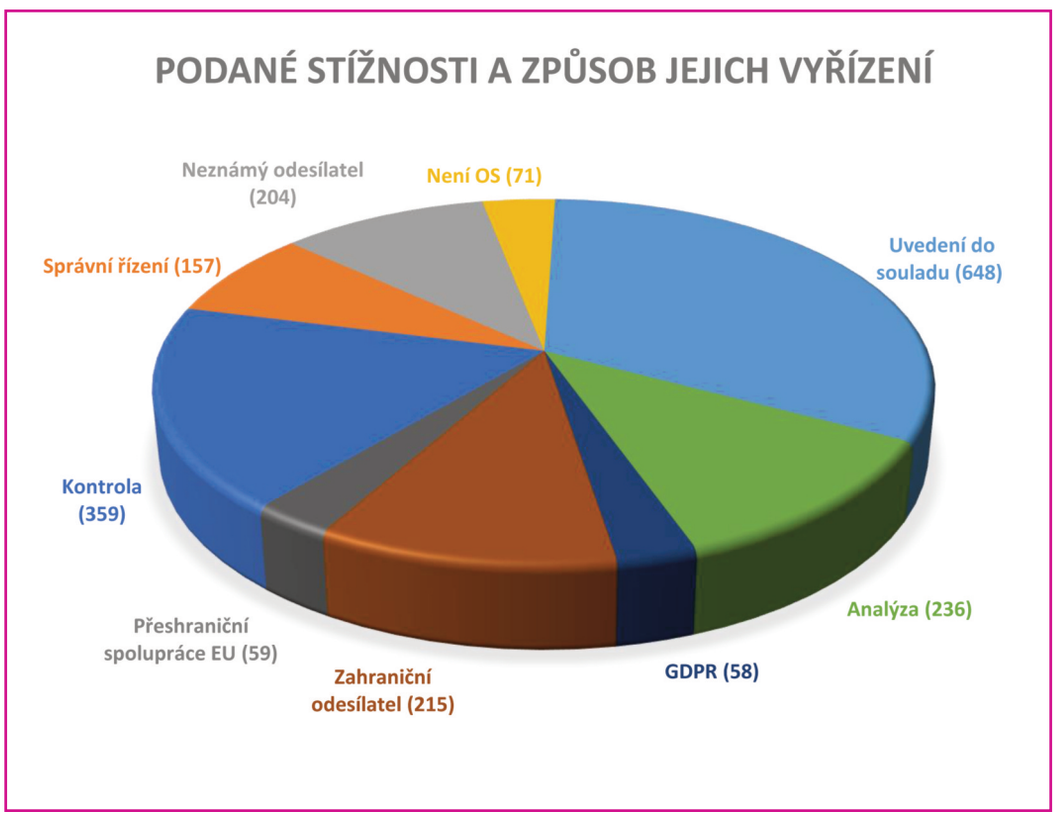
Společnosti, v jejichž prospěch byla obchodní sdělení odesílána, se tak přenesením rozesílky obchodních sdělení (či její iniciací) na společnost GlobalAdvertisement s.r.o. nezbavují své odpovědnosti. Musí být naopak i přesto schopny doložit souhlasy adresátů obchodních sdělení, nebo musí být schopny zajistit tyto souhlasy prostřednictvím rozesílací společnosti. Nelze spoléhat pouze na případné ujištění rozesílací společnosti, že patřičným souhlasem disponuje.

Z povahy souhlasu se zasíláním obchodních sdělení je patrné, že osoba udělující souhlas, musí vědět, k čemu souhlas dává (pro jaký účel, k jakému zasílání obchodních sdělení), jakému subjektu nebo ve prospěch jakého subjektu jí budou obchodní sdělení zasílána. Tento souhlas musí být také prokazatelný.

Za výše uvedené porušení byla příslušným společnostem, v jejichž prospěch byla obchodní sdělení šířena, uložena sankce ve výši 350 000 Kč, 9 000 Kč a 15 000 Kč. V uložených sankcích byl zohledněn zejména počet obdržených stížností (tedy zaslaných obchodních sdělení). Jako významná polehčující okolnost byla zohledněna především skutečnost, že tyto společnosti nebyly faktickým odesílatelem předmětných obchodních sdělení a nesprávným postupem odesílatele mohly i ony utrpět škodu na své dobré pověsti a jméně.

Na následující straně jsou graficky znázorněny dozorové činnosti v roce 2019 a stav vyřízení jednotlivých stížností v roce 2019.


DOZOROVÁ ČINNOST
Telefonické dotazy (100)
Písemné dotazy (50)
Odložené podněty (8)
Konzultace (6)
Správní řízení (39)
Kontrolní řízení (18)
Uvedení do souladu (390)


PODANÉ STÍŽNOSTI A ZPŮSOB JEJICH VYŘÍZENÍ
Neznámý odesílatel (204)
Není OS (71)
Správní řízení (157)
Uvedení do souladu (648)
Kontrola (359)
Analýza (236)
Přeshraniční spolupráce EU (59)
GDPR (58)
Zahraniční odesílatel (215)

• SPRÁVNÍ TRESTÁNÍ

Správní trestání bylo v roce 2019 výrazně ovlivněno nabytím účinnosti zákona č. 110/2019 Sb., o zpracování osobních údajů, který v některých aspektech doplňoval a dotvářel přímo účinné obecné nařízení.

Vzhledem ke skutečnosti, že v roce 2019 dobíhaly případy, které se staly ještě před účinností zákona o zpracování osobních údajů (tj. v době, kdy byl účinný zákon č. 101/2000 Sb., o ochraně osobních údajů, bylo v prvé řadě ve správním řízení nutné řešit otázku, podle jaké právní úpravy má být postupováno v případě kolize dvou právních předpisů.

Pokud bylo správní řízení zahájeno před účinností zákona o zpracování osobních údajů, bylo nutné se řídit ustanovením § 66 odst. 5 zákona č. 110/2019 Sb. a řízení zahájená za účinnosti předešlého zákona a pravomocně neskončená dokončit podle zákona č. 101/2000 Sb. Pokud se skutek stal za účinnosti zákona č. 101/2000 Sb., ale Úřad o něm rozhodoval až po nabytí účinnosti nového zákona o zpracování osobních údajů, bylo třeba zohlednit i čl. 40 odst. 6 Listiny základních práv a svobod, dle kterého se trestnost činu posuzuje a trest se ukládá podle zákona účinného v době, kdy byl čin spáchán.

Pozdějšího zákona se použije, jestliže je to pro pachatele příznivější. Typicky příznivější situace bylo porušení povinnosti stanovené v § 15 odst. 1 zákona č. 101/2000 Sb., tedy povinnosti zaměstnanců správce zachovávat mlčenlivost o osobních údajích, kdy toto jednání již podle zákona o zpracování osobních údajů nenaplňuje skutkovou podstatu přestupku.

Konkrétní ukázkou může být jednání zaměstnankyně Policie České republiky, která neoprávněně nahlížela prostřednictvím informačního systému do trestního spisu a zjištěné informace předala třetí osobě. Vzhledem k výše uvedenému musel Úřad danou věc usnesením odložit podle § 76 odst. 1 písm. a) zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, jelikož řízení vedl již za účinnosti zákona o zpracování osobních údajů, tedy pro pachatele příznivějšího zákona.

Účinnost zákona o zpracování osobních údajů také výrazně ovlivnila správní trestání orgánů veřejné moci a veřejných subjektů, vzhledem k jeho ustanovení § 62 odst. 5, které stanovuje, že Úřad upustí od uložení správního trestu také tehdy, jde-li o subjekty uvedené v čl. 83 odst. 7 obecného nařízení.

Tímto ustanovením Česká republika využila volnosti k vlastní úpravě a zakotvila možnost upuštění od uložení správního trestu v případě orgánů veřejné moci a veřejných subjektů usazených v daném státě. Toto ustanovení Úřad aplikoval v roce 2019 hned u sedmi subjektů (u dvou z nich takto rozhodl až odvolací orgán ÚOOÚ), u kterých konstatoval konkrétní porušení pravidel při zpracování osobních údajů stanovených obecným nařízením. Byly jimi např. ministerstvo vnitra, škola, město Brno nebo Česká školní inspekce.

V případě ministerstva dopravy bylo například konstatováno spáchání přestupku podle § 62 odst. 1 písm. a) zákona o zpracování osobních údajů. Ministerstvo zde nezajistilo, aby zadávací dokumentace poskytnutá několika uchazečům o veřejnou zakázku na dodávku systému elektronického mýtného neobsahovala i osobní údaje zaměstnanců společnosti podílející se na vytvoření zadání veřejné zakázky. Jednalo se o jméno, příjmení, telefon, pracovní e-mailovou adresu, pracovní pozici nebo zařazení a informace o absolvování školení, autorství či spoluautorství dokumentu nebo účast na jednání.

Ministerstvo je orgánem veřejné moci, resp. veřejným subjektem, Úřad proto musel podle § 62 odst. 5 zákona o zpracování osobních údajů upustit od uložení správního trestu.

ÚOOÚ při své rozhodovací činnosti v roce 2019 aplikoval také § 65 zákona o zpracování osobních údajů, který mu umožňuje určité typy protiprávního jednání usnesením odložit, aniž by zahajoval řízení o přestupku, přičemž musí být splněny stanovené podmínky. Jde zejména o nízkou míru porušení či ohrožení chráněného zájmu, který byl činem dotčen, nebo o skutečnost, že správce bezprostředně po shledání porušení pravidel pro zpracování osobních údajů své jednání napravil. Podobné ustanovení obsahoval již zákon č. 101/2000 Sb., a to v jeho § 40a.

Tímto způsobem Úřad postupoval ve 25 případech (z toho v šesti případech ještě podle předešlé právní úpravy obsažené v zákoně č. 101/2000 Sb.).

ÚOOÚ touto cestou často řešil např. zveřejnění dokumentů podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, bez dostatečné anonymizace. V takových případech, pokud nebyly příliš vysoké závažnosti, Úřad vyzval odpovědný subjekt podle § 54 odst. 1 písm. b) zákona o zpracování osobních údajů. Pokud došlo k okamžité nápravě, ÚOOÚ věc usnesením podle § 65 zákona o zpracování osobních údajů odložil. V opačném případě bylo s odpovědným subjektem zahájeno řízení o přestupku.

Konkrétním příkladem využití shora uvedeného ustanovení § 65 zákona o zpracování osobních údajů byla stížnost na zveřejnění žádostí na základě zákona č. 106/1999 Sb. na elektronické úřední desce obce Újezd pod Troskami, které obsahovaly osobní údaje žadatele. Z uvedeného podnětu vyplynulo podezření z porušení zásady účelového omezení stanovené v čl. 5 odst. 1 písm. b) obecného nařízení tím, že obec Újezd pod Troskami zpracovávala osobní údaje žadatele k jinému účelu, než ke kterému je původně shromáždila. Úřad zaslal obci výzvu k nápravě protiprávního stavu, které obec vyhověla. Proto ÚOOÚ, aniž zahájil řízení o přestupku, věc odložil, neboť vzhledem k chování podezřelého po spáchání činu bylo zřejmé, že požadovaného účelu spočívajícího v bezprostřední nápravě protiprávního stavu po zjištění porušení zákonem uložené povinnosti bylo dosaženo.

V roce 2019 bylo Úřadem nejčastěji konstatováno porušení ustanovení čl. 6 odst. 1 obecného nařízení, včetně ustanovení § 5 odst. 2 zákona č. 101/2000 Sb., které tomuto článku odpovídalo dříve. Tato ustanovení upravují povinnost zpracovávat osobní údaje na základě právního důvodu.

Dalším nejčastěji porušeným ustanovením byl čl. 5 odst. 1 písm. f) obecného nařízení, případně jemu odpovídající ustanovení § 13 zákona č. 101/2000 Sb. u řízení, která byla posuzována ještě dle předchozího zákona, tedy porušení zásady „integrity a důvěrnosti". To ukládá povinnost zpracovávat osobní údaje způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických a organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Též je potřeba zmínit často porušovaný výkon práv subjektů údajů, který je zakotven v čl. 12 až 23 obecného nařízení.

PŘÍKLADY ROZHODOVACÍ PRAXE ÚŘADU:

Na základě postoupeného spisového materiálu Policií České republiky rozhodl Úřad v příkazním řízení vedeném s fyzickou osobou podnikající o porušení čl. 6 odst. 1 obecného nařízení a uložení pokuty ve výši 54 000 Kč.

Účastník se protiprávního jednání dopustil tím, že jako zástupce finanční společnosti a zprostředkovatel při uzavírání smluv pro jinou finanční společnost použil za účelem vyplnění nabídek na uzavření pojistné smlouvy osobní údaje 18 osob v rozsahu jméno, příjmení, rodné číslo, místo narození, adresa trvalého bydliště, státní občanství, povolání a platební údaje. Tyto subjekty údajů o tomto způsobu využití svých osobních údajů nevěděly. Uvedené osobní údaje získal za účelem sjednání brigády a sepsání pracovní smlouvy. K zahájení prací nikdy nedošlo. Některé pojistné smlouvy se podařilo zrušit ještě před začátkem jejich plnění, ale několika subjektům údajů byla doručena výzva k uhrazení pravidelné platby pojistného.

Vzhledem k tomu, že si osoby nebyly vědomy toho, že by jednaly o uzavření pojistné smlouvy, bylo zřejmé, že účastník řízení nedisponoval žádným z právních důvodů ke zpracování osobních údajů subjektů údajů.

Úřad na základě postoupeného spisového materiálu od Policie České republiky zahájil správní řízení se společností s ručením omezeným, ve kterém byla uložena pokuta ve výši 30 000 Kč.

ÚOOÚ v řízení konstatoval, že společnost při zprostředkování úvěrů nezajistila osobní údaje přibližně 300 klientů v rozsahu jméno, příjmení, rodné číslo, číslo občanského průkazu, adresa bydliště, telefonní číslo a informace k úvěru obsažené ve smlouvách o spotřebitelském úvěru, které byly volně uloženy v papírové krabici v prostorách společných garáží bytového domu a následně byly nalezeny v kontejneru.

Zpracování osobních údajů musí být vždy v souladu se základními zásadami, které jsou zakotveny v čl. 5 obecného nařízení. Tyto zásady představují základní pravidla, od nichž se odvíjí všechny procesy zpracování, a zároveň jsou též nejdůležitějšími principy, které správci určují, jak má s osobními údaji nakládat.

Dodržení této zásady znamená v prvé řadě důsledně zvážit veškerá rizika, která jsou s jím prováděným zpracováním osobních údajů spojená, a přijmout odpovídající opatření k jejich maximálnímu vyloučení.

V daném případě společnost nedostatečně vyhodnotila rizika pro práva a svobody svých klientů, a tedy nepřijala ani odpovídající bezpečnostní opatření k jejich ochraně před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, když ponechala krabici s dokumenty pocházejícími z její činnosti a obsahující osobní údaje klientů volně uloženou v prostorách bytového domu. Muselo přitom být zřejmé, že k nim může mít přístup kdokoli z obyvatel domu, který s nimi mohl libovolně nakládat.

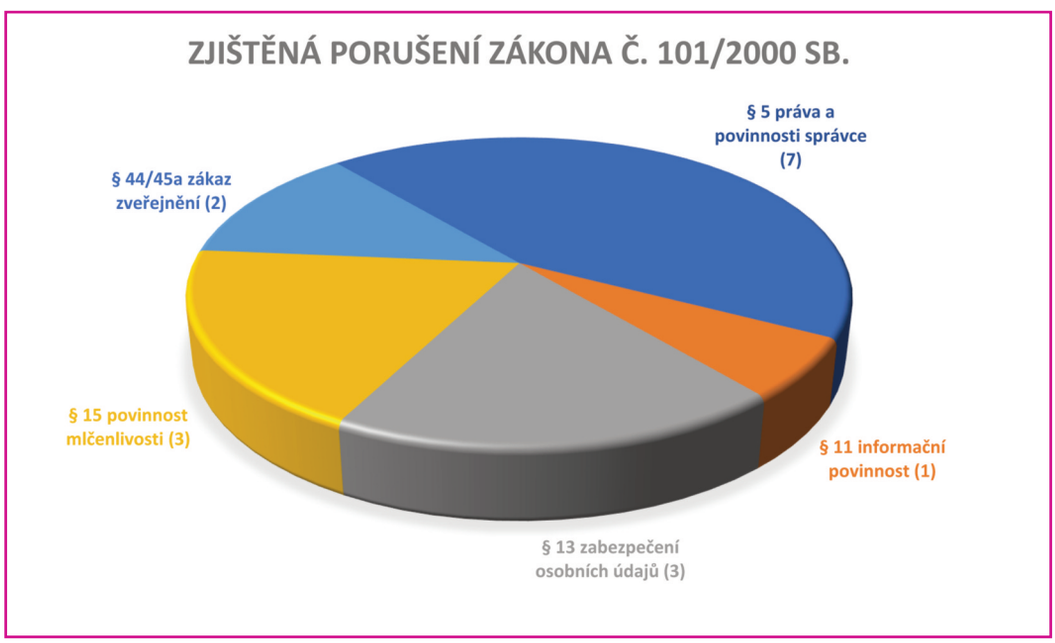
Na základě kontroly provedené v roce 2019 rozhodl Úřad v příkazním řízení o udělení pokuty ve výši 15 000 Kč internetovému obchodu za porušení čl. 15 odst. 1 GDPR, tedy práva subjektu údajů získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány. Pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k informacím stanoveným v čl. 15 odst. 1 písm. a) až g) tohoto nařízení, neboť nevyhověl žádosti svého klienta o sdělení informace, jaké osobní údaje jsou o něm zpracovávány.

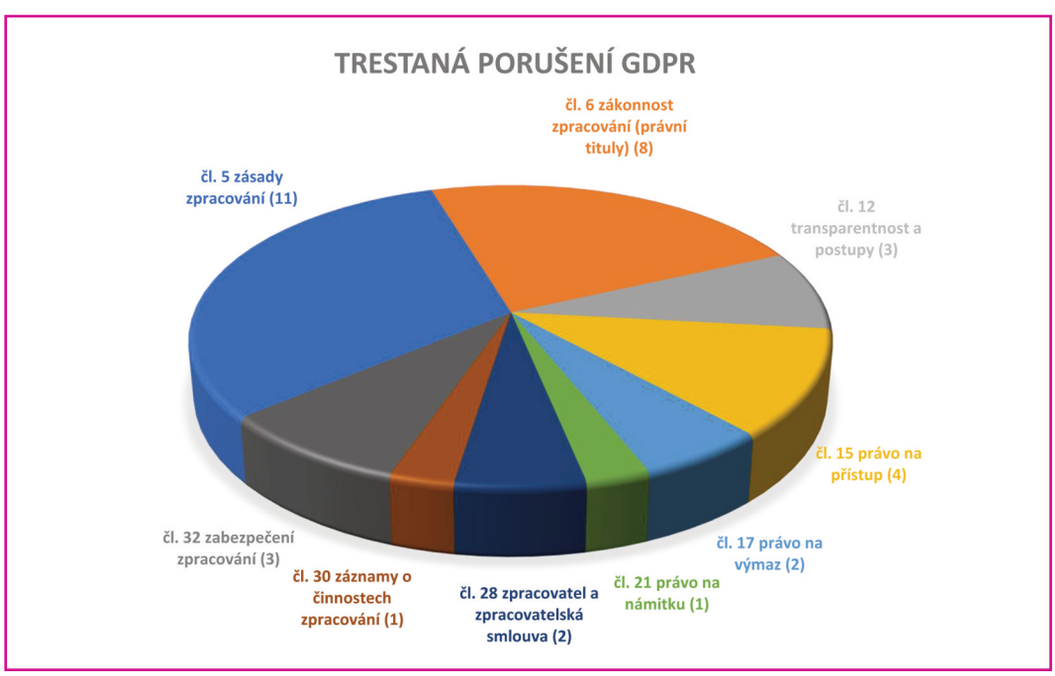
Úřad uložil v roce 2019 pokuty celkem 32 subjektům za porušení zákona č. 101/2000 Sb. a obecného nařízení, resp. zákona o zpracování osobních údajů, a to v souhrnné výši téměř jednoho milionu korun.

Možnost uložení jiného správního trestu než peněžité sankce ÚOOÚ využil v roce 2019 ve čtyřech méně závažných případech, a to ve formě udělení napomenutí.

Zákon o zpracování osobních údajů, stejně jako jeho předchůdce, opravňuje Úřad k postihování porušení zákazu zveřejnění, jakožto samostatnou skutkovou podstatu, nezávislou na porušení obecného nařízení.

Těmito oznámeními se Úřad zabýval v roce 2019 v několika desítkách případů. Řízení bylo zahájeno ve třech případech, z toho dva případy byly vedeny ještě dle předchozí právní úpravy (dle § 44a a § 45 zákona č. 101/2000 Sb.). Pokuty za porušení zákazu zveřejnění osobních údajů jiným právním předpisem byly uloženy ve dvou případech, a to právnické osobě ve výši 140 000 Kč a fyzické osobě ve výši 2 000 Kč.





• 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 zákona správního řádu.[7] 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 2019 zabýval celkem 30 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, zejména tehdy, pokud byla vznesená podezření vyhodnocena jako nedůvodná a podnět odložen bez dalších opatření. Ve čtyřech případech se stěžovatelé obrátili na Úřad se stížností proti kontrolním postupům.

Z výše uvedeného celkového počtu byly čtyři stížnosti posouzeny jako důvodné. V těchto případech byly následně zahájeny dozorové postupy, aby stížnost byla nově posouzena, a případně také následně vedeno kontrolní nebo správní řízení. Sedmi stížnostmi, které Úřad obdržel v roce 2019, se bude zabývat v roce 2020.

Ve čtyřech případech stěžovatel opětovně nesouhlasil s již provedeným posouzením stížnosti, a obrátil se proto na předsedkyni Úřadu. Ve všech těchto případech byl předchozí postup Úřadu shledán oprávněným a stížnosti byly vyhodnoceny jako bezdůvodné.

Stejně jako v přechozích letech, ani v roce 2019 nesměřoval žádný podnět, které Úřad obdržel od stěžovatelů, proti nevhodnému chování úředních osob.

• POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

1. Boj proti školní šikaně nemůže podpořit nezákonné zásahy do soukromí nezletilých dětí

Městský soud v Praze se ve svém rozsudku č. j. 14 A 89/2017-47 ze dne 11. března 2019 v řízení o žalobě proti rozhodnutí předsedkyně Úřadu ze dne 5. října 2017, č. j. UOOU-04002/17-23, podané městem Moravský Beroun zabýval narušením soukromí žáků 4. třídy, tj. nezletilých dětí, které požívají zvýšené ochrany soukromí.

V dané věci zpracovávalo zastupitelstvo města Moravský Beroun údaje žáků, kteří měli účast na šikaně (jako oběť šikany a aktéři), a to v rozsahu jméno a příjmení, informace o navštěvované škole, včetně ročníku, a veškeré informace vztahující se k průběhu šikany obsažené ve výstupu psychologické intervence (dále jen „posudek“).

ÚOOÚ v žalobou napadeném rozhodnutí uvedl, že řešení stížnosti na šikanu spadá do vyhrazené působnosti rady obce. Zastupitelstvo proto mělo být o faktu, že je řešena šikana žáka

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

příslušné školy a byly vypracovány určité postupy, informováno pouze rámcově. Informace o způsobu šikany a jména a příjmení dotčených žáků základní školy jsou údaji, jejichž šíření působí zvlášť závažný zásah do soukromého života těchto žáků, a které zastupitelstvo pro účely informování o přijatých opatřeních nepotřebuje znát.

S ohledem na princip proporcionality měla dle Úřadu ochrana osobních údajů žáků základní školy a zabránění neoprávněnému zásahu do jejich soukromí v takto citlivé záležitosti přednost před právem na informace.

Městský soud v Praze, který žalobu města Moravský Beroun zamítl, v odůvodnění svého rozsudku zejména konstatoval, že ochrana soukromí a důstojnosti je ve zvýšené míře dána právě při informování o nezletilých dětech či obdobně zranitelných osobách. Z toho vyplývá, že soudy i ostatní orgány veřejné moci (včetně Úřadu pro ochranu osobních údajů) jsou povinny právě těmto informacím věnovat zvýšenou pozornost a poskytnout jim mnohem důraznější ochranu (viz též nález Ústavního soudu ze dne 20. prosince 2016, sp. zn. Pl. ÚS 3/14).

Městský soud v Praze doplnil, že právě nezletilí (již pro svůj zatím omezený rozumový a mravní vývoj) mohou být citelněji zasaženi při prolomení jejich soukromí, resp. se mohou obtížněji vypořádat se situací, kdy jsou nad nezbytně nutnou míru zveřejněny jejich identifikační údaje. *„Uvedené platí obzvláště tehdy, pokud jsou zveřejňovány informace z velmi citlivé oblasti, jíž šikana bezesporu je. Ta je v prvé řadě velmi citlivě a negativně vnímána její obětí, ale rovněž její pachatelé mohou její příčiny i důsledky vnímat s ohledem na svůj věk omezeně, a proto je nezbytné na ně náležitě odborně působit, nikoli je cíleně ostrakizovat (obzvláště pokud se jedná o žáky prvního stupně základní školy).“*

Městský soud v Praze se rovněž zabýval pravomocemi zastupitelstva jakožto jednoho z orgánů obce, jež jsou taxativně vymezeny v § 84 zákona o obcích a pravomocemi rady města (ty jsou taxativně vyjmenovány v § 102 zákona o obcích). Z těchto ustanovení plyne, že vyjma zákonných výjimek rada nemůže své pravomoci přenášet na jiný orgán, ani zastupitelstvo si zákonné pravomoci rady nemůže atrahovat. Soud tak přisvědčil Úřadu, když uvedl, že *„[…] byla snížena intenzita nezbytnosti informovat dopodrobna zastupitele o vzniknuvších problémech, včetně poskytnutí Posudku bez jakýchkoli anonymizačních zásahů, neboť pokud zastupitelé ve věci pravomocně nerozhodovali, nebyl dán zásadní důvod, pro který by museli být dopodrobna (včetně jmen útočníků a oběti) seznámeni s nastalými problémy v 4. třídě Školy“.*

V daném případě tedy zastupitelé z výkonu své funkce o šikaně na škole, jejímž zřizovatelem je město Moravský Beroun, podrobně být informováni nemuseli, neboť z výkonu své funkce o dotčených otázkách nerozhodovali.

2. Povaze informací o zdravotním stavu musí odpovídat i úroveň jejich zabezpečení

Městský soud v Praze ve svém rozsudku č. j. 8 A 55/2014-68 zamítl žalobu Lužické nemocnice a polikliniky, a.s., se sídlem v Rumburku (dále jen „Lužická nemocnice“) proti rozhodnutí předsedy Úřadu ze dne 24. ledna 2014, č. j. UOOU-06285/13-32.

Tímto rozhodnutím zamítl předseda Úřadu rozklad Lužické nemocnice proti rozhodnutí Úřadu jako orgánu prvního stupně ze dne 27. listopadu 2013, č. j. UOOU-06285/13-27, kterým byla Lužické nemocnici uložena pokuta ve výši 120 000 Kč za spáchaný správní delikt podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. Toho se měla dopustit tím, že jako správce osobních údajů nepřijala nebo neprovedla opatření pro zajištění bezpečnosti zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace svých pacientů.

Podkladem pro správní řízení byla kontrola Úřadu, která proběhla v Lužické nemocnici v souvislosti s prošetřováním stížnosti pacientky nemocnice na ztrátu části její zdravotnické dokumentace obsahující citlivé údaje.

V rámci provedené kontroly bylo prověřováno zabezpečení osobních údajů dle požadavků § 13 zákona č. 101/2000 Sb. a bylo zjištěno porušení tohoto ustanovení jak v souvislosti s vedením zdravotnických dokumentací v listinné podobě, tak v podobě elektronické.

Zdravotnické dokumentace (jednalo se o více než tisíc dokumentací) v listinné podobě z gynekologicko-porodnického a chirurgického oddělení byly uchovávány v nezabezpečených (neuzamykatelných) skříních. Pochybení ohledně vedení zdravotnické dokumentace v elektronické podobě pak spočívalo v nepořizování elektronických záznamů, které by umožnily určit a ověřit, kdy, kým a z jakého důvodu bylo na osobní údaje ve zdravotnické dokumentaci vedené v elektronické podobě nahlíženo, a to v rozporu s povinností stanovenou v § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

Městský soud v Praze v této souvislosti konstatoval, že argumentace nejasností právní úpravy ze strany Lužické nemocnice neobstojí, a odkázal na rozsudek Nejvyššího správního soudu ze dne 10. května 2006, č. j. 3 As 21/2005-105. V něm se vyjádřil k zákonné povinnosti přijmout konkrétní opatření dle § 13 zákona č. 101/2000 Sb. takto: *„[…] opatřeními, která je správce povinen učinit, se rozumí opatření technická, organizační, právní a jiná. […] [U]žitá dikce klade na správce a zpracovatele v jistém smyslu vyšší nároky, když způsob a prostředky zabezpečení osobních údajů ponechává na jednu stranu jejich vlastní úvaze, na druhou stranu za nesplnění předmětné povinnosti hrozí poměrně vysokými sankcemi. Nelze však akceptovat směr, kterým se ubírá argumentace stěžovatelky, neboť tento by v konečném důsledku vedl k nepoužitelnosti ust. § 13 zákona jako celku."*

Městský soud v Praze dále uvedl, že zdravotní stav je řazen mezi citlivé údaje dle § 4 písm. b) zákona č. 101/2000 Sb., a tomu musí odpovídat i úroveň jejich zabezpečení. Přiměřená úroveň bezpečnosti odpovídající rizikům vyplývajícím z povahy údajů byla vyžadována i dle čl. 17 odst. 1 směrnice ES/95/46.

K povinnosti pořizování elektronických záznamů o nahlížení do systému (tzv. logování) se Městský soud v Praze vyjádřil tak, že pouhé smluvní zabezpečení aktualizací nemocničního informačního systému a prohlášení poskytovatele, že systém splňuje veškeré zákonné požadavky, nemůže zprostit žalobce odpovědnosti za správní delikt, přičemž poukázal, že k tomuto závěru dospěl Nejvyšší správní soud v rozsudku ze dne 26. prosince 2016, č. j. 3 As 121/2014-35. V něm mimo jiné uvádí, že povinnost ochrany osobních údajů je *„povinnost veřejnoprávní, které se správce či zpracovatel osobních údajů nemůže zprostit soukromoprávní dispozicí (uzavřením smlouvy s jinou osobou)".*

Mezi účastníky soudního řízení nebylo sporu, že nahlížení do zdravotnické dokumentace vedené v elektronické formě nebylo sledováno, přičemž žalobce neměl tuto službu (tzv. logování) ani předplacenu. K tomu soud vyložil, že ustanovení § 13 odst. 4 písm. c) zákona č. 101/2000 Sb. míří na ochranu osobních údajů v elektronické podobě, kdy je vyžadováno, aby bylo možno určit a ověřit, kdo údaje, které jsou předmětem ochrany, jakýmkoli způsobem zpracovával. Doplnil, že dle článku 17 směrnice ES/95/46 *„[…] správce je povinen chránit osobní údaje i před náhodným nebo neoprávněným přístupem. Taková ochrana je zajištěna, jen pokud lze zjistit, kdo, která konkrétní osoba do zdravotnické dokumentace nahlížela. Bez zajištění logování i pouhého nahlížení do zdravotnické dokumentace nelze tomuto požadavku dostát."*

3. Výrok rozhodnutí týkajícího se porušení povinností při zpracování osobních údajů je určitý i tehdy, pokud je počet subjektů určen obecnějším vymezením

Nejvyšší správní soud svým rozhodnutím č. j. 9 As 380/2017-46 ze dne 31. ledna 2019 zamítl jako nedůvodnou kasační stížnost Stavebního bytového družstva Praha (dále jen „SBD Praha"), proti rozsudku Městského soudu v Praze ze dne 12. října 2017, č. j. 11 A 83/2017-32, kterým tento soud zamítl žalobu SBD Praha proti rozhodnutí předsedkyně Úřadu ze dne 16. února 2017, č. j. UOOU-10704/16-15.

SBD Praha se žalobou podanou u Městského soudu v Praze domáhalo zrušení výše uvedeného rozhodnutí. Tímto předsedkyně Úřadu zamítla jeho rozklad proti prvostupňovému rozhodnutí Úřadu ze dne 29. listopadu 2016, č. j. UOOU-10704/16-8, kterým mu byla uložena pokuta ve výši 250 000 Kč za spáchání čtyř správních deliktů podle § 45 odst. 1 písm. c), d), f) a h) zákona č. 101/2000 Sb. Těchto deliktů se SBD Praha dopustilo v souvislosti se zpracováváním osobních údajů vlastníků, nájemců, podnájemců, manželů a manželek nájemců a dalších členů domácností bytových a nebytových jednotek, které byly v jeho vlastnictví nebo správě.

Především považoval Nejvyšší správní soud za správné vyjádření Úřadu, kterým upozornil na mimořádně vysoký počet subjektů údajů a jeho dynamickou, neustále se měnící povahu. Podle soudu *„[j]e zřejmé, že by bylo neúměrným zatížením žalovaného, pokud by musel pro účely vymezení skutku přesně na jednotky vyčíslovat počet dotčených subjektů údajů. To by samozřejmě bylo na místě v situacích, kdy se delikt týká jediného či několika jednotlivých subjektů údajů, nebo když bude možné přesnější počet zjistit bez vynaložení nepřiměřeného úsilí (např. pokud jsou osobní údaje zpracovány automatizovaně, a proto jsou přesně kvantifikovány). Obecně však lze očekávat, že právě ve sféře dohledu nad dodržováním předpisů v oblasti ochrany osobních údajů, které jsou zpravidla zpracovávány hromadně, bude často docházet k situacím, kdy dotčené osobní údaje, subjekty údajů a další okolnosti, budou vymezeny jen druhově s uvedením rozumného odhadu jejich počtu (a samozřejmě též jejich druhu)."* SBD Praha totiž spatřovalo vadu výroku rozhodnutí ÚOOÚ v tom, že nebyl konkretizován každý jednotlivý subjekt údajů. Jednalo se přitom o tisíce subjektů údajů, jejichž přesný počet se neustále měnil, takže by takováto konkretizace nebyla ani fakticky proveditelná.

Nejvyšší správní soud v této souvislosti přisvědčil odůvodnění napadeného rozsudku Městského soudu v Praze. V něm se mimo jiné uvádí, že *„[…] ve vztahu k úvaze o závažnosti protiprávního jednání žalobce soud nepovažuje za nezbytné, aby počet subjektů osobních údajů dotčených jednáním žalobce byl zcela přesně „'do jednoho' vyčíslen, řádové určení, že se jednalo o tisíce subjektů – vzhledem k počtu žalobcem spravovaných nebo vlastněných jednotek, jež jsou ve výroku rozhodnutí vyčísleny – je pro úvahu o závažnosti a rozsahu protiprávního jednání dle názoru soudu zcela dostačující"*.

Rozhodné naopak je, že Úřad ve svém rozhodnutí *„[…] skutek vymezil věcně a časově, uvedl jeho právní kvalifikaci a v maximální možné míře při zachování hospodárnosti řízení uvedl okruh subjektů údajů, jichž se delikt týká, a orientační počet těchto dotčených subjektů"*.

Nejvyšší správní soud se zabýval i otázkou možné aplikace nové právní úpravy obsažené v GDPR na odpovědnost SBD Praha, ze které pro sebe vyvozovalo beztrestnost.

Nejvyšší správní soud v této otázce přisvědčil Úřadu, jejž odkázal na usnesení rozšířeného senátu č. j. 5 As 104/2013-46, podle něhož lze použít nové – pro pachatele příznivější – úpravy pouze ve správním řízení, případně v řízení před krajským soudem.

Poradenská a konzultační činnost

I v druhém roce působnosti obecného nařízení se konzultační agenda zaměřovala jak na vysvětlování nových institutů, které toto přímo použitelné nařízení přineslo, tak na základní principy ochrany osobních údajů platné po desítky let, jejichž znalost a povědomí o nich je však třeba stále prohlubovat. Zejména se to týká správců, kteří nedisponují odborným právním aparátem či přímo pověřencem pro ochranu osobních údajů.

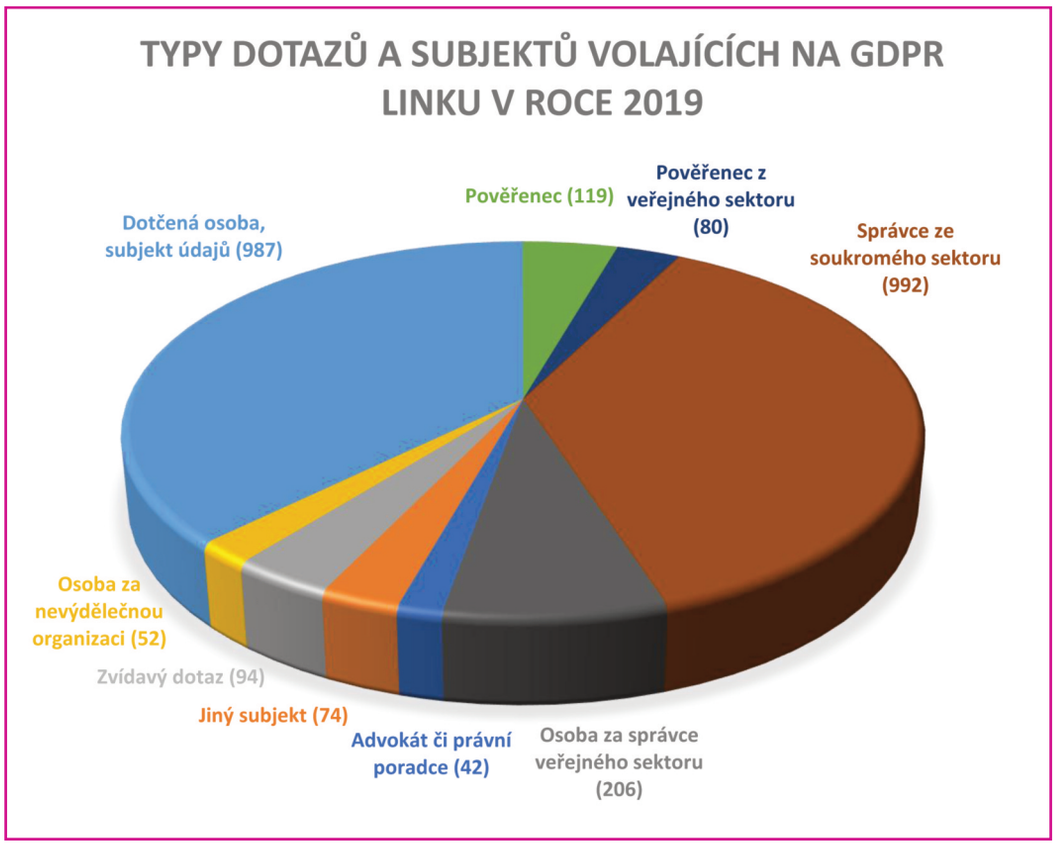
Od 24. dubna 2019 byly navíc odpovědi na dotazy a konzultace poskytovány již v návaznosti i na zákony vydané k GDPR a směrnici 2016/680, které v tomto roce nabyly účinnosti – zákon č. 110/2019 Sb., o zpracování osobních údajů, a zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Odpovědi na četné dotazy, jejichž počet však již nebyl tak enormní jako v roce nabytí účinnosti obecného nařízení, byly poskytovány jak formou písemného, tak telefonického kontaktu s tazatelem, případně osobním pohovorem při návštěvě tazatele v budově ÚOOÚ.

Pokud jde o písemnou formu, byly u většiny otázek preferovány stručné výstižné odpovědi elektronickou poštou, tedy v souladu s posláním Úřadu podporovat porozumění veřejnosti otázkám ochrany osobních údajů. Obsáhlejší právní rozbory byly poskytovány u žádostí týkajících se složitějších aspektů zpracování osobních údajů.

I v roce 2019 byla ze strany jak laické, tak odborné veřejnosti hojně využívána telefonní informační linka k GDPR, jejímž prostřednictvím bylo odpovězeno přes 2 600 dotazů. Velkou část volajících tvořily dotčené fyzické osoby, kterým pracovníci informační linky poskytovali informace, jakým způsobem mohou využít práva dle obecného nařízení. Velmi početně byly mezi volajícími dále zastoupeny osoby odpovědné za zpracování u správce, a to jak v soukromém, tak i veřejném sektoru. Pracovníky informační linky byly zodpovězeny též desítky dotazů ze strany pověřenců pro ochranu osobních údajů.

Telefonní linku často využívaly subjekty údajů, které zajímalo, zda nebyla porušena jejich práva v oblasti ochrany osobních údajů, ale také zaměstnanci správců nebo zpracovatelů, dotazující se na způsob plnění některé z povinností podle GDPR.



Setkat se bylo možné i s dalšími typy dotazů, například advokátů či advokátních koncipientů, mířících k meritu jimi řešené věci v oblasti zpracování osobních údajů.

Předností telefonického odpovídání dotazů je nejen jeho rychlost, ale i možnost bezprostřední reakce na doplňující dotaz tazatele, který jinak musí být při písemné komunikaci zodpovídán napodruhé. Tazatel však musí vzít na vědomí, že tento typ rychlého poradenství může poskytnout toliko obecné teze k řešenému problému či východiska pro uplatnění práv subjektu údajů v dané věci.

Vzhledem k velkému zájmu veřejnosti o problematiku zpracování osobních údajů prostřednictvím kamerových systémů byla v provozu i telefonní linka určená k zodpovídání otázek přímo z této oblasti.

Mnoho odpovědí na otázky mohla veřejnost seznat v rubrice *Často kladené otázky podle oblastí zpracování údajů* na webových stránkách Úřadu, které byly s ohledem na vývoj v problematice ochrany osobních údajů průběžně doplňovány a aktualizovány, případně jimi byla nahrazována starší stanoviska Úřadu. I tato rubrika sloužila k rychlému a efektivnímu poskytnutí odpovědi v případě některých písemných dotazů.

V uplynulém roce ÚOOÚ poskytl více než dvě desítky komplexnějších osobních konzultací na základě žádosti správců nebo zpracovatelů jak z veřejného, tak soukromoprávního sektoru. Z ústředních orgánů státní správy využili tuto možnost například zástupci ministerstva vnitra, ministerstva financí, ministerstva spravedlnosti, ministerstva průmyslu a obchodu a také Celní správy a Policie ČR.

V konzultacích poskytovaných soukromoprávním subjektům se opakovaně vyskytla problematika zpracování biometrických údajů jako zvláštní kategorie osobních údajů podle článku 9

GDPR, jehož znění přineslo zpřísnění podmínek pro zpracování těchto údajů umožňujících nebo potvrzujících jedinečnou identifikaci fyzické osoby oproti předchozí právní úpravě obsažené v již zrušeném zákoně č. 101/2000 Sb., o ochraně osobních údajů. Časté byly otázky na využívání dynamického biometrického podpisu pro potvrzení identifikace fyzické osoby uzavírající smluvní vztah.

Úřad též konzultoval využívání technologie rozpoznávání obličejů pro identifikaci pachatelů diváckého násilí na fotbalových stadionech za účelem zamezení dalších vstupů na stadion. Řešení dlouhodobého celoevropského problému diváckého násilí biometrickou identifikací návštěvníků fotbalového utkání bylo v některých zemích (např. v Dánsku) přijato na základě zákona zmocňujícího dozorový úřad povolit takové zpracování z důvodu významného veřejného zájmu fotbalovému klubu jako soukromoprávnímu subjektu, jestliže poskytne vhodné a konkrétní záruky ochrany osobních údajů požadované ustanovením článku 9 odst. 2 písm. g) obecného nařízení. Takové zmocnění pro ÚOOÚ ale český zákon o zpracování osobních údajů neobsahuje a požadované záruky neobsahuje ani dosavadní úprava v zákoně č. 115/2001 Sb., o podpoře sportu.

Bylo proto doporučeno vyčkat novely zákona o podpoře sportu připravované ministerstvem vnitra, jejíž příprava má zahrnovat i posouzení vlivu na ochranu osobních údajů podle článku 35 odst. 2 písm. b) GDPR. Jeho cílem musí být vypořádání se s důležitými otázkami ochrany soukromí, osobních údajů a riziky, které při využívání technologie rozpoznávání obličejů vyvstávají.

Druhým tématem, který se v konzultacích vyskytl opakovaně, je vztah mezi subjekty podílejícími se na určitém zpracování osobních údajů. Určení, zda jde o:

- vztah dvou samostatných správců, z nichž každý stanoví účel a prostředky zpracování,
- vztah správce a zpracovatele, který zpracovává osobní údaje pro správce či,
- vztah společných správců, kteří účel a prostředky zpracování stanoví společně,

v řadě případů závisí na tom, jak konkrétně jsou tyto vztahy upraveny např. ve smlouvě mezi těmito subjekty uzavírané.

Obecně však lze konstatovat, že jestliže správci, např. zdravotnickému zařízení nebo bance, stanoví účel zpracování zákon, nemusí být ani při zpracování pro jiný ze zákona vyplývající účel pro jiný subjekt v postavení zpracovatele, ale mohou být stále v postavení správce, případně společného správce. Smlouva mezi těmito subjekty v takovém případě nemusí obsahovat všechny náležitosti smlouvy se zpracovatelem podle článku 28 GDPR.

Úřad dále konzultoval široké spektrum dotazů ze školství, obecní samosprávy, soukromoprávních vztahů a dalších oblastí, kterými se zpracování osobních údajů prolíná.

Ani v roce 2019 ÚOOÚ neobdržel žádnou žádost, která by obsahově a kvalitativně představovala žádost o předchozí konzultaci podle článku 36 obecného nařízení. O tu by měl požádat správce osobních údajů, pokud dospěl k závěru, že z jím provedeného posouzení vlivu na ochranu osobních údajů podle článku 35 obecného nařízení vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, i přesto, že přijal opatření ke zmírnění tohoto rizika. Jak ovšem z tohoto ustanovení vyplývá, jde až o krajní případ vysoce rizikového zpracování, jehož výskyt je předpokládán zejména u zpracování prováděného zpravidla za použití nových, zatím neosvědčených technologií.

Úřad v průběhu roku 2019 uspořádal čtyři semináře pro pověřence pro ochranu osobních údajů navazující na semináře z předchozího roku, přičemž červnový seminář byl věnován i shora zmíněné nové národní legislativě pro ochranu osobních údajů a správnímu trestání. Informace o působení pověřenců u jednotlivých správců získal ÚOOÚ také dotazníkovým průzkumem.

Kapacita jednacího sálu Úřadu byla vždy plně využita, stejně jako při prosincovém Dnu menších správců navštíveném zástupci i majiteli malých a středně velkých firem, kteří povinnost jmenovat pověřence nemají.

Ve spolupráci s krajskými pověřenci byly v Pardubicích a Karlových Varech uspořádány další dva semináře pro pověřence v Pardubickém a Karlovarském kraji.

Pracovníci oddělení konzultací se také autorsky podíleli na příspěvcích do příručky k ochraně osobních údajů pro starosty vydávané Svazem měst a obcí. Jejím obsahem jsou krátká, praktická a srozumitelná doporučení, jak postupovat při nakládání s osobními údaji v různých činnostech obce, např. při blahopřání jubilantům a vítání občánků, zápisu údajů do obecní kroniky nebo při zpracování osobních údajů žadatelů o přidělení obecního bytu.

• LEGISLATIVA

Dne 24. dubna 2019 nabyl platnosti a účinnosti zákon č. 110/2019 Sb., o zpracování osobních údajů a doprovodný zákon č. 111/2019 Sb. Do českého právního řádu implementovaly nový unijní regulační rámec ochrany osobních údajů. Jedná se o:

1. GDPR,
2. směrnici 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,
3. směrnici 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.

Ani jeden uvedený zákon nepřinesl příliš zásadních změn oproti obecnému nařízení. Podstatnou byl rozpad dosavadní jednotné regulace ochrany osobních údajů do těchto segmentů:

1. základní, který se řídí GDPR, ať už přímo nebo na základě § 4 odst. 2 a výjimkami v §§ 5 až 15 zákona o zpracování osobních údajů
2. veřejný pořádek (§§ 24–42 zákona o zpracování osobních údajů)
3. národní bezpečnost (§§ 43–49 zákona o zpracování osobních údajů)

Zpracování osobních údajů v oblasti veřejného pořádku i národní bezpečnosti se řídí výlučně zákonem o zpracování osobních údajů, přičemž v obou těchto segmentech se na základě rozhodnutí národního zákonodárce obecné nařízení nepoužije ani podpůrně.

Druhou zásadní změnou je nesystémové vynětí celého veřejného sektoru z trestněprávní působnosti Úřadu. Ten v praxi zjistil, že ve veřejném sektoru chybí pověřenci pro ochranu osobních údajů. Tam, kde jsou jmenováni, mnohdy nejsou s nimi záležitosti ochrany osobních údajů projednány. Tento fakt vede k tomu, že koncepční pomůcky nejvyšších správních úřadů pro regulované subjekty nedávají vždy odpovědi na otázky praxe, nebo je dávají chybně. Tyto pomůcky jsou také málokdy plně aktuální, ačkoliv unijní vývoj práva ochrany osobních údajů je překotný, srov. nová stanoviska Sboru.[8]

[8] https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_cs

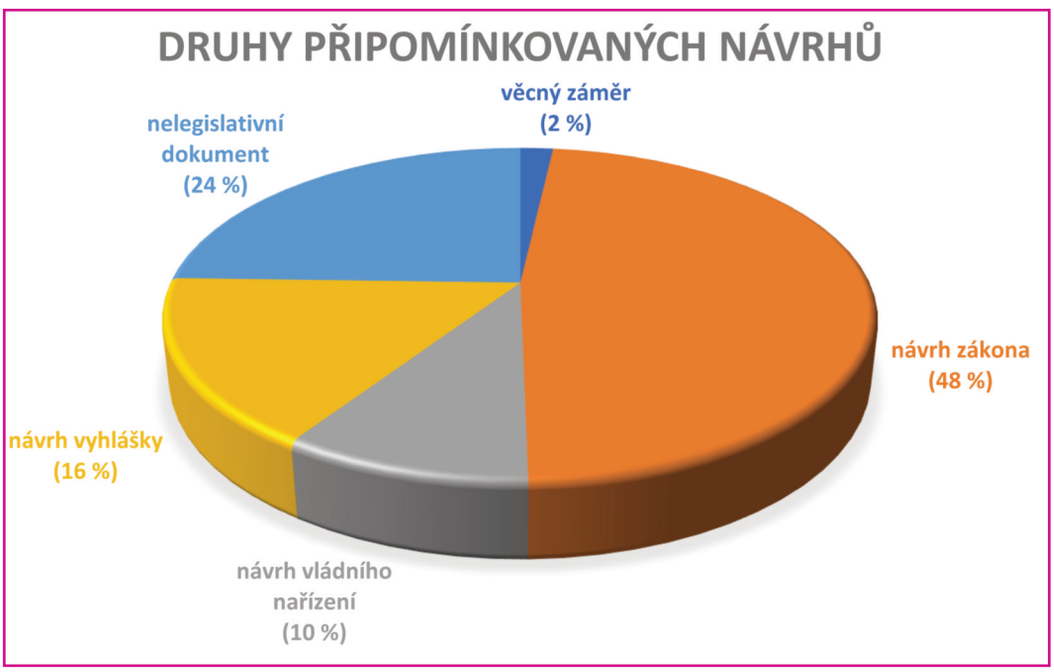
Třetí odlišnou právní úpravou oproti stávající je nová regulace zpracování osobních údajů za účelem vědeckého nebo historického výzkumu, pro statistické účely, novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu v §§ 16 až 23 zákona o zpracování osobních údajů. ÚOOÚ považuje za nezbytné, aby regulátoři připravili koncepční pomůcky, jak tuto novou právní úpravu používat v praxi.

Úřad v zákoně o zpracování osobních údajů prosadil v § 1 deklaraci, že ochrana osobních údajů je součástí širší ochrany soukromí a aby v § 7 byla stanovena věková hranice 15 let pro způsobilost dítěte k udělení souhlasu se zpracováním osobních údajů.

Neprosadil, aby GDPR bylo podpůrně použitelné pro veškerá zpracování osobních údajů a ponechání předchozí regulace trestání veřejného sektoru. Rovněž se nepodařilo napřímit vztah Úřadu a justice, aby špatná soudní rozhodnutí o osobních údajích nemusel napravit až Ústavní soud jako u platů státních úředníků ve věci Právo ve veřejném zájmu v. Zlín ze 17. října 2017, sp. zn. IV. ÚS 1378/16.

ÚOOÚ akceptoval dlouhodobé snahy části odborné veřejnosti svěřit mu působnost ve svobodném přístupu k informacím. Výsledná substandardní podoba, kde Parlament schválil zákon o zpracování osobních údajů v senátním znění (doprovodný zákon byl přitom schválen ve sněmovním znění), mu však vinou absence přechodných ustanovení způsobí krajní obtíže.

Úřad se tuto situaci pokusil napravit tak, že přesvědčil Poslaneckou sněmovnu o pozměňovacím návrhu; tato snaha však narazila na společný postoj ministerstva vnitra a Senátu. Hrozí tedy zahlcení ÚOOÚ řízeními, které může vést k překročení zákonných lhůt pro rozhodnutí.

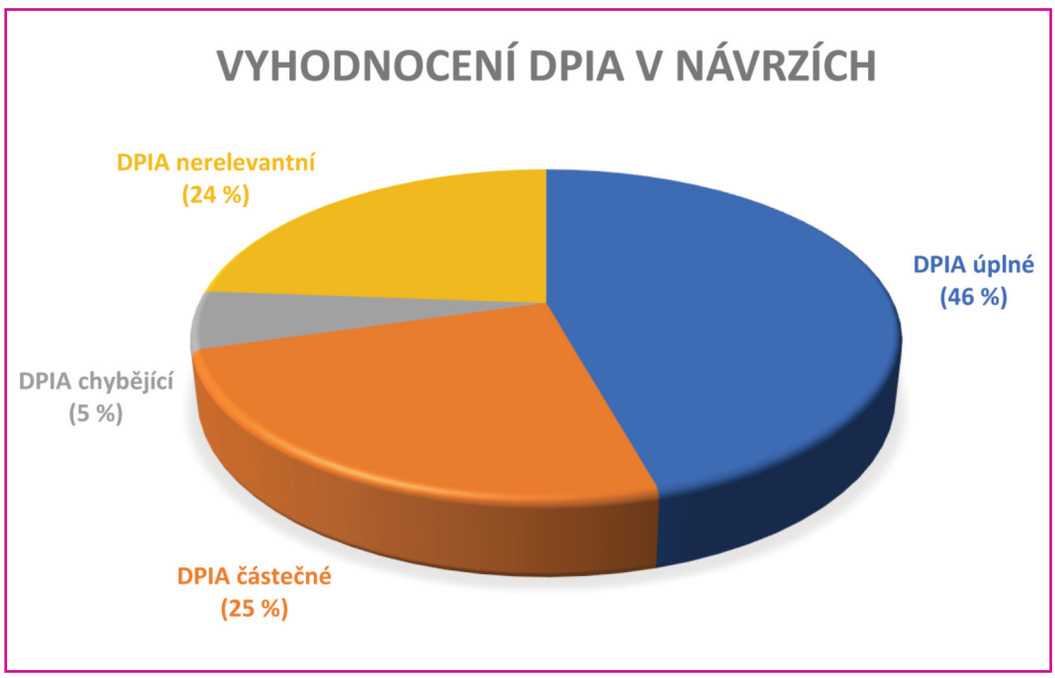


Vyhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Úřad nadále pokračoval ve své snaze zlepšit kvalitu legislativního vyhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů (DPIA), aby dostálo požadavkům článku 35 obecného nařízení. Nově se tato snaha opírá i o § 10 zákona o zpracování osobních údajů, podle kterého správce nemusí provádět posouzení vlivu zpracování na ochranu

osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést.

Je proto nezbytné, aby součástí legislativního DPIA byla rovněž vyhodnocení riskantních záležitostí spojených se zpracováním osobních údajů společně s vyhodnocením mechanismů použitých k jejich umenšení či úplné eliminaci.



Spolupráce s Poslaneckou sněmovnou a Senátem

Některé poslanecké kluby na základě § 54 odst. 3 zákona o zpracování osobních údajů neformálně projednaly s ÚOOÚ připravované pozměňovací návrhy, což je pro ochranu soukromí v ČR velice záslužné. Úřad například sdělil, že přirovnání centrální evidence exekucí k insolvenčnímu rejstříku je nevhodné kvůli odlišnému účelu zpracování osobních údajů. Podobu insolvenčního rejstříku, založeného na bezbřehém zpřístupňování informací bez struktury a klasifikace životních rolí a k tomu potřebných údajů, považuje ÚOOÚ za nevyhovující, na což bylo již v roce 2012 ministerstvo spravedlnosti upozorněno.

Soukromé právo

Ministerstvo spravedlnosti připravilo návrh novely nového občanského zákoníku k transpozici směrnice o smlouvách o poskytování digitálního obsahu a digitálních služeb. Její součástí je i sporný článek 3 odst. 1 alinea 2 o monetizaci osobních údajů.

Úřad s předkladatelem i nadále jedná o tom, jak toto ustanovení unijního práva do českého právního řádu nejlépe transponovat, tak aby byla maximálně zaručena ochrana osobních údajů jako lidského práva podle Charty základních práv EU.

Ministerstvo práce a sociálních věcí předložilo návrh novely nového zákoníku práce, ve kterém však opomnělo regulovat biometriku. Zaměstnavatelé přitom často zakládají zpracování některých biometrických údajů zaměstnanců pro účely kontroly vstupu, přítomnosti a přístupů na souhlasu zaměstnanců. Takové používání souhlasu ve vztahu zaměstnavatel – zaměstnanec je však nepřijatelné, a to s ohledem na právní úpravu obecného nařízení. MPSV připomínku

ÚOOÚ neakceptovalo s ohledem na úzké zaměření novely. Dohodlo však s Úřadem, že bude na regulaci biometriky pracovat.

Ministerstvo zdravotnictví připravilo návrh zákona o elektronickém zdravotnictví a bezpečném sdílení dat mezi poskytovateli zdravotních služeb (zákon o elektronickém zdravotnictví; angl. eHealth), což je největší změna zdravotnictví v posledních letech. O její podobě bude ÚOOÚ s předkladatelem i nadále jednat.

Veřejné právo

Zásadní dopad na soukromí bude mít sčítání lidu, domů a bytů v roce 2021. Úřad při projednávání návrhu paragrafovaného znění navázal na spolupráci s Českým statistickým úřadem při přípravě návrhu věcného záměru zákona. Podařilo se provázat zmocnění k přebírání údajů s účelem jejich zpracování. ÚOOÚ má za to, že toto sčítání lidu vytvoří předpoklady k plně administrativnímu sčítání v roce 2031, tj. bez jakéhokoliv vyplňování dotazníků.

Ministerstvo obrany předložilo vládě návrh novely zákona o Vojenském zpravodajství. K posílení ochrany soukromí Úřad prosadil, aby bylo navrženo zřízení inspektora pro kybernetickou obranu podléhajícího přímo ministrovi po vzoru pověřence pro ochranu osobních údajů. Další zárukou by mělo být rozhodnutí o povinnosti zřídit a zabezpečit rozhraní pro připojení nástrojů detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování těchto nástrojů.

S ministerstvem spravedlnosti navíc dohodl změnu návrhu právní úpravy zveřejňování koncových vlastníků podílů v obchodních společnostech tak, aby bylo lépe ochráněno jejich soukromí.

Soukromí v elektronických komunikacích

Návrh nařízení o respektování soukromého života a ochrany osobních údajů v elektronických komunikacích ani po mnoha měsících projednávání za finského předsednictví nepostoupil do stadia obecného přístupu Rady EU. Úřad upozornil zejména na neprovázanost zmocnění pro národní regulaci s unijní a na problematičnost prolomení důvěrnosti komunikací kvůli boji s dětskou pornografií a terorismem.

• ANALYTICKÁ ČINNOST

Analytické oddělení se i v roce 2019 podílelo na úkolech a činnostech Úřadu, které vyžadovaly podrobnější analýzu a hledání systémových řešení souladných s východisky, principy a požadavky obecného nařízení.

Současná činnost ÚOOÚ se odehrává na pozadí velmi dynamického vývoje evropské ochrany osobních údajů, který je v případě potřeby sjednocován v rámci Evropského sboru pro ochranu osobních údajů (dále Sbor),[9] a navenek může být veřejností sledován v podobě přijatých pokynů, stanovisek či doporučení k dílčím otázkám či problémům.[10]

Právě materiály Sboru odráží vícevrstevnatost problematiky a významně přispívají k prohlubování know-how v oblasti ochrany osobních údajů. Jeho výstupy jsou přitom orientovány prakticky a jsou určeny především povinným subjektům, zejména správcům/zpracovatelům. Analytické oddělení se také podílí na přípravě uvedených materiálů pro Sbor.

Je skutečností, že ačkoli v současné době již v ČR existuje úplný rámec ochrany osobních údajů, a to poté, co byl přijat zákon o zpracování osobních údajů, neznamená to, že jsou zcela uspokojivě vyřešeny všechny otázky ochrany osobních údajů v jednotlivých oblastech či činnostech, kde dochází k jejich zpracování.

Z pohledu obecného nařízení lze spíše říct, že dochází k postupné kultivaci v jednotlivých oblastech, a to v nestejné míře. ÚOOÚ si je této skutečnosti vědom a přizpůsobuje své aktivity reálně existující situaci s cílem přispívat k postupnému zlepšování stavu ochrany osobních údajů v České republice.

Návaznost Úřadu na evropský vývoj ochrany osobních údajů je v tomto ohledu zcela zřejmá. Jako nezávislý dozorový orgán není přitom pouze tím, kdo kontroluje, ale také tím, kdo radí a pomáhá nastavovat prostředí v souladu s požadavky ochrany osobních údajů.

1. BIOMETRIKA

Jednou z oblastí, které ÚOOÚ v roce 2019 věnoval systematickou pozornost z pohledu budoucího nastavení řešení souladných s požadavky obecného nařízení, byla oblast biometriky. V posledních letech totiž docházelo k nárůstu používání biometrických zařízení soukromými subjekty, nezřídka aniž správce dostatečně zvažoval požadavky ochrany osobních údajů či tyto požadavky řešil pouze formálně. Jedná se např. o používání biometrického dynamického podpisu v bankách a pojišťovnách, při doručování zboží či uzavírání zakázek velkými prodejci.

Je však třeba zdůraznit, že správce, který se rozhodne používat zařízení využívající biometrické osobní údaje, by si měl ještě před pořízením takového zařízení položit některé otázky. Mělo by jej především zajímat, co vůbec jsou biometrické osobní údaje, jaká jsou jejich rizika, zda je možné a vhodné jejich použití v zamýšlené konkrétní situaci, jaký právní důvod zpracování přichází v úvahu či jaká technická a organizační opatření musí zavést. Musí rovněž poskytnout poučení osobám, jejichž osobní údaje budou zpracovávány, optimálně v rámci aktivní

[9] Dle čl. 68 obecného nařízení je Evropský sbor pro ochranu osobních údajů subjekt Evropské unie s právní subjektivitou. Sbor tvoří vedoucí jednoho dozorového úřadu z každého členského státu a evropský inspektor ochrany údajů nebo jejich zástupci. Sbor zastupuje jeho předseda.

[10] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_cs

informační povinnosti, případně v souvislosti s dalšími právy subjektů údajů podle kapitoly III. obecného nařízení.

Níže uvádíme některé příklady otázek z oblasti biometriky, o něž by se měli zajímat správci/zpracovatelé i subjekty údajů:

Co jsou biometrické osobní údaje, jak a kde jsou definovány?

Biometrické údaje mohou být definovány jako informace o biologických vlastnostech, fyziologických charakteristikách, znacích jedince nebo opakovatelném jednání, kdy jsou tyto rysy a/nebo jednání pro daného jedince jedinečné a měřitelné, a to i tehdy, když použité vzorky zahrnují určitý stupeň pravděpodobnosti. Typickými příklady takových biometrických dat jsou otisky prstů, struktura obličeje, hlas, ale také geometrie rukou, vzorky žil nebo některé hluboce zakořeněné dovednosti nebo jiné charakteristiky chování (například ručně psaný podpis, stisknutí kláves, konkrétní způsob chůze nebo mluvy atd.).

Samotné obecné nařízení výslovně definuje biometrické údaje v čl. 4 odst. 14 jako *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“.*

Biometrické údaje byly dlouhodobě považovány za osobní údaje. Spornou však zůstávala otázka, zda se jedná o citlivé údaje.[11] Obecné nařízení tento problém vyřešilo, když je zařadilo mezi zvláštní kategorie osobních údajů, tedy takové, které jsou svou povahou zvláště zranitelné a vyžadují zvláštní ochranu při jejich zpracování s ohledem na možný vznik závažných rizik pro základní práva a svobody fyzických osob. Nařízení obsahuje nástroje k ochraně biometrických údajů, které je správce povinen použít. Zvláště je třeba upozornit na to, že u biometrických údajů se zpravidla předpokládá posouzení vlivu na ochranu osobních údajů.[12]

Jaká jsou rizika používání biometrických osobních údajů? Jaké jsou výhody a nevýhody biometrických systémů?

Pokud jde o dopad na ochranu osobních údajů a soukromí, nebyly biometrické systémy dosud v ČR předmětem systematického odborného zájmu ani veřejné diskuse. Jako i v případě jiných technologií, začaly být fakticky používány, aniž by byly řešeny právní a etické důsledky.

Obecně lze říct, že biometrické údaje mají svá pozitiva i negativa. Jako hlavní pozitiva používání biometriky se uvádí efektivní prokazování skutečné identity uživatelů, poskytnutí většího komfortu fyzické osobě, která tak nemůže zapomenout či ztratit identifikátor nebo heslo, případně osobní údaje lze obtížně padělat nebo falšovat.

Biometrické systémy jsou ovšem spojeny i s řadou negativ, která nemusí být na první pohled zřejmá. Rizika, která představují biometrické systémy, vyplývají z jejich samotné povahy.

V první řadě nemohou zaručit úplnou přesnost, vždy existuje riziko vyplývající z nesprávné identifikace, a tedy možnost chybného odmítnutí. Obecně představují riziko především v tom, že jsou založeny na vztahu mezi tělem a identitou, jelikož umožňují, že jsou znaky lidského těla „strojově čitelné“ a mohou být dále použity.

---

[11] Stanovisko WP č. 3/2012 k vývoji biometrických technologií ze dne 27. 4. 2012.
[12] Čl. 35 obecného nařízení a čl. 91 preambule obecného nařízení.

K potenciálním rizikům patří možnost skrytého shromažďování, uchovávání a zpracování údajů, ale i shromažďování materiálů s citlivými informacemi, které mohou narušovat intimní prostor jednotlivce. Únik biometrických údajů může mít dopad na práva a svobody fyzických osob, např. na lidskou důstojnost, soukromí a právo na ochranu údajů. To platí hlavně u zranitelných osob, jako jsou děti, starší osoby a osoby, které nejsou s to provést úplnou registraci.

Jak postupovat při používání biometrických údajů?

Na počátku úvah o použití biometrických zařízení je vždy nutné nejprve zvážit, zda je skutečně v dané situaci nezbytné použít biometrické technologie a zpracovávat biometrické údaje. Takové zvážení bude obzvlášť na místě, pokud se bude jednat o některou ze skupin, které obecné nařízení považuje za zranitelné, např. děti a zaměstnanci. Pokud by nebylo nezbytné použít osobní údaje, je třeba dát přednost jiné alternativě. Často používané zdůvodnění, že použití biometrických údajů je pro zákazníka pohodlné, protože si nemusí nic pamatovat, není dostatečným argumentem.

Je třeba také upozornit, že biometrické technologie, přes jejich stále větší dostupnost (technickou i finanční), nejsou plnou náhradou jiných bezpečnostních řešení a samy o sobě ani nezajišťují větší bezpečnost. Z tohoto hlediska je vždy vhodnější zvažovat kombinaci různých bezpečnostních opatření. Čím vyšší je plánovaná úroveň bezpečnosti, tím méně budou samotné biometrické údaje schopny dosáhnout tohoto cíle právě pro výše uvedená rizika, která jsou s nimi spojena, tj. že nejsou stoprocentně spolehlivé.

Jak bylo uvedeno, biometrické údaje jsou nově řazeny do zvláštní kategorie osobních údajů, pro kterou je stanoven přísnější režim zacházení. Vychází se přitom z toho, že mají citlivou povahu, takže jejich zacházení je spojeno s riziky. Vyžadují tak přísnější zacházení než běžné osobní údaje. Jejich zpracování čl. 9 odst. 1 obecného nařízení se zakazuje, pokud není na místě některá z výjimek v odst. 2 téhož ustanovení.

Pokud jde o to, jak přistupovat k samotnému zpracování biometrických údajů, obecně platí, že po účinnosti GDPR je třeba vždy nově nastavit či zkontrolovat soulad s jeho požadavky. Na prvním místě je vždy třeba posoudit soulad s obecnými principy ochrany dat. Jedná se o principy uvedené v čl. 5 obecného nařízení, k nimž patří především zákonnost, korektnost a transparentnost, ale také účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost a odpovědnost správce. Počítá se zde také s použitím technických a organizačních opatření.

Veškerá opatření v oblasti ochrany osobních údajů nejsou přitom nastavena jednou provždy a je třeba je průběžně aktualizovat.

Nejčastější rizika uváděná ve spojitosti s používáním biometrických osobních údajů

- Biometrické technologie nemohou zajistit úplnou přesnost, vždy existuje riziko vyplývající z nesprávné identifikace.
- Existují potenciální diskriminační důsledky pro osoby, které systém odmítne, nebo které nemohou biometrický údaj z nějakých důvodů poskytnout (např. hendikepované osoby).
- Krádež identity na základě použití zfalšovaných nebo odcizených zdrojů biometrických údajů může vést k vážným škodám.
- Na rozdíl od jiných identifikačních systémů nelze jednotlivci poskytnout novou identifikaci, pokud dojde k jejímu narušení.

- Některé biometrické údaje mohou odhalovat fyzické údaje o jednotlivci, které nezamýšlel poskytnout.
- Mnoho biometrických technologií umožňuje automatické sledování osob nebo vytváření jejich profilů.
- Biometrické technologie, přes jejich stále větší dostupnost (technickou i finanční), nejsou plnou náhradou jiných bezpečnostních řešení a samy o sobě nezajišťují větší bezpečnost. Čím vyšší je plánovaná úroveň bezpečnosti, tím méně budou samotné biometrické údaje schopny dosáhnout tohoto cíle.
- Biometrické systémy často obsahují více informací, než je zapotřebí pro funkce porovnávání, což znamená zvýšené riziko pro osobní údaje.

2. KAMEROVÉ SLEDOVÁNÍ

Další oblastí, které analytické oddělení věnovalo systematickou pozornost, je oblast kamerového sledování. To je dáno tím, že soukromé i veřejné subjekty v posledních letech v rostoucí míře využívají kamerových systémů, přičemž rychlý rozvoj a dostupnost kamer se staly fenoménem, který předstihl právní regulaci.

Na tuto oblast dopadá obecné nařízení a je také předmětem pokynů Sboru k videosledování, do jejichž závěrečné podoby byly zapracovány připomínky z veřejné diskuse. Ačkoliv tyto pokyny nejsou obecně závazné, jsou významnou interpretační pomůckou; jsou formulovány tak, aby byly co nejvíce srozumitelné a návodné pro jejich adresáty (správce, zpracovatele, subjekty údajů).

Pokyny Sboru uvádí, že používání kamer má široké dopady na ochranu soukromí a osobních údajů. To vedlo v rámci EU i v jejích členských státech k průběžné diskusi, jejímž cílem bylo stanovit předpoklady a omezení týkající se instalací zařízení pro kamerové sledování, a nezbytná opatření pro subjekty údajů. K tomu bylo nezbytné hledání vyváženého přístupu mezi více konkurenčními právy. Kamerové sledování z bezpečnostních důvodů je totiž veřejností považováno, ať již oprávněně či nikoli, za jeden z nejefektivnějších způsobů předcházení trestné činnosti. Jejich účelem je odradit potenciální narušitele soukromí, a pokud k narušení již došlo, zajistit důkazy pro účely vedení správního či trestního (přestupkového) řízení. Na druhé straně kamerové sledování představuje velmi závažný zásah do soukromí a ochrany osobních údajů a je třeba jednoznačně stanovit jeho hranice.

Současná právní úprava v oblasti kamerového sledování v ČR[13] se řídí, pokud jde o její principy a stanovení technických a organizačních opatření, která ji mají doprovázet, především obecným nařízením. Jako vhodný praktický návod pro aplikaci konkrétních pravidel je možné použít právě pokyny Sboru ke kamerovému sledování.

Úřad zmíněné pokyny, na jejichž znění se podílel,[14] vnímá jako důležitý nástroj, který povede k celkové kultivaci prostředí v ČR, ve kterém jsou kamery mnohdy používány nadměrně, a nezřídka také v rozporu s právními předpisy. Ovšem jako i u jiných technologií, které se v současné době masově rozšiřují, jejich použití nemůže být neomezené. Pomyslnou hranicí a kritériem pro poměřování situace, zda a kdy mají přednost zájmy nebo základní práva a svobody subjektů údajů, je právo na soukromí a osobní údaje fyzických osob. Pokud jde o kamery, jejich registrace v ČR byla ukončena po zrušení zákona č. 101/2000 Sb.

---

[13] V některých státech existují speciální zákony.
[14] Návrhy Úřadu byly přijaty pouze částečně.

Vzhledem k tomu, že v ČR neexistuje speciální zákon zabývající se kamerami, pro kamerové sledování platí pouze úprava občanského zákoníku a obecného nařízení. Přesné rozhraničení není nastaveno, přičemž v zásadě by se tyto systémy měly doplňovat. Zatímco dříve neexistence speciálního zákona v ČR před účinností GDPR paralyzovala možnost postihu kamerového sledování, současné obecné nařízení umožňuje postupovat pomocí aplikace obecných principů.

GDPR přineslo ve vztahu ke kamerám některé dílčí změny, někdy již současná právní úprava platila, ale nebyla jí věnována pozornost. Tak jako i u zpracování jiných osobních údajů, také při zpracování osobních údajů prostřednictvím kamerového sledování platí, že je to správce, který je plně odpovědný za kamerové sledování, které provádí. Je povinen postupovat podle ustanovení GDPR a jeho zásad, k nimž patří transparentnost, korektnost a zákonnost zpracování, omezení účelem, minimalizace uložení osobních údajů, jejich přesnost a aktualizace, omezení doby zpracování na dobu nezbytně nutnou a integrita zpracování.

Pro správce platí povinnosti stanovené v kapitole IV. obecného nařízení, pokud je po něm lze rozumně požadovat. Pokud se nejedná o výjimku domácího zpracování, která povoluje zpracování osobních údajů v soukromých prostorách vlastníka, správce není oprávněn sledovat veřejný prostor. Výjimky z tohoto zákazu, jak vyplývá z případu SD EU ve věci Ryneš[15] a navazující judikatury NSS,[16] jsou velmi úzké a musí být vždy posuzovány individuálně. Správce je přirozeně povinen veškeré okolnosti, které se týkají jím prováděného kamerového sledování, nejen tvrdit, ale také prokázat. S tím souvisí také to, že je povinen, pokud se nejedná o již zmíněnou domácí výjimku, vést a případně předložit záznamy o zpracování osobních údajů.

Pokud jde o zkušenosti dozorového úřadu v oblasti kamerového sledování, nejčastější jsou stížnosti občanů na to, že jsou neoprávněně sledováni kamerou. ÚOOÚ zpravidla postupuje tak, že vyhodnotí situaci a její závažnost. V některých případech zašle informační dopis vlastníku kamerového systému a informuje ho o právní úpravě a o jeho případných povinnostech. Velmi často je takto sjednána náprava. Informační dopis je důležitý také proto, že dává osobě dotčené sledováním do rukou důkaz, který může použít, pokud dojde k soudnímu sporu.

V dalším průběhu Úřad postupuje individuálně v závislosti na působnosti stanovené zákonem (ta je upravena pro oblast osobních údajů, nikoli soukromí), závažnosti věci a poskytnutých důkazech. V některých případech ÚOOÚ postupuje v součinnosti s jinými orgány, např. s obcí. Použití dozorových a nápravných pravomocí je do jisté míry limitováno tím, že obvykle nemůže ověřit skutečný stav věci na místě sporu, takže ze skutkového hlediska má k dispozici pouze sporná tvrzení účastníků řízení. Právní úprava totiž Úřadu neumožňuje vstup do obydlí a na pozemek soukromé osoby,[17] to je možné pouze v případě vstupu do obydlí podnikatele.

Přesto ÚOOÚ nerezignuje na svou roli v oblasti kamerového sledování. V souvislosti se zveřejněním nových pokynů ke kamerovému sledování bude také veřejnost průběžně informovat o změnách.

---

[15] Rozsudek Soudního dvora (čtvrtého senátu) ze dne 11. prosince 2014 František Ryneš v. Úřad pro ochranu osobních údajů, věc C 212/13.

[16] Rozsudek NSS 1 As 113/2012 - 133.

[17] Ustanovení § 7 zákona č. 255/2012 Sb., o kontrole (kontrolní řád).

Zahraniční spolupráce

• KODEXY CHOVÁNÍ

Kodexy chování jsou dobrovolné nástroje odpovědnosti, které stanoví konkrétní pravidla pro ochranu osobních údajů, tedy nejvíce vhodný právní a etický soubor chování určitého odvětví. Podobně jako osvědčení o ochraně osobních údajů (certifikace) jsou dalším z nových nástrojů pro správce nebo zpracovatele pro zajištění souladu s obecným nařízením.

V červnu roku 2019 byl Sborem schválen dokument „Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679" (Pokyny 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679), který upravil obsah kodexů chování, schvalování (včetně kritérií) kodexů chování či požadavky na akreditaci subjektů pro monitorování kodexů chování.

Koncem roku byly jednotlivé země vyzvány k předložení akreditačních kritérií pro kodexy chování. Úřad Sboru předložil akreditační požadavky v listopadu. Následně probíhala jednání o jejich konečné podobě.

Kvůli určitým nejasnostem v přístupu k řešené problematice a požadavkům ze strany expertní podskupiny *Compliance, eGovernment and Health* bude nutno text upravit a znovu předložit v příštím roce.

• OSVĚDČENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (CERTIFIKACE)

Vydávání osvědčení o ochraně osobních údajů je jedním z nástrojů pro správce nebo zpracovatele osobních údajů, prostřednictvím kterého může doložit soulad prováděného zpracování s obecným nařízením o ochraně osobních údajů.

Podle § 15 zákona č. 110/2019 Sb., o zpracování osobních údajů, byla odpovědnost za vydávání akreditací subjektům pro vydávání osvědčení vložena do rukou národního akreditačního orgánu, kterým je Český institut pro akreditaci. Tato skutečnost ovšem neznamená, že by Úřad v této oblasti neměl žádné kompetence. Především zůstává v gesci ÚOOÚ vytvořit požadavky pro akreditaci subjektů pro vydávání osvědčení a kritéria pro vydávání osvědčení.

V prosinci roku 2017 Úřad zveřejnil a začátkem roku 2018 proběhla veřejná diskuse ke kritériím pro vydávání osvědčení (zahrnují požadavky pro akreditaci i certifikační kritéria).

V červnu roku 2019 byl Evropským sborem pro ochranu osobních údajů (dále „Sbor") schválen dokument „Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (Pokyny 4/2018 pro akreditaci subjektů vydávajících osvědčení podle nařízení 2016/679), který v příloze 1 upravil akreditační požadavky na subjekty pro vydávání osvědčení.

Následně v červenci 2019 poskytl Úřad materiál „Kritéria pro vydávání osvědčení" expertní podskupině Sboru *Compliance, eGovernment and Health* a v říjnu toho roku je oficiálně předal k posouzení v rámci zajištění mechanismu jednotnosti. Následně probíhají jednání o konečné podobě.

Podání žádosti o vydání osvědčení podle obecného nařízení je dobrovolné rozhodnutí správce či zpracovatele, jehož cílem je prokázat soulad s obecným nařízením, nikoliv novou povinností. Do doby, než dojde ke schválení akreditačních požadavků a certifikačních kritérií ze strany Sboru, nelze zatím Úřad žádat ani o vydání akreditace, ani o vydání osvědčení.

V současné době rovněž probíhá v rámci hodnocení požadavků pro akreditaci v odborných pracovních skupinách Sboru diskuse o tom, zda mají být požadavky pro akreditaci, ale i certifikační kritéria, zpracovány na konkrétní zpracování osobních údajů, případně i výrobky či služby. Otázkou je také, zda mohou být tato kritéria i obecnějšího charakteru.

• POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (DPIA)

V roce 2018 předložil Úřad Sboru Seznam druhů operací zpracování osobních údajů, která podléhají posouzení vlivu na ochranu osobních údajů. Konečná verze tohoto dokumentu byla definitivně přijata v lednu 2019.

Následně byl seznam uveřejněn na webových stránkách Úřadu. V březnu 2019 Úřad Sboru předložil rovněž Seznam operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů. Po jeho schválení (v současné době byly zapracovány připomínky Sboru a materiál byl předložen v nové verzi) budou oba seznamy sloučeny do jednoho dokumentu. Ten bude uveřejněn počátkem roku 2020 na webových stránkách Úřadu.

Pro usnadnění činnosti správců ÚOOÚ rovněž připravil a publikoval k veřejné diskusi Metodiku obecného posouzení vlivu na ochranu osobních údajů. Zasílání připomínek a návrhů bylo ukončeno 15. prosince 2019. V průběhu prvního čtvrtletí roku 2020 se pak předpokládá její uveřejnění v upravené verzi.

• PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

V roce 2019 vydal Úřad jedno povolení pro předávání osobních údajů do třetích zemí s neodpovídající úrovní ochrany osobních údajů podle čl. 46 odst. 3 obecného nařízení. Konkrétně šlo o povolení České národní bance, která Úřadu předložila ke schválení správní ujednání pro předávání osobních údajů mezi úřady pro finanční dohled v Evropském hospodářském prostoru a úřady pro finanční dohled mimo Evropský hospodářský prostor.

Uvedené správní ujednání společně vypracovaly Evropský orgán pro cenné papíry a trhy (ESMA) a Mezinárodní organizace komisí pro cenné papíry (IOSCO). Stalo se tak v úzké spolupráci s expertní podskupinou pro mezinárodní transfery Sboru, s níž výše uvedení tvůrci text správního ujednání dlouhodobě konzultovali.

Formou oficiálního dopisu předložily ESMA a IOSCO uvedené správní ujednání ve své finální podobě předsedovi Sboru, který jej následně požádal o stanovisko podle čl. 64 odst. 2 obecného nařízení. Na základě této žádosti vypracoval Sbor stanovisko č. 4/2019 ze dne 12. února 2019, ve kterém konstatoval, že předložené správní ujednání zajistí vhodné záruky pro předávání osobních údajů. Ta budou realizována na základě tohoto správního ujednání, ve smyslu ustanovení čl. 46 odst. 1 a odst. 3 písm. b) obecného nařízení.

Úřad se tedy ve svém rozhodnutí mohl opřít o právě uvedené stanovisko Sboru, přičemž vyhodnotil, že v daném případě česká právní úprava ochrany osobních údajů nevyžaduje žádné další záruky, a nejsou známy jiné skutečnosti, z nichž by vyplývala konkrétní rizika specifická pro Českou republiku. Proto dané správní ujednání povolil jako nástroj poskytující a stanovující vhodné záruky pro předání osobních údajů do třetích zemí nebo mezinárodní organizaci podle čl. 46 odst. 1 a odst. 3 písm. b) obecného nařízení.

Vznik daného správního ujednání a použitá schvalovací procedura představují do značné míry precedens a modelový příklad, jakým způsobem by se mělo postupovat i v dalších případech tvorby nezávazných „správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektů údajů" podle čl. 46 odst. 3 písm. b) obecného nařízení.

Na výše probraném příkladu vývoje problematiky správních ujednání se zřetelně ukázalo, že i zbytkové povolovací kompetence ÚOOÚ jsou výrazně vázány na názory a stanoviska Sboru.

V důsledku se tak v režimu obecného nařízení těžiště činnosti Úřadu v oblasti předávání osobních údajů do třetích zemí přesunulo z vlastní samostatné výkladové a rozhodovací činnosti na spolupráci se Sborem, a to především v rámci expertní podskupiny pro mezinárodní transfery. V rámci expertní podskupiny pro mezinárodní transfery se ÚOOÚ aktivně podílel na formulaci dokumentu, který má vyjasnit vztah mezi aplikací čl. 3 a kapitoly V. obecného nařízení. Jde o vysvětlení, za jakých podmínek mohou správci a zpracovatelé ve třetích zemích, kteří podléhají přímo GDPR, zpracovávat osobní údaje předané či přenesené z Evropské unie.

Součástí dokumentu přitom měla být tak zásadní věc, jakou je definice předání osobních údajů do třetí země. Avšak z důvodu různých východisek jednotlivých národních delegací se v dané věci jen obtížně a dlouze nachází konsensus, takže práce na dokumentu bude završena až v následujícím období.

V pozici spoluautora se Úřad se také podílel na vypracování stanoviska Sboru č. 16/2019 ze dne 12. listopadu 2019 k návrhu rozhodnutí belgického dozorového úřadu o schválení závazných podnikových pravidel pro správce společnosti ExxonMobil Corporation. Spolu se stanoviskem Sboru č. 15/2019 k návrhu rozhodnutí britského dozorového úřadu o schválení závazných podnikových pravidel pro správce společnosti Equinix Inc. přitom šlo o první dvě vydaná stanoviska v rámci schvalovací procedury závazných podnikových pravidel v režimu obecného nařízení vůbec.

Kladné stanovisko Sboru, vydané v souladu s čl. 64 odst. 1 písm. f) obecného nařízení, tak prakticky završuje schvalovací proceduru závazných podnikových pravidel. Na takové stanovisko již navazuje pouze rozhodnutí vedoucího dozorového úřadu, kterým jsou konkrétní závazná podniková pravidla definitivně schválena, přičemž ostatní dozorové úřady již žádnou další autorizaci neprovádějí.

Za zmínku přitom stojí, že v současné době čeká na projednání v rámci expertní podskupiny pro mezinárodní transfery a na stanovisko Sboru několik desítek konkrétních návrhů závazných podnikových pravidel.

Stanovisku Sboru předchází několikafázové hodnocení konkrétního návrhu závazných podnikových pravidel, kterého se aktivně účastní vedle vedoucího dozorového úřadu především jeden až dva dozorové úřady v pozici spoluhodnotitelů (viz Pracovní dokument WP263 vykládající schvalovací proceduru závazných podnikových pravidel pro správce a pro zpracovatele v režimu obecného nařízení). V průběhu roku 2019 Úřad v roli spoluhodnotitele připomínkoval revidované návrhy závazných podnikových pravidel v rámci tří schvalovacích procedur.

Vedle práce na konkrétních návrzích správních ujednání a závazných podnikových pravidel, přípravě každoročního společného hodnocení amerického programu štítu soukromí, či řešení jiných aktuálních úkolů, se expertní podskupina pro mezinárodní transfery soustředila na formulování obecnějších výkladových materiálů. Ty budou vesměs dopracovány v příštím roce.

Kromě již výše zmíněného dokumentu o vzájemné souhře mezi čl. 3 a kapitolou V. obecného nařízení má podskupina rozpracovány ve finální fázi

- pokyny k předávání osobních údajů mezi veřejnými subjekty [čl. 46 odst. 3 písm. b) a odst. 2 písm. a) obecného nařízení],
- pokyny ke kodexům chování a certifikacím jako nástrojům předávání osobních údajů do třetích zemí [čl. 46 odst. 2 písm. e) a f) obecného nařízení].

Druhým úkolem, který Komisi a podskupinu čeká v příštím roce a který vyplývá ze znění čl. 45 odst. 3 obecného nařízení, je přezkum všech třinácti rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů. Ta byla přijata ještě v režimu směrnice 95/46/ES.

• SCHENGENSKÁ SPOLUPRÁCE

Zpracování osobních údajů rozsáhlými evropskými informačními systémy je významnou součástí schengenské spolupráce v oblasti svobody, bezpečnosti a práva. Ochrana osobních údajů zpracovávaných v těchto informačních systémech vyžaduje zvláštní pozornost, přičemž zcela nezastupitelnou roli v této oblasti plní nezbytné legislativní úpravy.

Mezi tyto systémy patří

- Schengenský informační systém druhé generace (SIS II),
- Vízový informační systém (VIS),
- databáze otisků prstů Eurodac,
- Celní informační systém (CIS).

Úřad a ostatní vnitrostátní dozorové orgány jednající v rozsahu svých příslušných pravomocí spolupracují s Evropským inspektorem ochrany údajů (EDPS) a za účelem koordinovaného dohledu nad informačními systémy se alespoň dvakrát do roka setkávají v rámci koordinačních skupin k těmto systémům – SIS II SCG, VIS SCG, Eurodac SCG, CIS SCG.

Jednání se kromě zástupců dozorových úřadů a EDPS pravidelně účastní zástupci Evropské komise spolu s pověřencem pro ochranu osobních údajů Evropské agentury pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (agentura eu-LISA). Ti informují přítomné zástupce členských států s ohledem na jednotlivé systémy o aktuálním stavu, legislativním vývoji a příslušných statistikách.

Úřad plní v rámci své působnosti v souvislosti se schengenskou spoluprací úlohu vnitrostátního dozorového orgánu, který vykonává dohled nad dodržováním příslušných předpisů a dále přispívá k ochraně základních práv osob, jejichž osobní údaje jsou předmětem zpracování v rámci schengenského prostoru. Pověřený zástupce Úřadu se navíc pravidelně účastní jednání již zmíněných koordinačních skupin, kde Úřad sdílí své zkušenosti z dozoru s ostatními členskými státy. K této spolupráci patří i speciálně zřízená Rada spolupráce pro Europol, která funguje od roku 2017.

Kromě dohledu a kontroly souvisejícími s plněním požadavků na zákonné zpracování osobních údajů ze strany správce v rámci výše zmíněných informačních systémů se Úřad v průběhu roku 2019 zabýval také přeměnou dosavadního modelu koordinovaného dozoru podle nového nařízení Evropského parlamentu a Rady (EU) 2018/1725. Tento model by měl nejpozději do roku 2021 plně zaštiťovat Evropský sbor pro ochranu osobních údajů.[18]

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. ÚOOÚ v roce 2019 v této věci obdržel celkem 58 podnětů týkajících se zpracování osobních údajů v SIS II, přičemž ve 26 případech přezkoumával postup Policie ČR ve věci zpracování osobních údajů. Ve většině případů se jednalo o podezření z porušení nedodržení zákonné lhůty k informování žadatelů o přístup k osobním údajům zpracovávaným v SIS II. Ve dvou případech se Úřad podílel na přeshraniční spolupráci mezi dozorovými orgány.

Úřad dále obdržel celkem 13 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 ÚOOÚ, byli jednotliví žadatelé odkázáni na ministerstvo zahraničních věcí a na příslušné zastupitelské úřady v zahraničí. Úřad v této souvislosti průběžně objasňoval své kompetence svěřené mu zákonem o zpracování osobních údajů, jakož i unijními právními předpisy.

---

[18] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (specificky čl. 62).

Statistiky ÚOOÚ týkající se navýšení počtu podnětů k SIS II zřetelně ukazují narůstající tendenci počtu žádostí o přístup k osobním údajům v SIS II, kdy počet těchto podnětů vzrostl oproti roku 2018 více než o 100 procent (zejména od občanů států bývalého Sovětského svazu). Oproti tomu mírně ubylo podnětů vztahujících se k vízové politice České republiky a vydávání víz.

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,
- ochrana osobních údajů.

Hodnotící týmy jsou vždy vytvářeny ad hoc k jednotlivým evaluacím a 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 návštěvy útvarů, včetně dalších místních šetření na místech, jež zajišťují provoz národní součásti schengenské databáze, orgánu pro ochranu osobních údajů a dalších dotčených institucí.

V roce 2019 se vyjma dalších čtyř států uskutečnila schengenská evaluace České republiky. Týdenní hodnotící mise přinesla Úřadu cenná doporučení, jež byla následně implementována do praxe nebo zahrnuta do plánu kontrol ÚOOÚ pro rok 2020.

V roce 2019 se zaměstnanec Úřadu účastnil jako národní expert evaluační týdenní mise v Maďarsku (říjen 2019).

• MEZINÁRODNÍ ČINNOST

Mezinárodní činnost probíhala s ohledem na působnost Úřadu v několika rovinách:

- v rámci kontroly (šetření případů s cizím prvkem),
- v rámci agendy předávání údajů do zahraničí,
- v neposlední řadě z titulu člena Sboru.

Tento oddíl se zabývá především zapojením ÚOOÚ do struktur Evropské unie a činností ve Sboru, zatímco předchozí dvě oblasti jsou zahrnuty v kapitolách výše.

Sbor byl ustaven obecným nařízením. Jeho členy jsou především předsedové dozorových úřadů z každého členského státu. Vnitrostátní dozorové úřady se tak mají příležitost přímo, v různých formách, podílet na činnosti Sboru, především na tvorbě odborných materiálů.

Členové Sboru se s výjimkou srpna scházejí na plenárním zasedání v Bruselu jednou měsíčně.

Vedle toho vyvíjí průběžně činnost několik expertních skupin, do kterých úřady mohou jmenovat své stálé delegáty nebo se podílet na jejich aktivitách formou písemného připomínkování. Tyto tematicky specializované skupiny se scházejí na svých jednáních podle potřeby a průběžně komunikují v rámci vlastní elektronické platformy:

- Expertní skupina pro klíčová ustanovení
- Expertní skupina pro mezinárodní předávání
- Expertní skupina pro technologii
- Expertní skupina pro spolupráci
- Expertní skupina pro hranice, cestování a vynucování práva
- Expertní skupina pro právní soulad, e-government a zdravotnictví
- Expertní skupina pro finanční záležitosti
- Expertní skupina pro prosazování práva
- Expertní skupina pro uživatele informačních technologií
- Expertní skupina pro sociální média

Každá ze skupin pracuje na základě plánu činnosti, který schvaluje plenární zasedání. Výsledkem činnosti jsou nejčastěji materiály ve formě pokynů nebo stanovisek. Tyto dokumenty jsou zpracovávány řešitelskými týmy, které jsou v expertních skupinách sestavovány na principu dobrovolnosti. Delegáti Úřadu se ve sledovaném roce podíleli coby členové řešitelského týmu na tvorbě dokumentů v devíti případech. Jednalo se o přípravu následujících materiálů, z nichž první dva byly již schváleny a publikovány:

- Stanovisko k otázkám a odpovědím týkajícím se vzájemného působení nařízení o klinických hodnoceních a obecného nařízení (čl. 70 odst. 1 písm. b)
- Pokyny k místní působnosti obecného nařízení (článek 3)
- Návrh stanoviska k pravomoci dozorového úřadu v případě změny okolností týkajících se hlavní nebo jediné provozovny
- Návrh pokynů ke zpracování osobních údajů prostřednictvím videozařízení
- Návrh pokynů k právům subjektu údajů – v přípravě (mandát schválen v září 2019)
- Návrh pokynů k monetizaci osobních údajů
- Návrh dokumentu vysvětlujícího vzájemný vztah mezi článkem 3 a kapitolou V. obecného nařízení
- Analýza seznamů druhů operací zpracování, u nichž není nutné posouzení vlivu na ochranu osobních údajů (čl. 35 odst. 5 obecného nařízení), předložených některými vnitrostátními úřady v rámci mechanismu jednotnosti a příprava stanovisek Sboru k těmto seznamům
- Analýza závazných podnikových pravidel předložených skupinou ExxonMobil a příprava stanoviska Sboru

ÚOOÚ se také podílí na činnosti Poradního výboru (T-PD) k Úmluvě Rady Evropy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat a svého delegáta vysílá na pravidelná plenární zasedání dvakrát do roka. Ve sledovaném roce se výbor zabýval například umělou inteligencí a zkoumáním dopadů tohoto fenoménu do soukromí jednotlivce nebo problematikou zařazování tématu ochrany dat do školní výuky.

Pracovníci Úřadu se účastní vybraných, převážně pravidelně pořádaných, konferencí a seminářů. Z nich nejvýznamnější jsou Evropská konference dozorových úřadů pro ochranu dat a Mezinárodní konference komisařů ochrany dat a soukromí (ICDPPC, nově GPA), která

poskytuje příležitost setkání a výměny poznatků s ochránci dat i z jiných kontinentů. Každá akce se koná jednou ročně.

Z dalších akcí, které stojí za zmínku, uveďme dvakrát ročně pořádaný seminář Evropské komise k výměně zkušeností z dozorové praxe (Case Handling Workshop) či zasedání Mezinárodní pracovní skupiny pro ochranu dat v telekomunikacích, což je jedna z pracovních skupin při ICDPPC (nově GPA).

Svobodný přístup k informacím

• PŘÍPRAVA NA ZAJIŠTĚNÍ NOVÉ PŮSOBNOSTI ÚŘADU DLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

Dne 24. dubna 2019 byl ve Sbírce zákonů publikován zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. Tím došlo mimo jiné ke změně zákona č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů (dále jen „Informační zákon"), kterým byla Úřadu stanovena nová působnost v oblasti práva na informace s účinností od 2. ledna 2020. Od tohoto data bude Úřad příslušný pro posuzování podnětů a vedení přezkumných řízení, stane se odvolacím orgánem pro ty povinné subjekty, u kterých nelze určit nadřízený orgán podle zákona č. 500/2004 Sb., správní řád, a rovněž bude poskytovat ochranu před nečinností nadřízených orgánů.

Informační zákon zcela nově připouští provedení přezkumného řízení u rozhodnutí o odvolání a rozhodnutí o rozkladu. Působnost k posouzení podnětů k zahájení přezkumného řízení a vedení přezkumného řízení ve všech případech náleží ÚOOÚ. Žadatel o informace, jehož žádost byla povinným subjektem odmítnuta, resp. odvolání nebo rozklad byl zamítnut, se bude moci s podnětem na přezkum rozhodnutí obrátit na Úřad. Využití tohoto institutu je výhradně volbou žadatele o informace a není tím dotčeno jeho právo napadnout dané rozhodnutí žalobou u soudu.

ÚOOÚ dále náleží působnost nadřízeného orgánu pro povinné subjekty, u kterých dosud odvolání či stížnosti vyřizoval ten, kdo stojí v čele povinného subjektu. Určení nadřízeného orgánu dle ustanovení Informačního zákona

přichází v úvahu pouze u povinných subjektů, u kterých nelze určit nadřízený orgán dle § 178 zákona č. 500/2004 Sb., správní řád. Typicky se jedná o obchodní společnosti ve 100% vlastnictví státu, krajů, měst či obcí, ale i další subjekty. Počet takto definovaných povinných subjektů, pro které bude Úřad plnit roli nadřízeného orgánu, nelze stanovit. Jeho působnost bude muset být vždy individuálně posouzena.

Úřad bude rovněž řešit podněty a žádosti na ochranu před nečinností nadřízených orgánů povinných subjektů. Tato agenda bude zajištěna pro řízení o odvolání nebo rozkladu a pro vyřizování stížností. Příslušnost Úřadu je dána i k provedení exekuce informačních příkazů, které sám vydá jako nadřízený orgán či v rámci vedeného přezkumného řízení.

S ohledem na přijetí výše uvedené změny zákona byly zahájeny přípravy na zajištění nové působnosti v oblasti práva na informace krátce po jeho publikaci ve Sbírce zákonů. V případě přezkumného řízení bylo nezbytné v rámci možností zejména vyhodnotit potenciální nápad podnětů, jelikož se jedná o zcela novou, dosud nevykonávanou činnost. Na základě statistických údajů u vybraných povinných subjektů byl stanoven základní odhad objemu této nové agendy. ÚOOÚ rovněž předběžně vyhodnotil, pro které povinné subjekty bude nadřízeným orgánem. Závazné posouzení v této otázce však bude možné činit až od účinnosti přijatých změn.

Nová působnost byla do právních předpisů doplněna na základě pozměňovacího návrhu v průběhu projednávání Poslaneckou sněmovnou Parlamentu ČR, proto bylo nutné vyčíslit požadavky Úřadu na její zajištění, zejména pak na posílení personální kapacity a navrhnout odpovídající změnu systemizace. Od listopadu 2019 bylo nově vytvořeno oddělení práva na informace, které agendu v oblasti práva na informace zajišťuje.

Již od června 2019 se na ÚOOÚ obraceli s podněty někteří žadatelé o informace. Kromě toho Úřad obdržel žádosti o stanovisko od řady povinných subjektů, zda bude či nebude jejich nadřízeným orgánem.

Činnost Úřadu, ač účinnost uvedených změn nastává až v lednu 2020, ve svěřené oblasti započala již ve druhé polovině roku 2019.

• POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

V oblasti poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, se v roce 2019 plně projevila účinnost obecného nařízení. Přestože nabylo účinnosti již v roce 2018, výrazně ovlivnilo agendu svobodného přístupu k informacím až v roce 2019. Důvodem bylo, že většina žádostí o informace byla motivována snahou získat poznatky z dozorové činnosti Úřadu ve vztahu k obecnému nařízení. Tato skutečnost tak ovlivnila jak obsah žádostí, tak i jejich počet, ve srovnání s předchozími roky.

Z obsahového hlediska měli žadatelé všech věkových i profesních skupin zájem především o obecné statistické informace k dozorové činnosti ÚOOÚ ve vztahu k obecnému nařízení, tj. kolik udělil pokut, v jaké výši, za porušení kterých článků, ale také kolik obdržel ohlášení porušení zabezpečení osobních údajů.

Mezi další informace, které žadatelé požadovali, patřily například výše rozpočtu, poskytnutí organizačního či pracovního řádu, výročních zpráv v tištěné podobě, či zda a v kolika případech Úřad řešil tzv. regresivní náhrady dle zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem.

Se zvýšeným zájmem veřejnosti o dozorovou činnost ÚOOÚ, resp. jejími konkrétními výsledky ve vztahu k obecnému nařízení, souvisel i vyšší počet žádostí, jejímž předmětem bylo samotné poskytnutí kontrolních protokolů či rozhodnutí Úřadu. Zvýšený zájem byl též o kontrolní protokoly či rozhodnutí ÚOOÚ v rámci dozorové činnosti v oblasti šíření obchodních sdělení dle zákona č. 480/2004 Sb., o některých službách informační společnosti.

Tyto výstupy z kontrolní a rozhodovací činnosti Úřadu byly žadatelům poskytovány, avšak s vyloučením informací, které zákon č. 106/1999 Sb. z poskytování vylučuje, jako jsou osobní údaje (např. stěžovatelů) a též informace, které spadají pod ustanovení § 11 odst. 2 a 3 zákona č. 106/1999 Sb. V tomto případě se jednalo o informace k zabezpečení osobních údajů u kontrolovaných osob či jiné významné informace, které ÚOOÚ od kontrolované osoby získal.

Od tří žadatelů, kteří požadovali poskytnutí velkého počtu kontrolních protokolů či rozhodnutí nebo poskytnutí jiné informace, zahrnující mimořádně rozsáhlé vyhledávání, byla v souladu s § 17 zákona č. 106/1999 Sb. požadována úhrada nákladů za mimořádně rozsáhlé vyhledávání, zahrnující i provedení nezbytného vyloučení informací z poskytovaných dokumentů. Předmětné náklady byly ve všech třech případech uhrazeny, souhrnná výše činila 4 950 Kč.

Oproti roku 2018, kdy Úřad obdržel 56 žádostí, se v roce 2019 věnoval celkem 90 žádostem. Z toho:

- v 63 případech byla informace poskytnuta v celém požadovaném rozsahu,
- ve 24 případech Úřad částečně odmítl informaci poskytnout,
- ve 3 případech informaci odmítl poskytnout úplně.

Informační systém ORG v systému základních registrů

Informační systém ORG Úřad provozuje od roku 2012 jako součást systému základních registrů a od roku 2018 jako součást kritické informační infrastruktury státu a součást e-governmentu České republiky. Jedná se o samostatnou působnost a její naplňování je v Úřadu organizačně odděleno.

Základní registry jsou unikátní zdroje nejčastěji využívaných údajů při výkonu veřejné správy. Zajišťují kvalitní, aktuální a ověřené údaje efektivně využívané pro výkon veřejné správy. Základní registry shromažďují a uchovávají základní informace o fyzických osobách, právnických osobách, podnikajících fyzických osobách, adresách a orgánech veřejné moci. Informační systém ORG jednotlivé registry propojuje a vede seznam agend, které mohou systém využívat. ÚOOÚ pro potřeby základních registrů vytváří zdrojové identifikátory fyzických osob a agendové identifikátory fyzických osob a zajišťuje převod agendového identifikátoru fyzické osoby v agendě na agendový identifikátor této fyzické osoby v jiné agendě.

Samotný provoz systému, který nadále pro Úřad zajišťoval systémový integrátor TESCO SW a. s., byl v roce 2019 bez výpadků v komunikaci a dostupnosti dat. Ke konci roku 2019 bylo v systému zaregistrováno 427 agend. Za rok 2019 bylo nově vygenerováno 91–100 zdrojových identifikátorů.

Po celou dobu je IS ORG provozován se stejnou infrastrukturou. Hardware je stále udržován pouze formou výměny poškozených částí (disky, zdroje apod.). Dnes se ukazuje, že je již technicky i morálně překonaný a zastaralý, a to nejen s ohledem na rozvojové záměry systému základních registrů. Provozování systému je silně závislé na dodavatelích komunikačních linek.

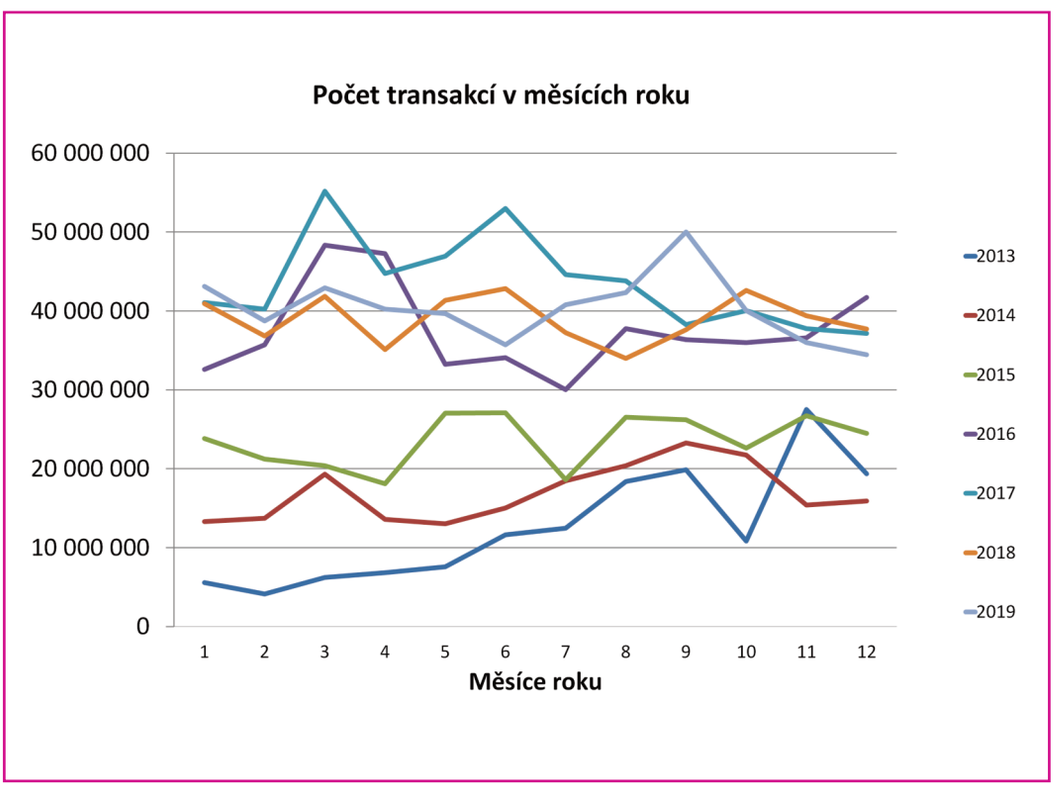
Zajištění nutného chodu a rozvoje systému vychází z těchto podmínek: roční 20% nárůst zatížení ZR do roku 2021, pokračování transformačního projektu řešícího obnovu a rozvoj základních registrů veřejné správy a návazných systémů, provoz ZR za stávajících úrovní poskytovaných služeb (SLA), provoz ZR pouze na výrobcem certifikovaném HW a SW a zajištění kybernetické bezpečnosti.

Na doporučení Správy základních registrů je IS ORG certifikován podle ČSN/ISO 27001:2014. V prosinci 2019 byl bez nálezu recertifikován na další tři roky. V tomto roce byl IS ORG rovněž zkontrolován Národním úřadem pro kybernetickou a informační bezpečnost. I tato kontrola, stejně jako interní audit, byly uzavřeny bez nálezu. Kontrolovány byly například směrnice pro řízení přístupu do datových center, provozní řády, bezpečnostní politiky, registr rizik a aktiv, plán obnovy apod. Bezpečnostní dokumentace předepsaná na základě zákona o kybernetické bezpečnosti byla aktualizována.

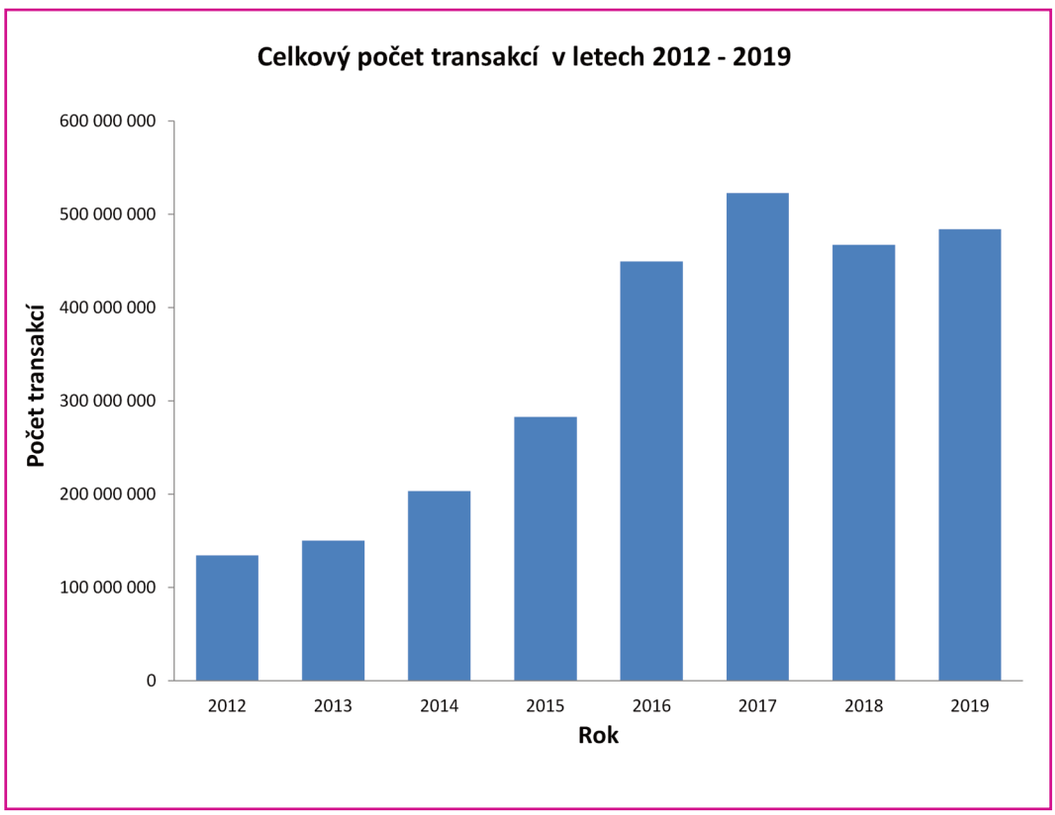
V roce 2019 byly nově nastaveny a doladěny nástroje pro sledování přístupů do systému pro bezpečnostní účely. Tyto nástroje hlásí a registrují pravděpodobné a skutečné kybernetické útoky na IS ORG.

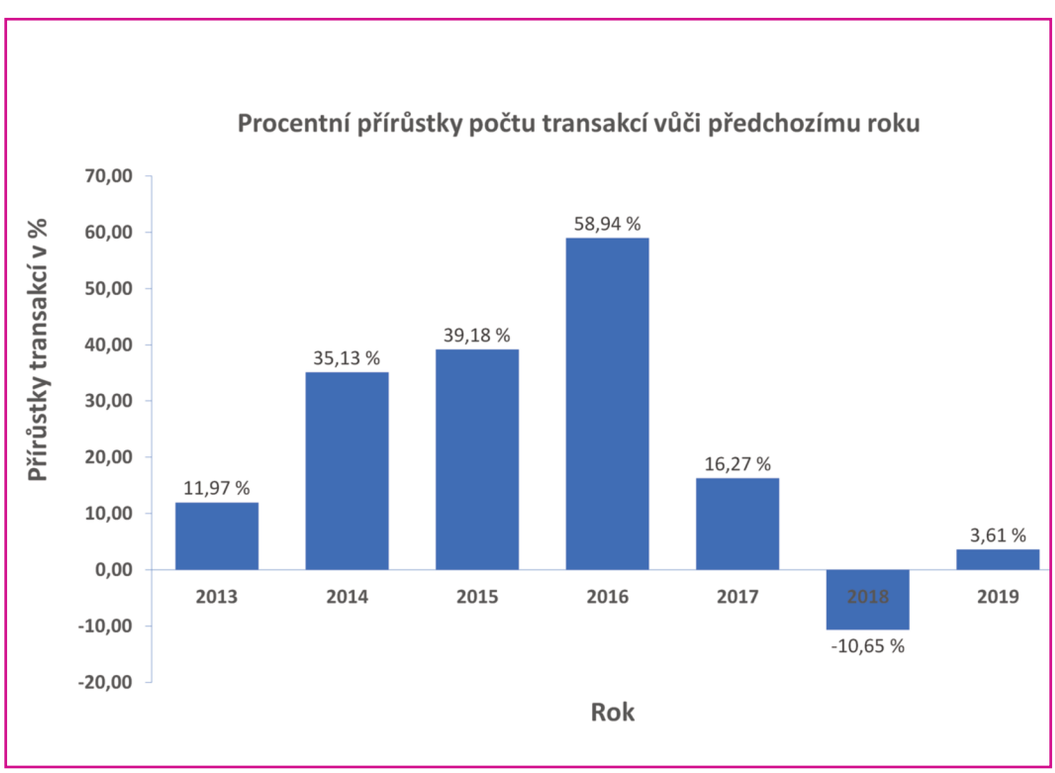
Na rozdíl od předchozích let, kdy největší zatížení připadalo na jarní měsíce březen a duben, letos byla špička v září. Letošní denní maximum vytíženosti systému ORG bylo 4. září 2019 s počtem 2 155 924 transakcí. Naopak denní minimum bylo 6. 9. 2019 s počtem 140 869 transakcí. Měsíční maximum bylo v září s počtem transakcí 50 023 694 a měsíční minimum bylo v listopadu s počtem 35 000 469 transakcí. Proti minulému roku bylo o 3,98 procenta transakcí méně. V absolutních číslech to je pokles o 18 607 059 transakcí.

Jako každý rok i letos přinášíme přehled vytíženosti informačního systému ORG; vybrané parametry jsou uvedeny rovněž meziročně.



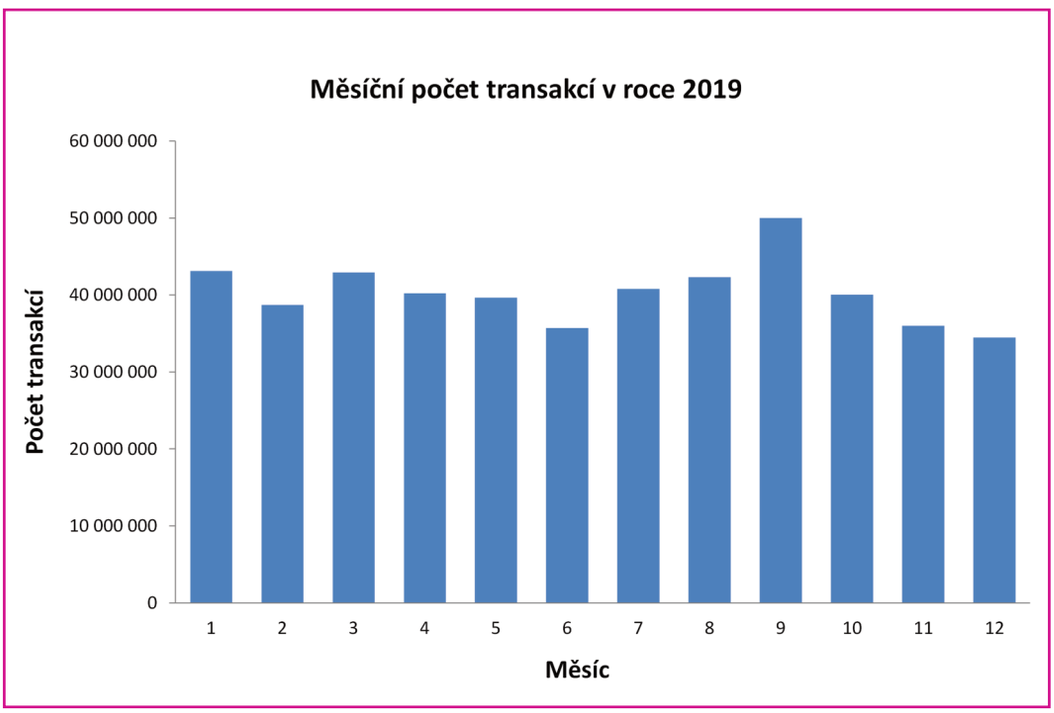
Využívání IS ORG je patrné z grafu „Celkový počet transakcí v letech 2012–2019“.



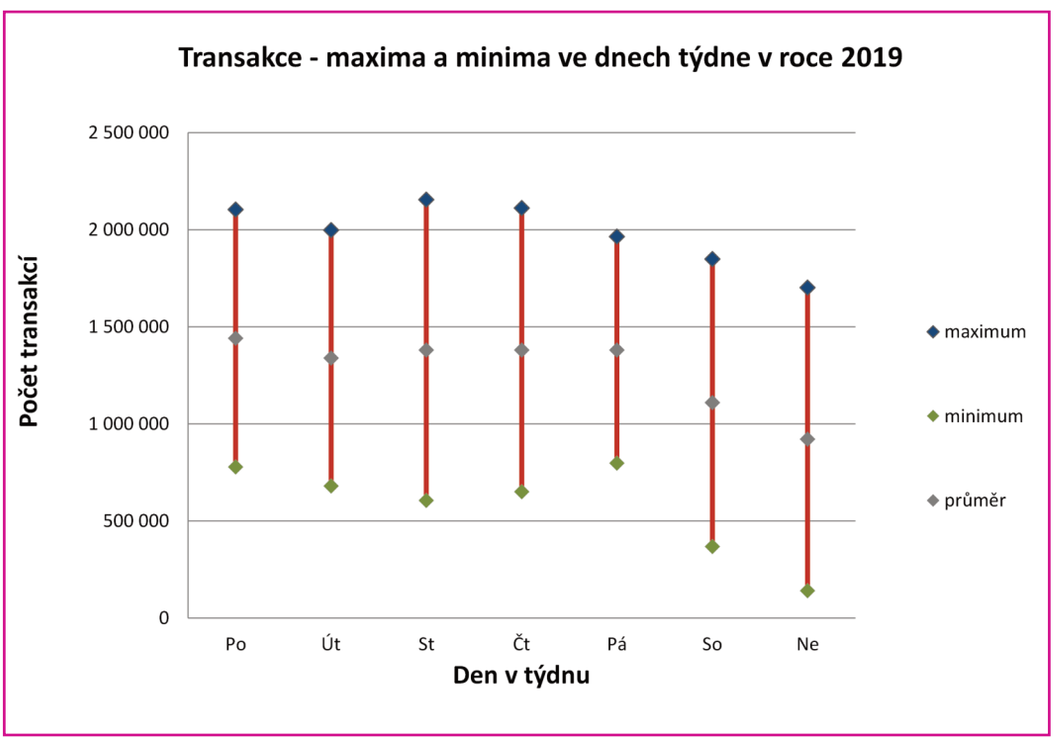


Zobrazení pohybu počtu transakcí proti předchozím letům v procentech obsahuje předchozí graf „Procentní přírůstky počtu transakcí vůči předchozímu roku“.

Rozložení požadavků na systém základních registrů v průběhu roku je vidět na grafu „Měsíční počet transakcí v roce 2019“.



Další graf ukazuje vytížení systému během týdne. Jsou zde uvedeny maximální a minimální hodnoty počtu transakcí v jednotlivých dnech.



Sdělovací prostředky a komunikační nástroje

Z mediálního pohledu byl pro Úřad rok 2019 obdobím výročí (rok od nabytí účinnosti obecného nařízení), ale také novinek (počátek účinnosti nové české právní legislativy k ochraně osobních údajů).[19] Významnou mediální agendou ÚOOÚ byly také úniky dat velkých internetových subjektů a porušení zabezpečení ve formě hackerských útoků.[20]

Dalšími častými tématy, o která se novináři v roce 2019 zajímali, byla otázka provozování kamer a kamerových systémů, telemarketing, kontroly Úřadu, cookies, sdílená doprava, biometrické údaje, nevyžádaná obchodní sdělení a obecně zveřejňování údajů na internetu. ÚOOÚ musel také často reagovat na dotazy týkající se nulového správního trestu pro orgány veřejné moci a veřejné subjekty, i v případech, kdy došlo k porušení zákona.

Úřad se stejně jako v předchozích letech věnoval podpoře mezinárodního Dne ochrany osobních údajů a připojil se rovněž k oslavám Dne bezpečnějšího internetu na podporu bezpečnějšího internetu. Velký význam přikládá dlouhodobě také Středoškolské soutěži v kybernetické bezpečnosti, která má za cíl prověřit znalosti a dovednosti studentů právě v kybernetické oblasti. Další ročník proto ÚOOÚ opět podpořil, jak odborně, tak materiálně.

Ani rok 2019 nebyl pro Úřad výjimkou z hlediska osvěty. Připravil akce jak pro laickou, tak odbornou veřejnost, s cílem zvýšení povědomí o ochraně dat. Velkému zájmu se těšily zejména semináře určené pověřencům pro ochranu osobních údajů, které sloužily k předávání praktických poznatků z praxe. V uplynulém roce bylo v prostorách ÚOOÚ uspořádáno pět takových setkání.

Úřad rovněž pokračoval v uveřejňování vlastních neoficiálních překladů materiálů Evropského sboru pro ochranu osobních údajů. Věnoval se též konzultační činnosti všemi dostupnými komunikačními kanály.

---

[19] Zákon č. 110/2019 Sb. ze dne 12. března 2019 o zpracování osobních údajů, který nahradil již neúčinný zákon č. 101/2000 Sb., o ochraně osobních údajů.

[20] Útok provedený počítačovými odborníky nelegální formou. Bez oprávnění dochází z jejich strany k průniku do systémů, obvykle prostřednictvím škodlivého softwaru, s cílem získat přístup k interním datům. Častou formou hackerských útoků bývá také zahlcení systému nadměrným počtem přístupů na konkrétní stránku.

MEDIÁLNÍ OBRAZ

Z hlediska mediálního nebyl ÚOOÚ v roce 2019 spojován s žádnou mediálně negativní kauzou. Novináři se však výraznějším způsobem zabývali výší pokut v souvislosti s obecným nařízením. Úkolem Úřadu proto bylo zdůrazňovat, že pokuty za porušení obecného nařízení mají být odrazující, nikoli však likvidační, což bylo potvrzeno výší pokut udělených v průběhu roku.

KNIHOVNA

V roce 2019 se knihovna ÚOOÚ rozrostla o 90 svazků, z čehož čtyři obdržela darem. Ve většině případů se jednalo o publikace potřebné ke každodenní práci zaměstnanců Úřadu. Kromě toho pokračovalo budování knihovny jako odborného místa zaměřeného na ochranu osobních údajů. Proto byly pořízeny všechny publikace, které v rámci České republiky v uvedeném roce k problematice ochrany dat vyšly. Úřad zakoupil také některé odborné zahraniční knihy (např. *Post-Reform Personal Data Protection in the EU; Privacy, Data Protection and Cybersecurity in Europe; The EU GDPR General Data Protection Regulation: Answers to the Most Frequently Asked Questions nebo Internet of Things Security and Data Protection*).

V roce 2019 reagoval ÚOOÚ na všechny žádosti o návštěvu knihovny či zapůjčení knih z řad veřejnosti kladně s jednou výjimkou. V této souvislosti je třeba připomenout, že knihovna je veřejnosti k dispozici pouze prezenčně a na základě předchozí domluvy. Předmětné žádosti proto nebylo možno vyhovět. V ostatních případech žadatelé knihovnu navštívili a získali zde potřebné informace buď pro svou práci nebo pro studium. V několika případech využili jejích služeb také zájemci o složení úřednické zkoušky v oboru 60 – Ochrana osobních údajů.

Ve dvou případech byly knihovně věnovány výtisky studentských prací. Jednalo se o jednu disertační a jednu bakalářskou práci. Právě ta byla dokonce v roce 2019 vyhlášena **nejlepší bakalářskou prací v rámci soutěže ESOP 2019** (Excelentní Studentské Odborné Práce), kterou vyhlašuje Vysoká škola ekonomická v Praze.

Ke konci roku 2019 disponovala knihovna Úřadu téměř 2600 svazky. Seznam odborných publikací o ochraně osobních údajů a příbuzných tématech je trvale dostupný na webových stránkách ÚOOÚ.

WEBOVÉ STRÁNKY

Primární komunikační kanál i nadále představují webové stránky. Úřad je využíval pro zveřejňování informací pro širokou veřejnost, včetně mládeže. Pokračoval také v aktualizaci webu a ve změnách jeho struktury s cílem udělat jej přehlednějším a s rychle dostupnými aktuálními informacemi. Rubrika GDPR (obecné nařízení) si sice ponechala své výsadní postavení, ale ÚOOÚ se věnoval rozvoji související Poradny, ve které veřejnost nalezne celou řadu cenných informací a praktických návodů pro řešení běžných životních situací.

Novinkou na konci roku byla rubrika Právo na informace popisující novou působnost Úřadu vyplývající z novely zákona o svobodném přístupu k informacím.

Provoz Úřadu

• PERSONÁLNÍ OBSAZENÍ

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

Celkový počet systemizovaných míst k 1. lednu 2019 byl 109. K poslednímu dni roku 2019 pak činil 115.

Fluktuace zaměstnanců se v roce 2019 v meziročním srovnání s předchozím rokem zvýšila z 9 % na 11,8 %.

Plynule pokračoval chod jednotlivých procesů personální správy ÚOOÚ v návaznosti na vývoj zákona o státní službě a dalších relevantních změn legislativy. Nově vzniklá funkce místopředsedy Úřadu byla na základě usnesení Senátu Parlamentu České republiky v červnu obsazena Mgr. Josefem Prokešem.

S účinností od 1. října 2019 byla systemizace Úřadu navýšena o pět systemizovaných míst. Jednalo se o přípravu na svěření nové působnosti ve vztahu k zákonu č. 106/1999 Sb., o svobodném přístupu k informacím od roku 2020.

Počátkem roku 2019 bylo provedeno služební hodnocení státních zaměstnanců zařazených k výkonu služby v ÚOOÚ. Na základě těchto hodnocení bylo 28 státních zaměstnanců hodnoceno jako vynikajících a 30 jako dobrých. Žádný státní zaměstnanec nebyl hodnocen jako nevyhovující.

Do služebního poměru bylo nově přijato osm zaměstnanců a devět zaměstnanců služební poměr ukončilo. Do jiného služebního úřadu byli zařazeni nebo jmenováni tři státní zaměstnanci. Do pracovního poměru pak byli přijati dva zaměstnanci, přičemž tři zaměstnanci pracovní poměr ukončili.

V rámci Úřadem zajišťované zvláštní části úřednické zkoušky pro obor služby „ochrana osobních údajů“ bylo vyzkoušeno celkem 35 žadatelů, z nichž 31 složilo zkoušku úspěšně a čtyři byli hodnoceni jako neúspěšní.

K 1. lednu 2019 bylo v ÚOOÚ v evidenčním stavu 101 zaměstnanců, k 31. prosinci 2019 byl pak jejich počet také 101.

Průměrný evidenční přepočtený počet zaměstnanců za rok 2019 činil 102,636.

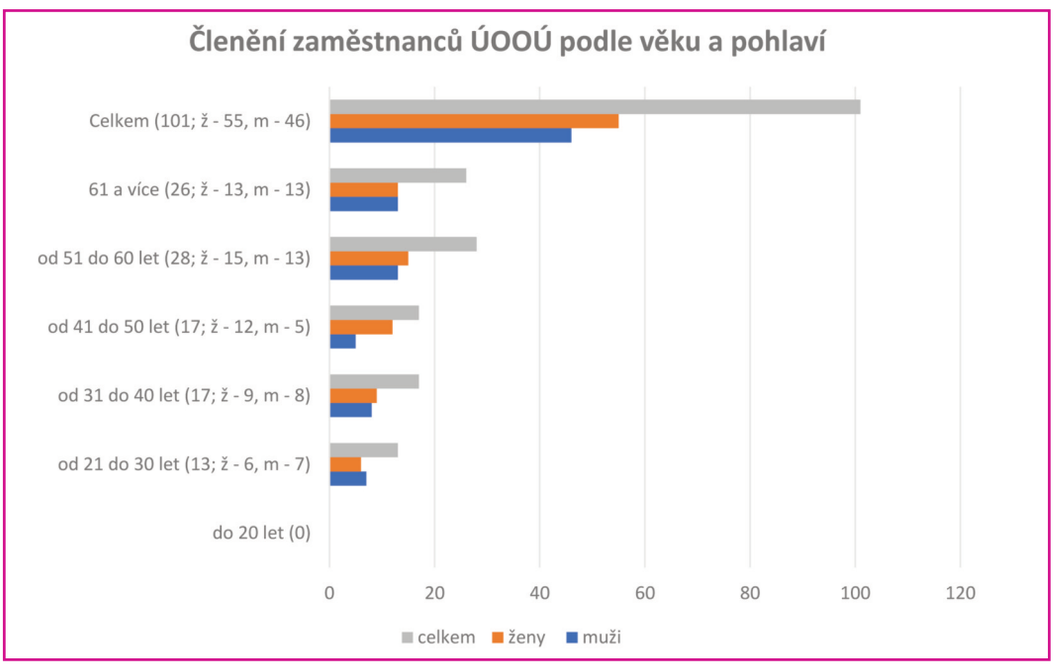
Dalších 31 osob vykonávalo v Úřadu činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr.

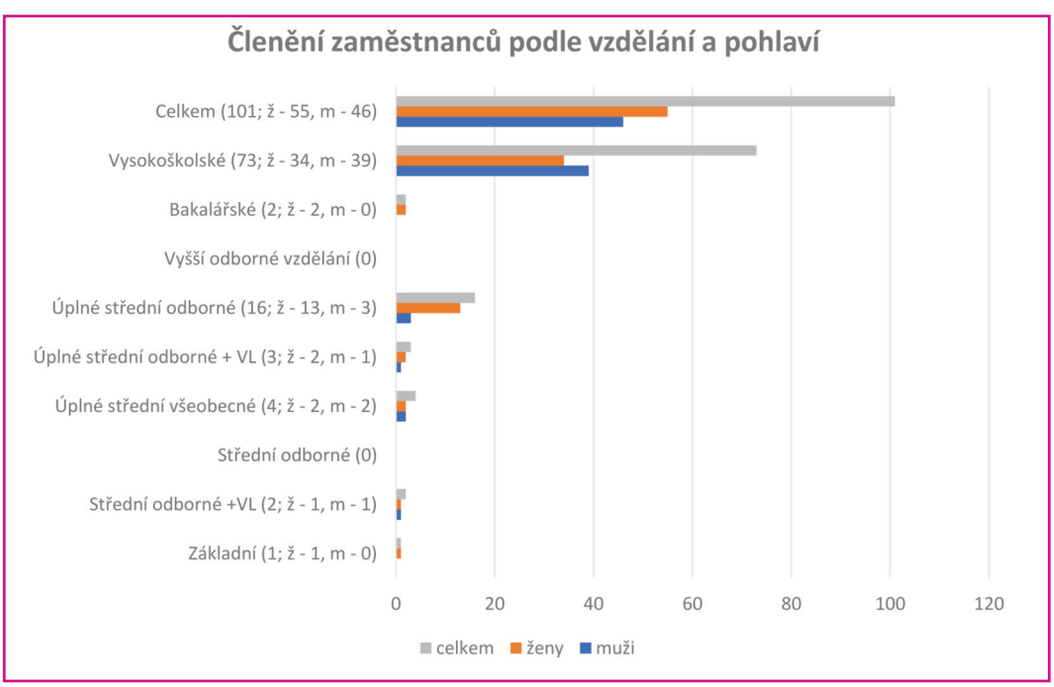
Z grafu „Členění zaměstnanců ÚOOÚ podle věku a pohlaví“ vyplývá, že v Úřadu pracují převážně zaměstnanci ve věku 50 let a výše. Tito zaměstnanci mají kromě odpovídajícího vzdělání i dlouhodobou praxi a velké zkušenosti. Řada z nich působí v Úřadu dlouhou dobu a svoje zkušenosti předávají novým zaměstnancům, 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 ÚOOÚ 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 stále více na významu. Studentům středních a vysokých škol Úřad poskytuje možnost absolvovat odbornou praxi. Tím podporuje jejich zájem o oblast ochrany osobních údajů a zároveň tak vyhledává nové potenciální zaměstnance.

Následující statistiky jsou k 31. prosinci 2019:





• HOSPODAŘENÍ

Rozpočet Úřadu byl schválen zákonem č. 336/2018 Sb., o státním rozpočtu České republiky na rok 2019.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

	v tisících Kč
Souhrnné ukazatele	
Příjmy celkem	2 398,53
Výdaje celkem	169 618,88
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	2 398,53
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	0,00
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	2 398,53
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	169 618,88
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	67 726,64
Povinné pojistné placené zaměstnavatelem*)	22 765,48
Základní příděl fondu kulturních a sociálních potřeb	1 324,29
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	13 112,93
Platy zaměstnanců na služebních místech podle zákona o státní službě	41 921,20
Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	11 180,27
Výdaje spolufinancované zcela nebo částečně 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	17 443,20

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

1. Příjmy

Příjmy pro rok 2019 nebyly schváleným rozpočtem stanoveny.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částkou 2 398,53 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, resp. podle zákona č. 110/2019 Sb., o zpracování osobních údajů a jiných zákonů,
- náhrady nákladů řízení,
- příjmy vztahující se k roku 2018 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2018).

2. Výdaje

Čerpání výdajů ve výši 169 618,88 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. základního přídělu FKSP a náhrad v době nemoci, ve výši **92 039,33** tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. prosinci 2019 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 **17 443,20 tisíc Kč**.

Přehled čerpání rozpočtu v roce 2019

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2019 v tis. Kč	Konečný rozpočet 2019 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2019 v tis. Kč	Skutečný konečný rozpočet v %
2211, 2212, 2322, 2324, 4132	Ostatní nedaňové příjmy	0,00	0,00	2 398,53	
	PŘÍJMY CELKEM	**0,00**	**0,00**	**2 398,53**	
501	Platy	65 531,78	69 445,92	66 214,39	95,33
5011	Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	12 665,27	13 212,93	13 112,93	99,24
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	39 640,11	42 721,20	41 921,20	98,13
5014	Platy zaměstanců v prac. poměru odvoz. od platů úst. činitelů	13 226,40	13 521,80	11 180,27	82,68
502	Ostatní platby za provedenou práci	1 890,91	2 056,23	1 512,25	73,54
5021	Ostatní osobní výdaje	1 890,91	2 056,23	2 512,25	73,54
503	Povin. pojist. plac. zaměstnavatelem	22 923,72	25 415,65	22 765,48	89,57
5031	Povin. pojist. na sociál. zabezpečení	16 855,67	18 774,38	16 686,71	88,88
5032	Povin. pojist. na veřej. zdrav. pojištění	6 068,04	6 641,27	6 078,77	91,53
512	Výdaje na některé úpravy hm. věcí a pořízení některých práv k hm. věcem	40,00	11,00	9,90	90,00
513	Nákup materiálu	1 115,00	1 400,25	1 262,68	90,18
514	Úroky a ost. fin. výdaje	30,00	40,00	33,21	83,02
515	Nákup vody, paliv a energie	1 580,00	1 629,54	1 580,64	97,00

516	Nákup služeb	41 532,29	54 818,07	51 333,63	93,64
517	Ostatní nákupy	2 930,50	4 149,94	2 666,91	64,26
518	Výdaje na netransfer. převody uvnitř organizace, povinnosti a jistoty	485,00	35,00	0,00	0,00
519	Výdaje souvis. s neinv. nákupy, příspěvky, náhrady a věcné dary	4 503,50	4 131,75	3 240,58	78,43
534	Převody vlastním fondům a ve vztahu k útv. bez plné práv. subjektivity	1 310,64	1 366,73	1 324,29	96,89
5342	Základní příděl FKSP a soc. fondů obcí a krajů	1 310,64	1 366,73	1 324,29	96,89
536	Ost. neinv. transf. jin. veřej. rozp. platby daní a další povinné platby	22,00	15,50	8,80	56,79
542	Náhrady plac. obyvatelstvu	200,00	228,53	222,93	97,55
5424	Náhrady v době nemoci	200,00	228,53	222,93	77,55
	Běžné výdaje celkem	**146 569,86**	**161 320,40**	**148 594,10**	**92,11**
611	Pořízení dlouh. nehmot. majetku	11 300,00	11 300,00	3 615,24	31,99
612	Pořízení dlouh. hmot. majetku	11 800,00	20 034,04	13 827,95	69,02
	Kapitálové výdaje celkem	**23 100,00**	**31 334,04**	**17 443,20**	**55,67**
	VÝDAJE CELKEM	**167 195,34**	**196 088,15**	**169 618,88**	**86,50**

Číselné údaje jsou použity z výkazů zpracovaných k 31. prosinci 2019.

INTERNÍ AUDIT

Základními právními a regulatorními normami upravujícími činnost interního auditu v roce 2019 v ÚOOÚ 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 a
- vnitřní směrnice Úřadu.

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

Roční plán interního auditu na rok 2019 byl schválen předsedkyní Úřadu 15. ledna 2019. Vycházel:

- 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 a
- z kapacitních možností interního auditu.

Interní audit na základě schváleného ročního plánu na rok 2019 realizoval celkem dva 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 možná rizika v auditovaných oblastech a jejich potenciálních dopadech.

Interní audity byly zaměřeny na prověření:

- zadávání veřejných zakázek malého rozsahu;
  Audit vyhodnotil správnost postupů u zadávání veřejných zakázek malého rozsahu podle zákona a podle vnitřních předpisů a prověřil peněžní prostředky vynaložené na nákupy v objemech do 100 000 Kč z hlediska hospodárnosti, účelnosti a efektivnosti.
- nakládání s majetkem České republiky;
  Audit vyhodnotil správnost postupů a plnění základních povinností při nakládání s majetkem České republiky na vybraném vzorku nakupovaných služeb.
  Šetřeny byly služby poštovní, služby telekomunikační a radiokomunikační, služby peněžních ústavů, nájemné, služby konzultační, právní a poradenské, služby školení a vzdělávání, zpracování dat a ostatní služby.
- funkčnosti a účinnosti vnitřního kontrolního systému;
  Audit musí prověřit, nejméně jednou ročně, účinnost vnitřního kontrolního systému na základě ustanovení § 30 odst. 7 zákona o finanční kontrole.

Výsledky auditů ukončených v roce 2019 byly projednány s vedoucími zaměstnanci auditovaných útvarů a s předsedkyní Úřadu. Svými zjištěními přinesly přidanou hodnotu k účinnějšímu fungování finančního řízení, dodržování obecně závazných právních a vnitřních předpisů, jak jsou vybrané auditované systémy nastaveny a zda jsou dostatečně funkční.

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

K zjištěním byla přijata 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 2019:

1. zajišťoval konzultační činnost a metodickou činnost především v oblasti řízení rizik, vnitřních předpisů, majetkové evidence a 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, ochranu oprávněných práv a zájmů ÚOOÚ.

ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2019 a informace o jejím předání proběhne v řádném termínu do 31. července 2020 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., resp. podle zákona č. 110/2019 Sb., o zpracování osobních údajů, nemá Úřad povinnost schvalovat účetní závěrku auditorem.

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2019
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. 110/2019 Sb.,
o zpracování osobních údajů, § 54 odst. 3 písm. a) a § 57,
zveřejnil Úřad pro ochranu osobních údajů tuto výroční zprávu
v únoru 2020 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, Andrea Sklenářová
Tisk: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno
Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, Brno, 2020

ISBN 978-80-210-9548-9