VÝROČNÍ ZPRÁVA 2020

Úřad
pro ochranu
osobních
údajů

ISBN 978-80-210-9835-0 (brožováno)
ISBN 978-80-210-9836-7 (online; pdf)

Úvodní slovo předsedy

Vážené dámy, vážení pánové,
úvodní slovo nového předsedy Úřadu pro ochranu osobních údajů k výroční zprávě by kromě zhodnocení výsledků vlastní činnosti Úřadu za rok 2020, které je třeba připsat zejména jeho předchozí předsedkyni JUDr. Ivaně Janů, jež vedla Úřad předchozích pět let do 31. srpna 2020, mělo rovněž naznačit jeho konkrétní priority pro nadcházející funkční období. Za běžných okolností by se tak bezpochyby stalo, nicméně neblahé události roku 2020 spojené s pandemií nemoci COVID-19, které zásadním způsobem zasáhly do života jednotlivých lidí, jejich rodin, společností i institucí, na počátku vytyčené priority i jejich postupné projevování se v praxi významným způsobem ovlivnily a ovlivňují.

Úřad, který oslavil 20. výročí svého vzniku, musel v loňském roce čelit novým zásadním výzvám (zejména konfliktu ochrany soukromí a ochrany veřejného zdraví v době pandemie) a zároveň procházel zásadní vnitřní proměnou související s novým organizačním a kompetenčním uspořádáním, které stanovily zákon č. 110/2019 Sb., o zpracování osobních údajů (jmenování druhého místopředsedy a vznik sekcí), a novela zákona č. 106/1999 Sb., o svobodném přístupu k informacím, která stanovila Úřadu nové a zcela ojedinělé kompetence. Uvedené bylo ještě umocněno skutečností, že bylo nezbytné upřednostnit ochranu života a zdraví zaměstnanců a jejich blízkých před lpěním na zachovávání obvyklých standardů zejména dozorové činnosti. I přes výše uvedené zůstal Úřad akceschopný.

Rok 2020 byl v českém i evropském kontextu obdobím *docenění* a popularizace ochrany osobních údajů, byť v tragickém kontextu. Pandemie COVID-19 přinesla zcela nové otázky zpracování *citlivých* osobních údajů. Bylo prověřeno obecné nařízení (GDPR) a sjednocující role Evropského sboru pro ochranu osobních údajů (EDPB). Již na jaře 2020 byly např. formulovány základní principy fungování mobilních aplikací pro *trasování* nákazy, aby bylo maximálně šetřeno soukromí osob. V českém prostředí se požadavek právního základu a nastavení rozumných mezí v zákoně dosud zcela naplnit nepodařilo. Nové výzvy pro ochranu osobních údajů představují i další chystaná opatření spojená s očkováním a uvažovaným dalším využitím informací o zdravotním stavu. Pouze stávající naléhavostí bezprostředních kroků pro ochranu zdraví a životů občanů lze snad obhájit jistou dlouhodobou neujasněnost kroků příslušných státních orgánů, kdy zákonnost a celkový zaváděný mechanismus zpracování osobních údajů v rámci prováděných opatření nejsou zvažovány na počátku a následně navíc podléhají takovým změnám, které následně znesnadňují monitoring těchto kroků.

V této souvislosti je třeba uvést, že ačkoliv Úřad měl k dispozici pouze zprostředkované informace, poskytoval maximální součinnost při hledání optimálního řešení tak naléhavé otázky veřejného zájmu, jakou je ochrana veřejného zdraví v době pandemie.

Vedle této činnosti se Úřad v loňském roce věnoval řadě témat, s nimiž se na následujících stránkách budete moci seznámit, ačkoliv byla vnější činnost Úřadu do značné míry omezena vládními opatřeními.

Pokud jde o priority pro mé funkční období, než bych neumělými slovy parafrázoval to, s čím se v roce 2015 ujímala výkonu funkce má vážená předchůdkyně JUDr. Ivana Janů, dovolím si svůj program pro nadcházející funkční období vyjádřit jejími slovy z úvodního slova k výroční zprávě za rok 2015:

„Bez soukromí, bez možnosti být alespoň někdy a někde sám a rozhodovat o tom, co o sobě ostatním řeknu a co si již nechám pro sebe, nemůže být člověk svobodným. A bez svobodných a zároveň za svůj život a své skutky odpovědných lidí nemůže existovat ani svobodná a spravedlivá společnost".

„Úřad … proto, aby plnil svoji roli, musí být důsledný, přesvědčivý a srozumitelný jak při kontrole nebo řízení o porušení zákona, tak i při formulování a prosazování připomínek k návrhům nových právních předpisů. Stejně tak je důležitá jeho role jako konzultačního orgánu pro odbornou i širokou veřejnost…"

A konečně: *„Úřad pro ochranu osobních údajů… může a musí hrát pro občana důležitou roli, ta však nemůže být úplná bez spolupráce těch, kterým osud jejich soukromí není lhostejný. A to bychom měli být my všichni!"*

Pokud lze definovat něco, v čem bych rád změnil vnější činnost Úřadu, tak je to kladení většího důrazu na jeho účast v legislativním procesu, na metodickou činnost a spolupráci s územní samosprávou, zejména s obcemi. Již v loňském roce se nám v těchto oblastech podařilo dosáhnout jistých drobných úspěchů. Jako příklady způsobu, jakým bychom chtěli aktivněji působit, lze uvést úpravu Centrálního registru oznámení podle zákona o střetu zájmů tak, aby majetkové poměry veřejných funkcionářů, kterými jsou představitelé územních samosprávných celků, nebyly volně a nekontrolovaně přístupné komukoliv na internetu. Ačkoliv v té době ještě nenabyl účinků nález Ústavního soudu, který by tak učinil závazně, vyšlo Ministerstvo spravedlnosti našim obavám, vycházejícím z podnětu Sdružení místních samospráv, vstříc.

V legislativní oblasti jsme se kromě reakcí na často z hlediska ochrany soukromí nedořešenou „covidovou legislativu" zaměřili i na jiné legislativní návrhy, pokud jsme v nich viděli potenciální rizika pro ochranu soukromí nebo nesoulad s pravidly zpracování osobních údajů. Naší snahou do budoucna bude, aby se Úřad neprofiloval jen jako někdo, kdo říká, že nějaký legislativní návrh porušuje stanovená pravidla, ale aby, pokud je to možné a úprava je věcně odůvodněná, pomáhal s formulací legislativního řešení v tom smyslu, aby zásah do soukromí občanů byl co možná nejmenší při respektování potřeby dosažení legislativního cíle vytčeného navrhovatelem konkrétní právní úpravy. Jako příklad lze uvést, že Úřad byl osloven s žádostí o stanovisko ohledně povinnosti exekutora plošně nahrávat telefonní hovory; naše stanovisko formulovalo záruky ochrany osobních údajů: zabezpečení nahrávek před neoprávněným přístupem, omezení oprávnění na přístup, ochranu soukromí třetích osob a zákonné stanovení konkrétní přiměřené doby uchování záznamů.

Úřad je také třeba za účelem realizace uvedených priorit co nejvíce otevřít. Vést dialog s našimi partnery, s odbornou veřejností, s těmi, kdo data ostatních zpracovávají, stejně jako s těmi, jejichž data jsou zpracovávána.

Nemohu na tomto místě nyní pominout, že mimořádným počinem Úřadu bylo v loňském roce uložení pokuty 6 000 000 Kč za rozesílání tzv. nevyžádaných obchodních sdělení. Naším cílem je individuální, a především generální prevence. Nejen výše hrozící sankce, ale především její neodvratnost by měly pomoci kultivovat prostředí v této oblasti. Nevyžádaná obchodní sdělení přestanou být problémem v okamžiku, kdy se podstatné části těch, kteří je rozesílají, přestanou vyplácet.

Netřeba zdůrazňovat, že po účinnosti obecného nařízení již nelze evropskou spolupráci pojímat jako volitelnou součást *vnějších vztahů*, nýbrž jako každodenní kmenovou a zřejmě i rozhodující agendu Úřadu. Dozorové úřady členských států tvoří pevnou strukturu se vzájemným vlivem na své rozhodování, a to zejména prostřednictvím EDPB.

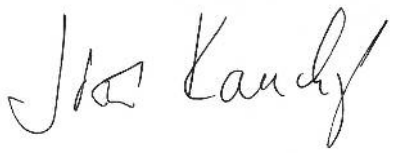
Podstatnou změnu pro Úřad přinesla v loňském roce také zcela nová a originální zákonná kompetence v oblasti svobodného přístupu k informacím. Přestože dobrý úmysl zákonodárce sjednotit rozhodovací praxi v České republice prostřednictvím přezkumného (a částečně i odvolacího) řízení vedeného Úřadem nebyl zcela provázán s dostatečným personálním a rozpočtovým zajištěním, shledáte z příslušné kapitoly, že Úřad se svých povinností ujal od počátku v plném rozsahu a efektivně.

Personální obsazení vedení bylo dokončeno, když na základě volby Parlamentu ČR uskutečněné na můj návrh v prosinci roku 2020 vedení Úřadu doplnil s nástupem od 1. ledna 2021 Mgr. Petr Jäger, Ph.D., jakožto druhý ze zákonem předvídaných místopředsedů Úřadu.

S ohledem na nelehký rok 2020 považuji za nutné upřímně poděkovat všem zaměstnancům, kteří bez ohledu na ztížené podmínky zodpovědně plnili své pracovní povinnosti, a to nejen ve všech třech pilířích činnosti Úřadu, tedy ve věcech týkajících se ochrany osobních údajů, svobodného přístupu k informacím a provozování kritického informačního systému poskytujícího základní a agendové identifikátory fyzických osob, ale i v dalších souvisejících činnostech, a bez jejichž obětavosti by se mj. nepodařilo bránit nedotknutelné hranice soukromí nás všech.

Vážené dámy, vážení pánové,

při úvahách o smyslu práva na soukromí připomínám, že celý koncept základních práv byl vytvořen jako ochrana jednotlivce před zvůlí státní moci. Historicky je to právě stát, který byl, je a bude náchylný ke zneužití svého mocenského aparátu, k invazi do soukromí obyvatel a podle potřeby k nátlaku, šikaně či přímo persekuci. S rozvojem technologií a jejich *průběžným* a *nepřetržitým* využíváním své osobní údaje předáváme dalším, zpravidla nestátním aktérům. Historickou úlohou ochránců osobních údajů není technologický rozvoj zastavit, nýbrž nastavit takové mantinely pro správce osobních údajů, aby poučené a vědomé rozhodování o vlastním soukromí zůstávalo nadále v rukou občanů.



předseda Úřadu pro ochranu osobních údajů

Obsah

Úřad v číslech 2020

Dotazy a konzultace	celkový počet písemných dotazů	1571
	počet vyřízených hovorů v rámci konzultační GDPR linky	1351
	předchozí konzultace ve smyslu čl. 36 obecného nařízení	0
Podání a stížnosti	přijaté podněty	1855
	vyřízeno upozorněním správce na možné porušení	452
	předáno ke kontrole nebo jinému řízení	125
	ohlášení porušení zabezpečení osobních údajů ve smyslu čl. 33 obecného nařízení poskytnutí	292
	vyřízeno součinnosti orgánům činným v trestním řízení	14
	jiným způsobem	1278
Kontrolní činnost (vyjma kontrol týkajících se obchodních sdělení)	zahájeno	54
	ukončeno	48
	z toho z předchozích let	16
	uložená opatření k nápravě	8
	napadeno námitkami	8
	námitkám vyhověno	1
	nevyhověno	4
	částečně vyhověno	1
	pokuty za neposkytnutí součinnosti v kontrole	5
Obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	3031
	zahájených kontrol	15
	ukončených kontrol	8
	z toho z předchozích let	1
	napadeno námitkami	-
	námitkám vyhověno	-
	nevyhověno	-
	částečně vyhověno	-
	řízení o sankci	20
	pokuty za neposkytnutí součinnosti v kontrole	15
	vyřízeno bez zahájení kontroly upozorněním subjektu na možné porušení povinností	402
Správní trestání (s výjimkou řízení týkajících se nevyžádaných obchodních sdělení)	řízení o sankci vedená s právnickými osobami a fyzickými osobami podnikajícími	46
	řízení o sankci s fyzickými osobami	5
	upuštění od uložení pokuty podle § 65 zákona č. 110/2019 Sb.	27
	napomenutí	4
	upuštěno od uložení správního trestu z důvodu nemožnosti trestání orgánů veřejné moci a veřejných subjektů	3

Rozhodování předsedy Úřadu	rozklady napadená rozhodnutí	18
	zamítnutých rozkladů	13
	zrušeno a vráceno k novému projednání	-
	zrušených rozhodnutí a zastaveno řízení	-
	změna rozhodnutí	1
Soudní přezkum (Pozn.: **celkem od r. 2001*)	podaných žalob k soudu	5 (*170)
	zamítnutých žalob soudem (z toho zastavených řízení)	11 (4)
	zrušených rozhodnutí soudem	1
	ukončených/neukončených soudních řízení od roku 2001	155/15
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí	-
	rozhodnutí o povolení předávání	-
	rozhodnutí o nepovolení	-
	zastavená řízení z procesních důvodů	-
Stížnosti podle § 175 správního řádu	přijatých stížností podle § 175	53
	z toho stížností podle § 175 odst. 1	38
	z toho žádostí podle § 175 odst. 7	15
	vyřízených podání podle § 175	57
	z toho stížností podle § 175 odst. 1	40
	z toho žádostí podle § 175 odst. 7	17
	ze všech vyřízených podání posouzeno jako	
	stížnosti důvodné	1
	stížnosti částečně důvodné	4
	žádosti důvodné	-
	žádosti částečně důvodné	1
	nedůvodných	51
	nevyřízeno	2
Podání dle zákona č. 106/1999 Sb.	podání dle § 16b (nečinnost nadřízeného orgánu, přezkum)	215
	podání dle § 20 odst. 5 (odvolání, stížnosti)	312
	z celkového počtu 527 podání vyřízeno	508
Žádosti podle zákona o svobodném přístupu k informacím	přijatých žádostí	99
	zcela vyhověno	88
	částečně odmítnuto	8
	zcela odmítnuto	3
Připomínkované návrhy	věcné záměry zákonů	1
	zákony	61
	prováděcí předpisy	56
	návrhy nařízení vlády	15
	návrhy vyhlášek	41
	nelegislativní dokumenty	32

Dozorová činnost

KONTROLNÍ ČINNOST

Dozorové a kontrolní postupy dle zákona o kontrole (kontrolní řád) byly v roce 2020 poznamenány situací a opatřeními souvisejícími s pandemií COVID-19 zejména v průběhu jarního a podzimního období. Fakticky to znamenalo utlumení určitých forem dozoru, které se zejména týkalo jak zahajování a provádění některých kontrolních úkonů, například místních šetření, tak v prodlužování lhůt pro úkony, mj. s přihlédnutím k situaci, v níž se nacházely kontrolované osoby. Úřad v roce 2020 přesto zahájil 54 a ukončil 48 kontrol v oblasti zpracování osobních údajů dle obecného nařízení.[1]

Kontroly byly uskutečňovány tradičně na základě kontrolního plánu (28), na základě důvodných skutečností, vyplývajících z podnětů a stížností (24), které Úřad obdržel, a také na základě ohlášení porušení zabezpečení osobních údajů (2).

Ve dvou případech tvořily podklady (stížnosti) pro zahájení kontroly též informace ze Systému pro výměnu informací o vnitřním trhu, což je online systém provozovaný Evropskou komisí mimo jiné i pro usnadnění spolupráce mezi jednotlivými dozorovými úřady.

Mezi nejčastěji zjištěná porušení v rámci kontrolní činnosti v roce 2020 patřila také absence řádného právního důvodu pro uskutečňované zpracování ze strany správce osobních údajů. V řadě případů bylo kontrolami také zjištěno porušení výkonu práv subjektu údajů.

V případech, kdy kontrolovaná osoba nenapravila zjištěné nedostatky ještě v průběhu kontroly, byla ukládána nápravná opatření. Těch Úřad uložil jen v oblasti zpracování osobních údajů dle obecného nařízení v roce 2020 osm.

I v roce 2020 se Úřad setkával při vykonu kontrolní činnosti s nespolupracujícími subjekty, které odmítaly poskytnout základní součinnost, a proto muselo být přistoupeno k ukládání pořádkových pokut dle zákona č. 255/2012 Sb., o kontrole. Úřad je uložil v pěti případech v celkové výši 1 323 000 Kč.

[1] Tyto druhy kontrol nejsou jediné, které Úřad provádí. Významnou agendu tvoří v tomto směru také kontrolní činnost podle zákona o některých službách informační společnosti a o změně některých zákonů. Jejím výsledkům se věnuje samostatná kapitola „Dozorová činnost v oblasti šíření obchodních sdělení“ na straně 25.

KONTROLNÍ PLÁN

Do kontrolního plánu pro rok 2020 bylo zařazeno celkem 29 kontrol. Při jeho koncipování byly tradičně využity poznatky z podnětové a stížnostní agendy, ale zároveň také poznatky získané dozorovou činností v podobě kontrol, správních řízení nebo informací z médií. Zahrnuty byly jak veřejnoprávní, tak soukromoprávní subjekty.

Vyjma na závěrečné čtvrtletí roku 2020 plánované kontroly Ústavu zdravotnických informací a statistiky, která byla z důvodu zapojení značné kapacity tohoto ústavu do boje proti pandemii koronaviru zatím odložena, byly všechny ostatní plánované kontroly zahájeny a 19 jich bylo také ukončeno. Součástí kontrolního plánu pro rok 2020 byly i tři kontroly v oblasti šíření obchodních sdělení, přičemž ve dvou se Úřad zaměřil na kontrolu subjektů, které se často vyskytovaly v tzv. spamových pastích.

Ucelenou část tvořilo osm kontrol zpracování osobních údajů prostřednictvím cookies provozovateli mediálně významných internetových stránek či vyhledavačů v České republice. Bylo vybráno šest soukromých provozovatelů, Česká televize a Český rozhlas. Kontroly se zaměřily především na správnou identifikaci účelu a nastavení právního důvodu zpracování osobních údajů při využívání cookies, včetně splnění podmínek pro předávání osobních údajů do zahraničí a plnění práv subjektů údajů.

Těmito kontrolami bylo zjištěno, že některé subjekty přistupovaly k problematice zajištění souladu využívání cookies s právními předpisy liknavě. Neměly například při jejich využívání dostatečně ujasněno, jaké druhy využívají, za jakým účelem a zdali jsou či nejsou informace zpřístupňovány i třetím stranám. Mnohdy si také nebyly vědomy skutečnosti, že na zpracování osobních údajů prostřednictvím cookies dopadá nejen informační povinnost a případné zajištění souhlasu s jejich využitím, ale i další související povinnosti, například při předávání osobních údajů do zahraničí jiným subjektům. Úřad však v rámci těchto kontrol, a z nich vyvozovaných závěrů, výrazně přihlížel ke skutečnosti, že v České republice neexistuje ucelená právní úprava využívání osobních údajů uživatelů internetu v tzv. cookies.

Významnou část kontrolního plánu tvořily kontroly soukromých subjektů, u kterých Úřad ověřoval plnění povinností například i ve vztahu k plnění práv subjektů údajů, jakožto jednoho ze základních pilířů, na kterém je evropská úprava zpracování osobních údajů postavena. Jednalo se o dva poskytovatele nebankovních drobných půjček a dva prodejce energií a dalších služeb. V rámci této oblasti Úřad provedl také kontrolu u poskytovatele nebankovních úvěrů ve vztahu k pořizování a uchovávání kopií občanských průkazů. Jedna z kontrol skončila bez zjištěného porušení obecného nařízení, druhá stále probíhá.

Ve veřejnoprávní oblasti provedl Úřad kontroly dvou škol se zaměřením na dodržování zásad zpracování osobních údajů, zabezpečení osobních údajů a rolí dodavatelů informačních služeb. Nadto kontroloval i jedno školské zařízení zařazené do projektu Bezpečná škola v Karlovarském kraji. Vše bez zjištěného porušení obecného nařízení.

Kontrolována byla též Pražská správa sociálního zabezpečení, kde se Úřad zaměřil na role dodavatelů a s tím spojených povinností správce. Ani v tomto případě kontrolující porušení obecného nařízení nezjistili.

Tradičně se Úřad při kontrolní činnosti na základě plánu kontrol věnoval také oblasti zdravotnictví. Zkontroloval plnění povinností při zpracování osobních údajů a jejich zabezpečení prostřednictvím programu pro vedení zdravotnické dokumentace lékaři či prověřil zabezpečení osobních údajů v elektronické a listinné podobě provozovatelem ambulancí.

POZNATKY Z KONTROLNÍ ČINNOSTI

Inspektorka Jana Rybínová

Vynucený souhlas se zpracováním osobních údajů ve spolku chovatelů psů

Kontrola byla zahájena na základě podnětu, který směřoval proti spolku chovatelů psů.

Stěžovatelka uvedla, že byla spolkem pod pohrůžkou vyloučení donucena k podepsání souhlasu se zpracováním osobních údajů. Domáhala se ukončení zpracování svých osobních údajů, vyjma zpracování, jež spolek provádí v souvislosti s evidencí chovu psů v chovné stanici, ve které za chov psů zodpovídá.

Kontrolou bylo zjištěno, že spolek jako správce osobních údajů členů porušil obecné nařízení, neboť nezpracovával osobní údaje za účely nezbytnými pro naplnění určitých článků stanov spolku (účel, cíl činnosti) na základě nesprávného právního titulu. Právním titulem pro toto zpracování je nezbytnost pro účely oprávněných zájmů spolku, včetně zájmů Českomoravské kynologické unie, přičemž oprávněnost zpracování osobních údajů žadatelů o členství, včetně žadatelů o zajištění služeb – nečlenů, je dána souhlasem s podmínkami stanov ve smyslu § 223 zákona č. 89/2012 Sb., občanský zákoník, tedy ve smyslu čl. 6 odst. 1 písm. b) obecného nařízení.

Spolek také porušil povinnost dle čl. 6 odst. 1 obecného nařízení. Daný souhlas totiž neměl náležitosti dle čl. 4 odst. 11 obecného nařízení, protože byl vynucený pod podmínkou nepřijetí za člena, resp. poskytnutí služeb nečlenovi. Nebyl tedy udělen svobodně na základě konkrétní a přesné informace o zpracování osobních údajů.

Zároveň byla porušena další povinnost správce osobních údajů dle obecného nařízení. Spolek totiž nepodal jak stěžovatelce, tak ani ostatním členům i nečlenům přesné informace o účelech zpracování jejich osobních údajů. Zároveň podal nesprávné informace o právním titulu pro zpracování osobních údajů členů i nečlenů a konkrétně stěžovatelce nepřesnou a nesprávnou informaci o zpracování jejích osobních údajů a nepravdivou informaci o jejich likvidaci.

Odhaleno bylo také provinění proti čl. 30 obecného nařízení, neboť spolek neměl vypracovány žádné vnitřní dokumenty o zpracování osobních údajů. Tím porušil povinnost dle čl. 24 odst. 1 obecného nařízení. Důsledkem neexistence takových opatření bylo neoprávněné zveřejnění osobních údajů stěžovatelky v rozporu s čl. 32 obecného nařízení.

Spolek proti všem zjištěním uvedeným v protokolu o kontrole podal námitky, které byly předsedkyní Úřadu zamítnuty.

Vzhledem k tomu, že zásah do soukromí stěžovatelky nedosahoval většího rozsahu, spolek jednal v dobré víře a také přijal opatření k nápravě závadného stavu, nebylo důvodné zahájit řízení podle zákona o zpracování osobních údajů, tj. řízení o uložení opatření k odstranění zjištěných nedostatků.

Zpracování osobních údajů v CÚeR Státního ústavu pro kontrolu léčiv (SÚKL)

Kontrola se zaměřila na dodržování povinností stanovených obecným nařízením v souvislosti se zpracováním osobních údajů v Centrálním úložišti elektronických receptů (dále jen „CÚeR"), vedeného podle zákona o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), a to v návaznosti na zavedení povinnosti vydávat elektronické recepty (od 1. ledna 2018) a s tím související rozsáhlé zpracování osobních údajů, zejména kontrola zabezpečení osobních údajů při tomto zpracování.

Kontrola se zde zaměřila na kontrolní mechanismy odhalující neoprávněné přístupy do CÚeR. V několika případech bylo zjištěno přímo SÚKL, že výdej receptů provádí neoprávněná osoba. Kontrola byla ukončena 6. dubna 2020. V důsledku detekce neoprávněného přístupu do CÚeR v ní bylo zjištěno porušení důvěrnosti osobních údajů zvláštní kategorie.

K nejzávažnějšímu incidentu došlo v případě lékárnice, která své přístupové údaje, včetně přístupového hesla do softwarové aplikace Pilulka.cz, rozeslala k širokému použití uživatelům aplikace. V důsledku toho se mohl kdokoli znalý kódu receptu dostat k jeho elektronickému záznamu v CÚeR. Přesný rozsah zneužití nebylo možné vyčíslit, neboť v transakčních lozích jsou evidována všechna přihlášení pod jedním účtem. Počet přístupů pod tímto účtem činil 327 556.

SÚKL účet lékárnice zablokoval a incident byl rovněž nahlášen Národnímu úřadu pro kybernetickou a informační bezpečnost.

Na základě výše uvedeného zjištění kontrola mimo jiné konstatovala, že SÚKL, jako správce osobních údajů, nemá žádnou možnost systémově zabránit zneužívání přístupových práv, jež byly v souladu s právními předpisy předány oprávněným fyzickým osobám, které splňují veškeré podmínky dle zákona o léčivech.

Současně je nezbytné doplnit, že hlavní architekt eGovernmentu se k žádosti SÚKL o stanovisko k plánované strategii informačních technologií vyjádřil kladně.

Kontrolující konstatovali, že SÚKL neměl od nabytí účinnosti změnového zákona č. 262/2019 Sb., tedy k 1. prosinci 2019, povinnost zajistit přístup oprávněných osob do IS eRecept ve smyslu stanovení dvou- nebo vícefaktorového zabezpečení, dle předpisů v oblasti kybernetické bezpečnosti. Současně s ohledem na povinnost SÚKL, která mu vznikla dnem 21. května 2018, v souvislosti s nabytím účinnosti vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, lze konstatovat, že ve smyslu § 12 této vyhlášky, byl SÚKL, jako povinná osoba v rámci řízení přístupu k informačnímu a komunikačnímu systému, pověřen, aby prováděl pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových rolí.

V této souvislosti bylo rovněž nutné, aby uživatelé při používání privátních autentizačních informací dodržovali stanovené postupy a současně aby SÚKL jako správce osobních údajů s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob přijal dostatečná vhodná technická a organizační opatření. Měl tedy zajistit úroveň zabezpečení odpovídající danému riziku, ve smyslu čl. 32 odst. 1 obecného nařízení, a to s ohledem na rizika, která zpracování představuje. V tomto případě se jedná především o náhodné nebo protiprávní zpřístupnění uložených osobních údajů, resp. v daném případě osobních údajů zvláštní kategorie, kterými jsou osobní údaje zpracovávané v rámci eReceptu.

Význam zacházení s léčivy oprávněnou osobou v souvislosti s výdejem léčivých přípravků je přitom konkrétně upraven v § 81a odst. 7 zákona o léčivech. Tato část obsahuje povinnost, dle které *„informace, k nimž v systému eRecept mají přístup lékaři a farmaceuti prostřednictvím informačních systémů, které využívají, lze využívat pouze v rámci poskytování zdravotních služeb. Jiné využití těchto údajů nebo jejich zpřístupnění třetím osobám je zakázáno"*. Porušení tohoto ustanovení je kvalifikováno jako přestupek ve smyslu § 108 odst. 1 písm. l) zákona o léčivech, dle kterého se *„fyzická osoba dopustí přestupku tím, že jako lékař nebo farmaceut v rozporu s § 81a odst. 7 zpřístupní nebo předá údaje obsažené v jeho informačním systému třetí osobě"*, přičemž předání přístupových práv, tedy jména, hesla a certifikátu, takovými údaji jsou.

Dle zákona o léčivech *„za přestupek lze uložit pokutu do 20 mil. Kč, jde-li o přestupek podle odst. 12 písm. a) až c), g), j) nebo l)"*. Dle novely zákona o léčivech, která vstoupila v účinnost dne 1. prosince 2019, však tyto druhy přestupků projednává SÚKL.

Kontrola rovněž konstatovala, že v rámci posouzení vyhodnocování rizik, významu neoprávněného nahlížení do CÚeR ve smyslu obecného nařízení, bylo nezbytné vyhodnotit, že při předávání přístupových práv jednotlivými oprávněnými pracovníky došlo kromě incidentu u provozovatele prodejní aplikace Pilulka.cz k předání v rámci konkrétního zdravotnického zařízení, a to za účelem vydání léčiva vydaného na základě eReceptu, a ne za účelem nahlížení na osobní údaje pacientů.

Závěr kontroly konstatoval, že v případě zpracování osobních údajů a osobních údajů vypovídajících o zdravotním stavu pacientů v CÚeR prostřednictvím IS eRecept jsou porušovány povinnosti dle obecného nařízení, protože i s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob docházelo k narušení jejich bezpečnosti.

Inspektorka Božena Čajková

Zpracování osobních údajů kamerami společností provozující internetovou televizi

Předmětem incidenční kontroly bylo dodržování povinností stanovených obecným nařízením a zákonem o zpracování osobních údajů v souvislosti se zpracováním osobních údajů kamerami, se zaměřením na provoz kamery instalované na budově radnice Městské části Praha 5 – Řeporyje a kamery snímající okolí památníku vlasovcům na křižovatce ulic K Třebonicům a Smíchovská.

Na budově radnice Městské části Praha 5 – Řeporyje byla instalována stacionární kamera, jejímž prostřednictvím byl kontinuálně monitorován veřejný prostor, přičemž výstup z tohoto systému byl přenášen a nepřetržitě vysílán internetovou televizí. Na webových stránkách společnosti se nacházelo také živé vysílání z kamery instalované na křižovatce ulic K Třebonicům a Smíchovská. V tomto případě kamera kontinuálně zabírala veřejný prostor v okolí památníku vlasovcům.

Společnost zpracovávala osobní údaje ze záznamu dvou stacionárních kamer, které kontinuálně zabíraly veřejné prostranství a jejichž záznam byl v reálném čase zveřejňován na internetové televizi. Záznam z těchto kamer byl pořizován v takovém rozlišení, že procházející osoby a projíždějící vozidla byly jednoznačně identifikovatelné. Takové zpracování může nepřiměřeným způsobem zasahovat do soukromí, práv a svobod těchto osob, zejména pak pokud se v daném veřejném prostoru musí pohybovat každý den. Takové zpracování překračuje rámec „novinářské licence", jelikož jej není možné považovat za přiměřené, jak je požadováno v obecném nařízení.

Jedním z hlavních projevů zásady zákonnosti v obecném nařízení je, že správce může osobní údaje zpracovávat pouze v případě, že k tomu má alespoň jeden z právních titulů, které jsou zde stanoveny. Zpracování je zákonné, *„pokud je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě"*.

Oprávněný zájem je jeden z nejflexibilnějších právních titulů. Pokud lze nějaký zájem správce považovat za oprávněný a za účelem dosažení tohoto zájmu je nezbytné zpracovávat osobní údaje, může tak správce činit. Osobní údaje však zpracovávat nemůže, pokud nad oprávněným zájmem v daném případě zpracování převáží zájmy nebo základní práva a svobody subjektů údajů, jejichž osobní údaje mají být zpracovány.

Jak je výše uvedeno, pořizování kontinuálního záznamu z veřejného prostranství a jeho zveřejnění na internetové televizi zasahuje nepřiměřeným způsobem do práv a svobod subjektů, jejichž osobní údaje jsou takto zpracovávány. V tomto případě není možné považovat zájem na ochraně památníku vlasovcům v Řeporyjích nebo bezpečnosti na vlakovém přejezdu v Řeporyjích za přednostní před ochranou základních práv a svobod subjektů, jejichž osobní údaje byly takto provozovanou kamerou zpracovávány.

Kontrolující vyhodnotili zjištěný stav tak, že společnost zpracovávala osobní údaje subjektů, zachycených na záznamu z kamery instalované na budově radnice Městské části Praha 5 – Řeporyje a kamery instalované na křižovatce ulic K Třebonicům a Smíchovská, bez právního titulu k tomuto zpracování.

Kontrolovaná osoba se tímto jednáním dopustila porušení obecného nařízení, na základě čehož jí byla uložena pokuta ve výši 70 000 Kč.

Inspektor Daniel Rovan

Ověření souladu zpracování osobních údajů dle obecného nařízení prostřednictvím kamerového systému

Kontrola byla zahájena na základě kontrolního plánu pro rok 2020. Předmětem kontroly bylo ověření souladu zpracování osobních údajů dle obecného nařízení prostřednictvím kamerového systému při zajišťování bezpečnosti návštěvníků stadionu, včetně případného využívání biometrických údajů.

Kontrolovaná osoba (prvoligový fotbalový klub) zpracovává prostřednictvím kamerového systému osobní údaje návštěvníků stadionu v podobě obrazových (např. fotografie, video), audiovizuálních či audiozáznamů, ale i údaje o využití permanentní vstupenky v případě, že je návštěvník jejím majitelem.

Provedená kontrola zjistila, že společnost zpracovává osobní údaje prostřednictvím dvou kamerových systémů. Na tomto místě určila účely zpracování osobních údajů (ochrana majetku správce a ochrana života a zdraví osob pohybujících se ve sledovaném prostoru, určení, výkon nebo obhajoba právních nároků správce, předcházení a odhalování protiprávní činnosti, porušování uděleného zákazu vstupu a porušování návštěvního řádu, doložení výše uvedených závadných jednání subjektu údajů). Zpracování a využívání biometrických osobních údajů nebylo prokázáno.

Kontrolovaná osoba zároveň přijala řadu technicko-organizačních opatření, včetně interního předpisu upravujícího provoz kamerového systému, a má zpracován záznam o činnosti zpracování a posouzení vlivu na ochranu osobních údajů pro kamerový systém (DPIA). Provádí také pravidelná školení zaměstnanců a na provoz kamerových systémů má uzavřenou smlouvu se zpracovatelem.

Kontrola v tomto případě nezjistila porušení povinností vyplývajících z obecného nařízení.

Zpracování osobních údajů v souvislosti s ransomware útokem na část počítačové sítě vysoké školy

Kontrola byla provedena na základě oznámení incidentu ve stravovacím informačním systému kontrolované osoby.

Předmětem kontroly bylo dodržování povinností při zpracování osobních údajů stanovených obecným nařízením a zákonem o zpracování osobních údajů v souvislosti s ransomwarovým útokem na část počítačové sítě kontrolované osoby, ve které její Správa kolejí a menz provozuje stravovací informační systém Kredit.

Kontrola potvrdila, že osobní údaje nebyly zpracovávány způsobem, který by zajistil jejich náležité zabezpečení, včetně jejich ochrany pomocí vhodných technických a organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Ač kontrolovaná osoba přijala technická a organizační opatření, aby zajistila úroveň zabezpečení odpovídající danému riziku, stejně jako zavedla vysokou úroveň záruk zpracování a minimalizace rizik negativních dopadů do práv a svobod subjektů (např. provádí proškolení odpovědných pracovníků v oblasti ochrany osobních údajů, aktualizaci záznamů o činnostech zpracování, stanovení pravidel pro řízení přístupu k osobním údajům, logy), stejně došlo k ransomwarovému útoku na část její počítačové sítě.

Při posuzování vhodné úrovně zabezpečení nebyla pravděpodobně prověřena všechna možná rizika, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Tím došlo ze strany kontrolované osoby k porušení obecného nařízení. S ohledem na skutečnost, že u kontrolované osoby došlo po ransomwarovém útoku k přijetí opatření k odstranění nedostatků, byl zjištěný protiprávní stav napraven.

V návaznosti na výše uvedené proto nebylo zahájení řízení o uložení opatření k odstranění zjištěných nedostatků důvodné, neboť účelu, jehož by bylo možné dosáhnout provedením řízení o přestupku, bylo již dosaženo.

Inspektorka Jiřina Rippelová

Zpracování osobních údajů žáků školským zařízením v elektronickém informačním systému BAKALÁŘI

Úřad provedl v roce 2020 na základě kontrolního plánu kontrolu dodržování zásad zpracování osobních údajů žáků školským zařízením v elektronickém informačním systému BAKALÁŘI. Kontrolovaným subjektem byla základní škola v Praze.

Kontrolující prověřovali dodržování zásad zákonnosti a transparentnosti při výkonu práv subjektů údajů a při zpracování osobních údajů subjektů údajů. Ty kontrolovaná osoba jakožto správce zpracovává v informačním systému BAKALÁŘI a jeho jednotlivých aplikacích včetně kontroly zabezpečení osobních údajů a rolí dodavatelů informačních služeb a s tím spojených povinností správce dle obecného nařízení.

Kontrola se nejprve zaměřila na vyhodnocení informací, které kontrolovaná osoba o subjektech údajů zpracovává v informačních systémech BAKALÁŘI. Zde bylo konstatováno, že se jedná o osobní údaje a kontrolovaná osoba je v postavení správce osobních údajů.

Kontrolující dále hodnotili roli zpracovatele a obsah uzavřené zpracovatelské smlouvy. Podle jejich závěrů zpracovatelská smlouva odpovídá všem požadavkům, které stanoví čl. 28 odst. 3 obecného nařízení.

Posuzována byla i zákonnost zpracování osobních údajů zpracovávaných v informačním systému BAKALÁŘI, tedy právní titul zpracování. Výsledkem bylo, že právním titulem zpracování je školský zákon č. 561/2004 Sb.

Kontrola se dále zabývala plněním informační povinnosti. Bylo konstatováno, že kontrolovaná osoba přijala vhodná opatření, aby poskytla subjektům údajů veškeré informace stručným, srozumitelným, transparentním a snadno přístupným způsobem. Kontrolovaná osoba rovněž plní svou povinnost vést záznamy o činnostech zpracování osobních údajů ve smyslu čl. 30 obecného nařízení.

V neposlední řadě se kontrola podrobně věnovala zabezpečení osobních údajů a plnění povinností stanovených v čl. 32 obecného nařízení. Ani zde nebylo konstatováno porušení plnění povinností. Na závěr bylo rovněž konstatováno, že kontrolovaná osoba splnila svou povinnost jmenovat pověřence pro ochranu osobních údajů.

V žádném z osmi kontrolních zjištění nebylo konstatováno porušení obecného nařízení.

Zpracování osobních údajů současných i potenciálních zákazníků společností nabízející provedení energetických aukcí

Předmětem kontroly dle kontrolního plánu bylo ověření dodržování zásad zákonnosti a transparentnosti a postupů při zpracování osobních údajů subjektů údajů shromážděných při realizaci nabízených energetických aukcí. Dále plnění informační povinnosti, zabezpečení osobních údajů a s tím souvisejících povinností správce dle obecného nařízení, a to zejména v rozsahu odpovídajících povinností podle čl. 5, čl. 6, čl. 12 až 23, čl. 25, čl. 28 až 32 a čl. 37 obecného nařízení.

Bylo zjištěno, že kontrolovaná osoba se nachází v postavení správce osobních údajů, přičemž právním titulem pro zpracování osobních údajů zákazníků a potencionálních zákazníků je primárně smlouva ve smyslu zákona č. 89/2012 Sb., občanský zákoník. Zpracování osobních údajů je nezbytné pro plnění smluv mezi kontrolovanou osobou a jejími zákazníky ve smyslu čl. 6 odst. 1 písm. b) obecného nařízení.

Dalším právním titulem zpracování osobních údajů je čl. 6 odst. 1 písm. c) obecného nařízení, kdy ke zpracování dochází rovněž v případě, kdy je nezbytné pro plnění právní povinnosti správce (oblast vedení správy daní, vedení účetnictví, mzdové povinnosti, toto zpracování se však netýká zpracování osobních údajů zákazníků kontrolované osoby, tedy předmětu kontroly). V neposlední řadě dochází ke zpracování osobních údajů za účelem nabídky dříve poskytnutých služeb (přímý marketing), pro prevenci podvodů či zajištění zabezpečení sítě a informací IT systémů, pro případné právní spory, zde je právním titulem zpracování oprávněný zájem správce dle čl. 6 odst. 1 písm. f) obecného nařízení.

Kontrolou bylo zjištěno, že kontrolovaná osoba v době kontroly zpracovává osobní údaje klientů v souladu s právním titulem ve smyslu čl. 6 odst. 1 písm. b), popřípadě písm. c) a f) obecného nařízení.

Kontrolující se rovněž zabývali plněním informační povinnosti ze strany kontrolované osoby, která je plněna v několika rovinách. Ta má jednak vypracovanou samostatnou informaci o zpracování osobních údajů pro zákazníky a podrobné informace o zpracování osobních údajů nalezneme také na přihlášce k energetické soutěži. Na internetové stránce kontrolované osoby jsou pak rozvedena pravidla zpracování osobních údajů.

Kontrola se zabývala také plněním povinností stanovených v čl. 30 obecného nařízení vést záznamy o činnostech zpracování a v neposlední řadě se zaměřila na plnění povinností stanovených v čl. 32 obecného nařízení, tedy na povinnost zabezpečení osobních údajů a zabezpečení zpracování.

Nebylo konstatováno porušení v žádném z osmi kontrolních zjištění výše citovaných článků obecného nařízení.

Inspektor František Bartoš

Zpracování osobních údajů při poskytování služeb elektronického podpisu certifikační autoritou PostSignum – Česká pošta, s.p.

Kontrola byla zahájena na základě stížnosti ve věci neoprávněného zpracování osobních údajů, které vypovídají o bonitě, platební morálce a důvěryhodnosti spotřebitele Českou poštou, s.p. Předmětem kontroly bylo dodržování povinností v souvislosti se zpracováním osobních údajů při poskytování služeb elektronického podpisu certifikační autoritou PostSignum, ve smyslu zákona o poštovních službách, zákona o elektronických úkonech a autorizované konverzi dokumentů, zákona o elektronickém podpisu a zákona o ochraně spotřebitele, se zaměřením na dodržování povinností stanovených obecným nařízením. Kontrolovaná osoba spolupracuje s Registrem platebních informací (REPI), do kterého informace vkládá a zároveň má náhled na takové, které jsou v něm uloženy. Pro účely zpracování osobních údajů v souvislosti s REPI kontrolovaná osoba souhlas svých zákazníků nepožaduje, neboť k tomuto zpracování není dle ustanovení zákona č. 634/1992 Sb., o ochraně spotřebitele, vyžadován.

Městský soud v Praze dne 21. března 2017 přerušil řízení ve věci žaloby, podané sdružením SOLUS, proti rozhodnutím Úřadu pro ochranu osobních údajů (spis. zn. 10a212L/2-13).

Zároveň dne 23. ledna 2018 rozhodl Ústavní soud ČR o návrhu skupiny senátorů Parlamentu České republiky na zrušení § 20z zákona o ochraně spotřebitele, a to tak, že návrh senátorů se spojuje s výše uvedeným řízením ve věci žaloby podané sdružením SOLUS, které vede Městský soud v Praze.

O obou návrzích Ústavní soud ČR dosud nerozhodl, proto kontrolující nemohli v daném případě učinit jednoznačný a objektivní závěr, zda kontrolovaná osoba v souvislosti se zpracováním osobních údajů svých zákazníků za účelem posouzení jejich bonity, platební morálky a důvěryhodnosti porušila či neporušila obecné nařízení.

Kontrolovaná osoba námitky proti kontrolním zjištěním nepodala.

Ústavní soud ČR nakonec návrh senátorů a Městského soudu v Praze na zrušení § 20z zamítnul a ve svém nálezu vyhlášeném dne 11. listopadu 2020 svůj závěr odůvodnil takto:

„Zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění zákona č. 378/2015 Sb., obsahuje v § 20z odst. 1 komplexní a podrobnou úpravu podmínek, za nichž mohou prodávající získávat informaci o úvěruschopnosti spotřebitelů i bez jejich souhlasu. Tato úprava ve svém souhrnu představuje dostatečné záruky proti nepřiměřenému šíření osobních údajů spotřebitelů. Ustanovení § 20z odst. 1 věty třetí a čtvrté zákona o ochraně spotřebitele jsou v souladu s ústavním pořádkem a lze je vyložit způsobem souladným s čl. 8 odst. 2 Úmluvy o ochraně lidských práv a základních svobod a čl. 8 odst. 2 Listiny základních práv Evropské unie. Tato ustanovení představují zásah do práva spotřebitelů na soukromí a na informační sebeurčení ve smyslu práva podle čl. 10 odst. 3 Listiny základních práv a svobod, neústí však v porušení těchto ústavně zaručených práv, neboť zásah je vyvažován silným veřejným zájmem na předcházení předlužování spotřebitelů. Tento veřejný zájem se pojí s oprávněnými zájmy podnikatelů nabízejících spotřebitelům finanční služby."

Inspektor Petr Krejčí

Kontrola používání platformy cookies ve veřejnoprávní instituci

Na základě kontrolního plánu byla provedena kontrola, jejímž předmětem bylo zpracování osobních údajů návštěvníků webových stránek souvisejících s provozováním rozhlasového vysílání a poskytování veřejné služby klientům v souvislosti s používáním platformy cookies. Kontrola se zaměřila především na zákonnost tohoto zpracování, zásady zpracování osobních údajů, poskytování informací o tomto zpracování a zabezpečení zpracovávaných osobních údajů.

Bylo zjištěno, že kontrolovaná osoba jako správce osobních údajů zpracovávala osobní údaje z platformy cookies v rozsahu internetový protokol, IP adresa, adresa URL odkazujícího webu, ze kterého byl soubor požadován, datum a čas přístupu, typ prohlížeče a operační systém, jaká byla navštívená stránka, objem přenesených dat a status přístupu.

Platformy cookies využívala, aby udržela krok s vývojem v oblasti elektronické komunikace k plnění jí ze zákona č. 127/2005 Sb., o elektronických komunikacích, zákona č. 231/2001 Sb., o provozování

rozhlasového a televizního vysílání, zákona č. 484/1991 Sb., o Českém rozhlasu, a z dalších obecně platných právních předpisů, uložených úkolů v oblasti šíření programů, sledovanosti pořadů, provádění statistického zjišťování poslechovosti, návštěvnosti webových stránek, analýz a sledování odezvy na literární, hudební a ostatní pořady a k zajištění příjmů z vlastní hudební a jiné tvorby. Chtěla tak zajistit kvalitu programové nabídky při naplňování veřejné služby v oblasti rozhlasového vysílání, a také v rámci ochrany před případnými útoky a trestnou činností k eventuálnímu použití orgány činnými v trestním řízení.

Kontrola dospěla k závěru, že si kontrolovaná osoba v rozsahu předmětu kontroly plní všechny povinnosti, které jí ukládá obecné nařízení a zákon o zpracování osobních údajů, resp. má jmenovaného pověřence pro ochranu osobních údajů. Dodržuje tak zásady zpracování a rovněž byla schopna prokázat právní důvod zpracování, plnění informační povinnosti a řádné vyřizování žádostí subjektů údajů v souvislosti s uplatněním jejich práv.

Doložila přijatá technická a organizační opatření pro zabezpečení osobních údajů, vedení záznamů o činnostech zpracování, a má zpracovanou metodiku analýzy rizik zpracování, resp. vnitřní předpisy obsahují mimo jiné vypracované obecné postupy pro posuzování vlivu na ochranu osobních údajů.

Kontrolující v souvislosti s předmětným zpracováním osobních údajů nezjistili porušení obecně platných právních předpisů. Nad rámec předmětu kontroly byla kontrolované osobě pouze dána určitá doporučení ve vztahu k nové právní úpravě.

Výsledek této kontroly nelze použít pro zevšeobecnění používání cookies ve všech případech a u všech správců či zpracovatelů osobních údajů, neboť v rámci daného zpracování osobních údajů došlo k očekávanému lepšímu plnění zákonných povinností, které se na správce vztahují.

Kontrola sdružování osobních údajů z různých databází na webové stránce provozované do doby dalšího prodeje databáze

Úřad zahájil kontrolu obchodní společnosti na základě postupně doručovaných stížností od více subjektů údajů. Stížnosti se týkaly nesouhlasu se zveřejněním osobních údajů subjektů údajů na její webové stránce.

V průběhu kontroly byly porovnávány ve vzájemné souvislosti tvrzené skutečnosti, včetně skutečností zjištěných v rámci vyžádané součinnosti s Policií ČR. Bylo zjištěno, že za dobu od koupě databáze do jejího dalšího prodeje uskutečněného v průběhu kontroly byly správcem osobních údajů u více než jednoho milionu subjektů údajů zpracovávané jejich osobní údaje na webové stránce bez právního důvodu a plnění některých dalších povinností správce.

Dle doloženého soupisu měla kontrolovaná osoba provést na žádost subjektů údajů cca 1 500 výmazů subjektů údajů z webové stránky.

Kontrolovaná osoba se tak v rámci této údajné změny podnikatelského záměru, a tedy prodejem databáze v dané aplikaci další obchodní společnosti, nemohla zbavit odpovědnosti za plnění povinností správce. Bylo zjištěno, že za dobu, kdy kontrolovaná osoba provozovala webové stránky, na kterých zpracovávala osobní údaje subjektů údajů, porušila povinnosti správce tak, jak byly kontrolou zjištěny a uvedeny v protokolu o kontrole.

Proti kontrolnímu zjištění podala kontrolovaná osoba námitky, kterým předsedkyně Úřadu částečně vyhověla. Pokud kontrolovaná osoba nebyla schopna doložit účel shromažďovaných osobních údajů, který by byl v souladu s obecným nařízením u tak velkého množství subjektů, jejichž osobní údaje zpracovávala, nebyla oprávněná v souvislosti se žádostí subjektů údajů o výmaz jejich osobních údajů od nich požadovat ještě další osobní údaje v rámci vyplňovaného formuláře na webové stránce, jako je e-mailová adresa.

Vzhledem k tomu, že kontrolovaná osoba v době ukončení kontroly již nezpracovávala osobní údaje subjektů údajů získané prostřednictvím dané aplikace koupí od jiné obchodní společnosti, a také případně od další osoby s následným doplňováním z dalších databází, resp. z veřejných rejstříků, nebylo jí uloženo opatření k nápravě.

Za zřejmá závažná porušení povinností správce byla kontrolované osobě ve správním řízení uložena již pravomocným rozhodnutím pokuta ve výši 100 000 Kč.

Oddělení kontroly soukromého sektoru

Zpracování osobních údajů z veřejnoprávních rejstříků prostřednictvím soukromoprávních internetových stránek

Kontrola byla zahájena na základě stížností, které směřovaly proti neoprávněnému zpracování osobních údajů na webových stránkách kontrolované osoby. Na nich agregovala stovky tisíc údajů o fyzických osobách podnikatelích formou prostého překlápění z veřejně dostupných veřejnoprávních rejstříků.

Úřad došel k závěru, že kontrolovaná osoba porušila čl. 6 odst. 1 obecného nařízení, protože v případě prostého překlápění osobních údajů z živnostenského rejstříku a obchodního rejstříku je takové zpracování nezákonné, neboť nesplňuje podmínku nezbytnosti ve vztahu k účelu zpracování osobních údajů. Právní titul – oprávněné zájmy kontrolované osoby – tak pro dané zpracování nebylo možné aplikovat.

Ze strany kontrolované osoby dále došlo k porušení čl. 12 odst. 2 obecného nařízení. Kontrolovaná osoba totiž neusnadňovala výkon práv stěžovatelů (subjektů údajů) dle čl. 15 až 22 obecného nařízení. Prakticky to znamenalo, že když se na ni stěžovatelé obrátili s písemnou žádostí o výmaz jejich osobních údajů na adresu uváděnou kontrolovanou osobou jako kontaktní adresou na webových stránkách, společnost na žádost nereagovala (dopis se stěžovatelům vrátil jako nedoručený s ne-známým adresátem). Telefonicky ji pak nebylo možné zastihnout vůbec. Na svých webových stránkách přitom kontrolovaná osoba umožňovala výmaz osobních údajů vyplněním interaktivního formuláře, což někteří stěžovatelé učinili, avšak jejich osobní údaje se na stránkách nacházely i nadále.

Kontrolovaná svým jednáním též porušila čl. 12 odst. 3 obecného nařízení, neboť stěžovatelé nebyli žádným způsobem vyrozuměni o způsobu vyřízení jejich žádosti o výmaz osobních údajů, resp. nebyli vyrozuměni vůbec.

V poslední řadě bylo protokolem o kontrole konstatováno i porušení čl. 14 obecného nařízení, neboť kontrolovaná osoba nesplnila svou informační povinnost dle tohoto článku (kontrolující měli za prokázané, že pouhým zveřejněním informací na webových stránkách kontrolované osoby nelze považovat tuto povinnost za splněnou).

V této souvislosti bylo třeba vyvrátit i výjimku uvedenou v čl. 14 odst. 5 písm. b) obecného nařízení, na kterou by se teoreticky mohla kontrolovaná osoba odvolávat. Tento výjimečný případ by mohl nastat tehdy, když by nebyla objektivně schopna subjekty údajů kontaktovat, nicméně Úřad měl za prokázané, že společnost znala minimálně adresu sídla podnikání fyzických osob či adresu jejich provozoven, na kterých bylo možné subjekty údajů kontaktovat a splnit tak informační povinnost. Tím, že informační povinnost nebyla dodržována, stovky tisíc fyzických osob neměly žádnou povědomost o tom, že jsou jejich osobní údaje zpracovávány.

Po doručení protokolu o kontrole kontrolovaná osoba nepodala námitky.

Následně bylo s kontrolovanou osobou zahájeno správní řízení, ve kterém byl vydán příkaz o uložení opatření k nápravě, a vzhledem k vysoké závažnosti porušení obecného nařízení a s ohledem na ohrožení a uveřejnění stovky tisíc osobních údajů fyzických osob bez právního důvodu stanovena pokuta ve výši 500 000 Kč. Je také třeba uvést, že v průběhu provádění kontroly kontrolované osobě byla uložena pokuta za nesoučinnost podle kontrolního řádu ve výši 100 000 Kč.

Kopírování občanských průkazů v půjčovně lyžařského vybavení

Na základě dat ze Systému pro výměnu informací o vnitřním trhu provedl Úřad mimo jiné i kontrolu společnosti zabývající se půjčováním lyžařského vybavení, která v rámci své činnosti pořizovala kopie občanských průkazů svých zákazníků.

Kontrolující místním šetřením v jedné z jejích poboček zjistili, že společnost v rámci výpůjček zimního vybavení zpracovávala osobní údaje svých klientů a zapisovala je do počítače umístěného na každé pobočce. Zároveň však byla vyhotovena smlouva o výpůjčce sportovního vybavení, která byla uložena v počítači a v tiskové podobě předložena k podpisu klientovi – nájemci. Právní titul pro předmětné zpracování byl v daném případě kontrolou shledán v čl. 6 odst. 1 písm. b) obecného nařízení, tj. plnění smlouvy, a to v souladu s praxí a předloženými záznamy o činnosti zpracování.

Vzhledem k vysokým cenám sportovního vybavení a velkému riziku z toho vyplývajícímu však kontrolovaná osoba dále požadovala složení finanční kauce za zapůjčené sportovní vybavení nebo provedení celé kopie platného průkazu totožnosti, se souhlasem majitele, tedy na základě zmiňovaného ustanovení obecného nařízení, kdy byla kopie průkazu totožnosti v elektronické podobě uložena v systému užívaném kontrolovanou osobou.

Souhlas s kopií občanského průkazu byl zakomponován do samotné smlouvy o výpůjčce sportovního vybavení. Podpisem smlouvy o výpůjčce sportovního vybavení byl tedy souběžně podepsán i samotný souhlas se zpracováním kopie průkazu totožnosti. Kontrolující tento způsob získávání souhlasu vyhodnotili jako porušení zákonnosti zpracování ve formě absence řádně uděleného souhlasu, jelikož souhlas nebyl získán způsobem, jak ukládá obecné nařízení.

V rámci výše popisované kontroly bylo souběžně kontrolováno plnění povinností vyplývajících z ustanovení čl. 12 a návazně čl. 13 obecného nařízení. Přitom bylo zjištěno, že subjekty údajů nebyly do doby zahájení kontroly písemně poučovány (informovány) o zpracování osobních údajů na místě ani prostřednictvím webových stránek kontrolované osoby, pouze ústně při podpisu smlouvy o výpůjčce sportovního vybavení.

Návazně bylo s kontrolovanou osobou zahájeno správní řízení, ve kterém byla uložena nápravná opatření a pokuta. Výše sankce byla stanovena s přihlédnutím k závažnosti a délce trvání (kdy kopie občanských průkazů byly mazány ihned po vrácení vypůjčeného vybavení a v průběhu místního šetření byly vymazány veškeré kopie, které v dané době měla kontrolovaná osoba uloženy), dále s přihlédnutím k míře spolupráce kontrolované osoby s Úřadem a snahou po okamžité nápravě závadného stavu.

Oddělení kontroly veřejného sektoru

Kontrola zabezpečení internetových stránek v souvislosti s předáváním výsledků zdravotních vyšetření

Kontrola provozovatele nestátního zdravotnického zařízení byla zahájena na základě ohlášení případu porušení zabezpečení osobních údajů, především však na základě dalších skutečností, které byly Úřadem zjištěny v rámci úkonů předcházejících kontrole. V rámci nich byly zjištěny zejména nedostatky v zabezpečení internetových stránek.

Předmětem kontroly bylo dodržování povinností stanovených kontrolované osobě obecným nařízením a zákonem o zpracování osobních údajů v souvislosti se zpracováním osobních údajů prostřednictvím elektronických komunikačních prostředků a jejich zabezpečení. Konkrétně se kontrola zaměřila na možné porušení čl. 24 a čl. 32 obecného nařízení při předávání výsledků zdravotních vyšetření prostřednictvím internetových stránek.

Kontrolovaná osoba je provozovatelem nestátního zdravotnického zařízení, které poskytuje pacientům řadu diagnostických vyšetření. Na svých internetových stránkách následně předává výsledky vyšetření, a to jak pacientům, tak i lékařům, kteří vyšetření doporučili. Dochází tak ke zpracování údajů i o zdravotním stavu, tj. i zvláštních kategorií osobních údajů ve smyslu čl. 9 odst. 1 obecného nařízení.

Předmětem ohlášení případu porušení zabezpečení bylo napadení internetové stránky neznámým útočníkem (později ztotožněným Policií ČR), který následně e-mailovou zprávou kontrolovanou osobu upozornil na nedostatky týkající se hesla, jímž byly výsledky vyšetření zpřístupňovány, a na slabé zabezpečení protokolu samotné stránky.

V návaznosti na tuto událost kontrolovaná osoba zastavila provoz předmětné internetové stránky a navrhla technická opatření pro vyšší zabezpečení. Kontrolující však zjistili, že i další internetové stránky, provozované kontrolovanou osobou za účelem předávání výsledků vyšetření, vykazují stejné nedostatky. Jejich provoz však nebyl omezen a ani nedošlo k implementaci nových technických opatření.

Provedenou kontrolou bylo zjištěno porušení povinností správce osobních údajů vyplývajících z čl. 24 a čl. 32 obecného nařízení, neboť kontrolovaná osoba nepřijala taková technická a organizační opatření, aby zajistila a byla schopna doložit, že zpracování osobních údajů je prováděno v souladu

s obecným nařízením, resp. neprovedla taková technická a organizační opatření, aby bylo dosaženo úrovně zabezpečení odpovídající danému riziku.

Kontrolovaná osoba využívala u internetových stránek zpřístupňujících výsledky vyšetření nezabezpečený protokol komunikace a slabě zabezpečené přístupové heslo. Totožné heslo ke zpřístupnění výsledků vyšetření bylo navíc předáváno jak subjektu údajů, tak i lékaři, který vyšetření doporučil. Absentovalo vedení evidence přístupů k osobním údajům a administrátorský přístup k systému zpřístupňování výsledků vyšetření, kterým disponuje zpracovatel osobních údajů, nebyl evidován a byl zabezpečen pouze heslem o síle tří znaků. Kontrolovaná osoba tak postrádala schopnost zajistit neustálou důvěrnost osobních údajů obsažených ve výsledcích vyšetření. Závadný stav začala kontrolovaná osoba napravovat již v průběhu kontroly. Zavedla zabezpečený protokol na internetových stránkách, změnila systém vytváření přístupových hesel a implementovala opatření, které má zabránit nahodilým pokusům získat neoprávněný přístup k výsledkům vyšetření, v podobě zablokování IP adresy v případě opakovaného zadávání nesprávného hesla.

Proti kontrolním zjištěním kontrolovaná osoba nepodala námitky. Po skončení kontroly byla Úřadem v rámci navazujícího správního řízení uložena opatření k nápravě, která kontrolovaná osoba splnila. Přistoupila přitom ke zcela novému řešení předávání výsledků vyšetření, kdy dosavadní jednotlivé internetové stránky nahradila novým jednotným systémem pro předávání výsledků vyšetření. Při jeho tvorbě poskytovatel IT služeb spolupracoval s pověřencem pro ochranu osobních údajů kontrolované osoby ve snaze vyhovět doporučením Úřadu.

Úřad v souvislosti s kontrolou uložil kontrolované osobě pokutu ve výši 10 000 Kč, a to za porušení povinnosti stanovené čl. 32 odst. 1 obecného nařízení. V tomto konkrétním případě nedošlo k úniku osobních údajů ve smyslu jejich dalšího neoprávněného zveřejnění či využití pro jiný účel a Úřad při stanovení sankce přihlédl též ke skutečnosti, že kontrolovaná osoba během kontroly spolupracovala, již v průběhu kontroly aktivně činila kroky k nápravě protiprávního stavu a navrhovala možná řešení s cílem dosáhnout vyšší úrovně zabezpečení. Jak již bylo uvedeno, v návaznosti na zjištěná pochybení a uložená opatření k nápravě pak nadto kontrolovaná osoba přistoupila ke zcela novému systému předávání výsledků vyšetření. Pokuta byla kontrolovanou osobou uhrazena.

Oddělení podpory

Zpracování osobních údajů při přímém marketingu

Kontrola byla provedena na základě několika stížností, kdy byli stěžovatelé kontaktováni zástupci kontrolované osoby, aniž by jí poskytli své osobní údaje. V minulosti (přibližně do roku 2016) stěžovatelé využili služby obchodníků kontrolované osoby při uzavírání pojistných nebo finančních smluv v době, kdy tito obchodníci vykonávali činnost pro jinou společnost. S tou měli obchodníci uzavřenu smlouvu o spolupráci pro podřízeného zprostředkovatele obchodní sítě.

Kontrolující zjistili, že obchodníci/poradci kontrolované osoby použili minimálně v případě stěžovatelů k jejich kontaktování osobní údaje, které jim byly známy z jejich předchozí obchodní činnosti za účelem přímého marketingu (telefonické hovory), čímž zároveň porušili smlouvu o spolupráci pro podřízeného zprostředkovatele obchodní sítě uzavřenou s předchozí společností. Nešlo tedy o zákonné zpracování ve smyslu obecného nařízení.

Kontrolovaná osoba nezpracovávala osobní údaje korektně a transparentním způsobem. Obchodníci/poradci kontrolované osoby minimálně v případě stěžovatelů nedisponovali žádným legitimním titulem pro další zpracování osobních údajů stěžovatelů. Zpracování takovýchto dat nemůže být nezbytným pro účely oprávněných zájmů příslušného správce (kontrolované osoby) či třetí strany.

Kontrolovaná osoba zpracovávala osobní údaje stěžovatelů ve smyslu obecného nařízení neoprávněně, tedy protizákonně, protože nedisponovala ani jedním legitimním titulem k takovému zpracování.

Kontrola tak konstatovala porušení ustanovení čl. 5 odst. 1 písm. a) a ustanovení čl. 6 odst. 1 obecného nařízení. Vzhledem k tomu, že kontrolovaná osoba závadný stav neprodleně napravila, neuložil Úřad opatření k odstranění zjištěných nedostatků.

Uloženou pokutu kontrolovaná osoba uhradila.

STÍŽNOSTI A PODNĚTY

Úřad v roce 2020 přijal 1855 podnětů a stížností. I přes probíhající pandemii koronaviru COVID-19 tak došlo, v porovnání s předchozím rokem (2482 doručených stížností a podnětů) pouze k mírnému poklesu. Ačkoli bylo nutné vykonávat značnou část činností z domova, nebyla plynulost řešení stížností a podnětů nijak výrazněji ovlivněna.

Epidemie ovlivnila nejen chod Úřadu, ale i obsahovou skladbu stížností a podnětů. Podatelé se na Úřad obraceli se stížnostmi a podněty, které vyvěraly z činnosti některých státních orgánů při zvládání epidemie. Od samotného začátku epidemie se podatelé obraceli na Úřad s řadou podnětů, ve kterých uváděli, že došlo k neoprávněnému předání jejich údajů při zasílání informativních SMS Ministerstvem zdravotnictví v rámci jarní vlny pandemie. V daném případě Úřad podatelům objasnil, že k předání údajů mobilním operátorem Ministerstvu zdravotnictví nedošlo. Ministerstvo zdravotnictví jako ústřední orgán státní správy pro ochranu veřejného zdraví **může požádat mobilní operátory o rozeslání informativní SMS o nebezpečí zavlečení infekčního onemocnění na území České republiky. V daném případě se tedy nejednalo o sledování pohybu občanů**.

Na podzim podatelé namítali zasílání SMS hlavní hygieničkou, prostřednictvím telefonních operátorů, nabádajících k instalaci aplikace eRouška. Tyto podněty nebyly shledány jako důvodné. Postup Ministerstva zdravotnictví při zasílání informace o možnosti nainstalovat si na chytré telefony aplikaci eRouška s odkazem na webové stránky, na nichž lze nalézt, jak tuto aplikaci nainstalovat, bylo posouzeno jako zpracování osobních údajů, které je nezbytné pro splnění úkolu prováděného ve veřejném zájmu, kterým ochrana veřejného zdraví a ochrana lidských životů bezesporu je.

Z těch podnětů a stížností týkajících se epidemie COVID-19, které Úřad seznal jako důvodné a dále se jimi aktuálně zabývá, ať již v rámci kontroly nebo předkontrolních opatření, lze zmínit podněty, které se týkaly aplikace, používající lokační údaje a nástroje k vysledování kontaktů nakažených osob, a dále stížnosti, v nichž podatelé namítali rozsah osobních údajů, k jejichž poskytnutí byli nuceni již ve fázi registrace k testování na COVID-19, popřípadě kdy podatel dokládá vynucování souhlasu se zpracováním údajů o zdravotním stavu, kdy takový souhlas nelze považovat za svobodný.

Úřad zaznamenal ojediněle i neoprávněné zpřístupnění výsledků testů na COVID-19 jiné osoby, ať již formou podnětu anebo ohlášení samotným správcem. V těchto případech se však nejednalo o systémové pochybení správce osobních údajů, ale ojedinělé selhání ze strany zaměstnance správce, a správci přijali opatření k předcházení dalších incidentů.

Z hlediska zastoupení stížností z oblastí veřejnoprávních a soukromoprávních vztahů lze konstatovat, že pokračuje trend výrazně převažujícího zastoupení podnětů a stížností směřujících proti zpracování osobních údajů v oblasti soukromoprávních vztahů. Z nich nejčastějším zůstává zpracování osobních údajů pro marketingové účely.

Přestože již v roce 2019 zveřejnil Úřad na svých webových stránkách materiál Jak se bránit nevyžádanému telemarketingu, směřovala i v roce 2020 značná část stížností na zpracování údajů pro marketingové účely proti telefonním marketingovým hovorům, které jsou uskutečňovány bez vazby na předchozí vztah mezi volaným a volajícím a jež dotčené osoby vnímaly jako velmi obtěžující.

Úřad obdržel jak stížnosti na zasílání obchodních sdělení, aniž by zpracováním dotčená osoba (subjekt údajů) znala zdroj, ze kterého správce získal její osobní údaje, tak i stížnosti na získávání souhlasu se zpracováním údajů za účelem marketingu, někdy i spojené s nemožností získat danou službu bez poskytnutí takového souhlasu. V této souvislosti je nutné zmínit i několik desítek stížností, jež se týkaly neetického jednání některých subjektů, které v době nouzového stavu zneužily možnost zasílání datových zpráv k tomu, aby šířily nevyžádané obchodní nabídky a sdělení uživatelům datových schránek. Tyto stížnosti byly dále řešeny v rámci správního řízení s předmětnými subjekty.

Pro možné uplatnění dozorových pravomocí Úřadu, a to nejen při řešení stížností na zpracování údajů v rámci telemarketingu, je stěžejní, aby tvrzení uvedená ve stížnosti byla doložena. Úřad proto obecně podatele vyzývá k uplatnění práv, která jim obecné nařízení přiznává, neboť bez doložení podkladů, které by odůvodňovaly tvrzení podatele, nelze zahájit úřední postup a vést šetření proti subjektu odpovědnému za zpracování údajů. V případech, kdy na doporučení Úřadu podatel reaguje, práva uplatní a podezření na porušení zásad při zpracování osobních údajů doloží, Úřad věc řeší v rámci

kontroly nebo správního řízení. S tím, jak se život v roce 2020 v mnoha ohledech přesunul do online prostředí, narostla četnost stížností, v nichž podatelé upozorňovali na zpracování osobních údajů prostřednictvím tzv. cookies. Ty slouží pro zvláštní, především marketingové účely a nelze je považovat za tzv. technické cookies (potřebné např. pro správné zobrazení webové stránky). Úřad se v této souvislosti zabýval řadou podnětů a stížností, v nichž správce dotčené osoby nedostatečně nebo netransparentně informoval o zpracování osobních údajů prostřednictvím cookies, případně uživateli webové stránky neumožňoval jejich odmítnutí, případně nekalým způsobem získával souhlas s jejich využitím (např. pouhým posunem na webové stránce). Při podezření na systémové porušení zásad ochrany osobních údajů tato podání Úřad aktuálně řeší v rámci svých kontrolních pravomocí, v ostatních případech k nápravě stavu vedla výzva Úřadu správci k odstranění protiprávního stavu.

Velká část stížností se týkala nerespektování práv subjektů údajů ze strany některých správců. Ti pokračovali v zasílání obchodních sdělení i poté, co dotčené osoby odvolaly souhlas, uplatnily právo na výmaz nebo vznesly námitku proti zpracování údajů pro marketingové účely. Dále se často jednalo o případy, kdy správce neposkytl subjektu údajů adekvátní informaci o zpracování údajů, případně na podobné žádosti ani nereagoval.

Úřad i nadále řešil případy, kdy správce odmítl na žádost subjektu údajů poskytnout kopii nahrávky hovoru (příp. jeho přepis), na jehož základě měl být smluvní vztah s ním uzavřen, nebo došlo ke změně smluvního vztahu, případně jím byl zaznamenán průběh plnění smlouvy.

V roce 2020 se podatelé obraceli na Úřad též s podněty na neplnění nebo nedostatečné plnění povinnosti správce informovat 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.

Tradičně se Úřad zabýval také stížnostmi na provozování kamer se záznamem, ať již v rámci sousedských sporů nebo provozovaných fyzickými či právnickými osobami k ochraně majetku, a to přesto, že v této oblasti šíří dlouhodobě osvětu, např. na svém webu v sekci Často kladené otázky podle oblastí zpracování údajů.

Obdobně jako v uplynulých letech byly i tentokrát součástí stížnostní agendy stížnosti na podmínění poskytnutí služby pořízením kopie dokladu totožnosti (občanského průkazu, cestovního pasu). Úřad při posouzení těchto stížností vycházel z hodnocení, zda v daném případě měl správce právní titul k pořízení kopie tohoto dokladu, včetně všech osobních údajů na něm uvedených, a zdali v případě, že právním titulem byl souhlas, byl dán svobodně, a v neposlední řadě zdali správce dodržel zásadu minimalizace údajů. Obdobně, především z hlediska existence právního titulu pro zpracování a zásady minimalizace údajů, posuzoval Úřad stížnosti na zpracování rodného čísla.

Nadále se na Úřad obracely fyzické osoby dotčené zpracováním svých dat zveřejněním na internetu, a to jak pro novinářské účely, tak v rámci příspěvků a diskusí na sociálních sítích a webových stránkách. Při posouzení těchto stížností Úřad vycházel ze zhodnocení, tj. zda se nejednalo o zveřejnění výlučně v rámci osobních činností (tj. na profilu na sociální síti, v rámci diskuse, blogu na sociální síti nebo na zájmové webové stránce) a zdali byl naplněn základní atribut zpracování, tj. určitá systematičnost jednání (jednalo-li se o výstup z evidence, nebo data vkládaná do evidence).

V případech ad hoc zveřejnění informací o člověku, na které věcná působnost obecného nařízení nedopadá, Úřad informoval podatele o možnosti využít ustanovení občanského zákoníku v rámci občanskoprávního řízení. V těchto případech Úřad podatele informoval i o odpovědnosti poskytovatelů internetových služeb (např. vyhledavačů) podle zákona o některých službách informační společnosti, i s odkazem na doporučení zveřejněné na webu Úřadu, jak v tomto případě postupovat, s názvem Jak mohu zažádat o opravu či odstranění údajů přímo u provozovatele služeb? V případech, kdy se jednalo o zveřejnění osobních údajů pro novinářské účely, Úřad věc posuzoval se zřetelem na omezení práva na výmaz a práva podat námitku v případě zpracování pro novinářský účel dle zákona o zpracování osobních údajů.

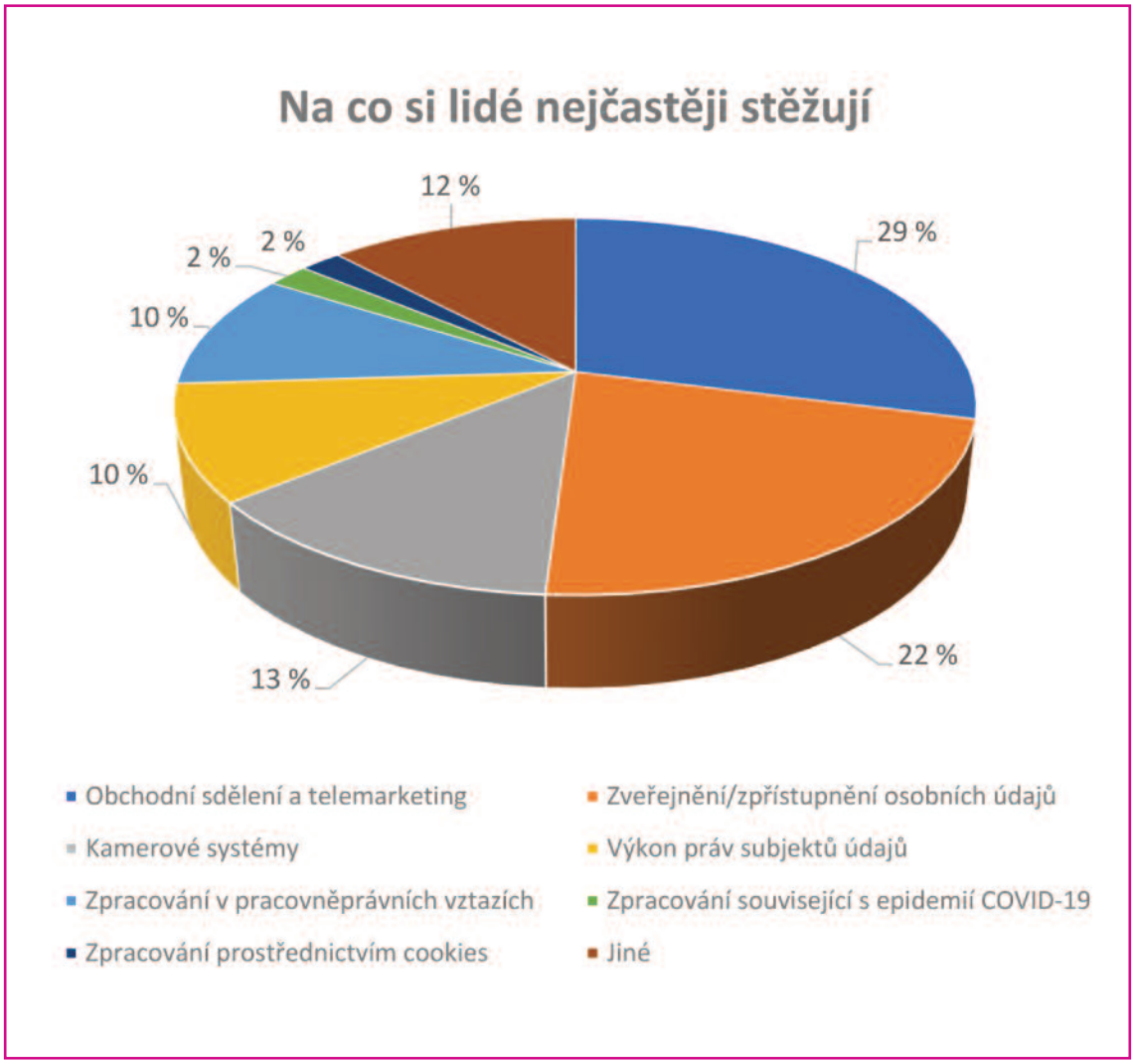
V rámci pracovněprávních vztahů se jednalo již tradičně o stížnosti týkající se sledování zaměstnanců, porušení zabezpečení údajů zaměstnanců, zpracování biometrických údajů zaměstnanců za účelem běžné evidence docházky či zpracování osobních údajů zaměstnanců po ukončení pracovního poměru (např. nezrušení e-mailové schránky nebo zveřejnění údajů na internetu).

Stížnosti směřující proti postupu správců z veřejnoprávní sféry se týkaly oblasti zveřejňování adresních údajů žadatelů při publikování poskytnuté informace podle zákona o svobodném přístupu

k informacím, kdy zejména obce neprovedly na zveřejněném dokumentu o poskytnutí informace anonymizaci žadatele, případně jen nedostatečně. Opakovaným předmětem stížností bylo zveřejnění záznamů (případně zápisů) z jednání zastupitelstva obce nebo rady města na internetu, a to bez nebo s nedostatečně provedenou anonymizací osobních údajů občanů či třetích osob, které mohou být v záznamu obsaženy v souvislosti s jejich soukromými záležitostmi. Úřad se i v uplynulém roce zabýval stížnostmi poukazujícími na nahlížení do základních registrů, aniž by stěžovateli byl znám účel a právní důvod předmětného nahlížení.

Stejně jako v předchozích letech Úřad pokračoval, v případě bagatelních porušení povinností ze strany správce, v osvědčeném informování správců o možném porušení pravidel ochrany osobních údajů. Tímto způsobem, kdy správci na základě upozornění ihned zjednali nápravu, došlo k vyřešení většiny stížností. Konkrétně bylo takto zasláno celkem 452 upozornění. Nicméně v případech, kdy k nápravě tímto postupem správcem údajů dobrovolně nedošlo, Úřad uplatňuje svoji dozorovou působnost v rámci kontroly nebo správního řízení.

Graf „Na co si lidé nejčastěji stěžují" zobrazuje zastoupení různých druhů podnětů a stížností, které Úřad v roce 2020 obdržel.



OHLAŠOVÁNÍ INCIDENTŮ S OSOBNÍMI ÚDAJI

V roce 2020 obdržel Úřad celkem 292 ohlášení porušení zabezpečení osobních údajů.

Škála jednotlivých hlášení byla různorodá, od zaslání informačního e-mailu v otevřené kopii pro příjemce až po porušení s velkým rizikem pro subjekty údajů. Jako příklad lze uvést hackerský útok na zdravotnické zařízení, přičemž nebezpečnost tohoto činu násobila probíhající první vlna pandemie koronaviru.

Vážným a častým důvodem ohlášení ze strany správců osobních údajů byl phishingový útok na počítačové systémy. Významný počet těchto případů byl způsoben nedostatečným poučením a proškolením jednotlivců, následkem jejichž pochybení mohlo docházet například k neuvážlivé manipulaci s přístupovými údaji.

Rok 2020 byl poznamenán i nárůstem potřeby většího zabezpečení internetové sítě v souvislosti se stále více rozšířenou prací z domova a distanční výukou. V tomto ohledu je třeba zmínit obdržené ohlášení z oblasti školství, kdy bylo v rámci online výuky nedostatečně ošetřeno soukromí třídy, čehož využil žák jiné třídy a část výuky uveřejnil na sociální síti. Hlášení tohoto typu bylo sice ojedinělé, nicméně poukázalona zvýšené riziko využívání komunikačních kanálů a nutnost zabývat se podmínkami online provozu komplexně a metodicky nejen ze strany pověřenců pro ochranu osobních údajů, kteří na školách působí.

Dva případy porušení se týkaly sdělování výsledků vyšetření na onemocnění koronavirem COVID-19, kdy bylo po omezenou dobu možné zobrazit data jiného pacienta po změně parametru. Ohlášení bylo podáno v době, kdy byla chyba odstraněna, proto Úřad nepřistupoval k dalším opatřením.

Z ohlášení je dále patrné, že správci osobních údajů mnohdy nepracují s bezpečností a ochranou osobních údajů systematicky a ne vždy dbají na vhodnou politiku hesel. Velmi nepravidelně také hodnotí úroveň zabezpečení přístupu do interních systémů. Dostačující přitom není jen dodržování základních zásad ochrany osobních údajů. Samostatně by měla být vyhodnocena také bezpečnost internetové komunikace (řada správců stále nedoceňuje, že v souladu s čl. 24 obecného nařízení je za standardní ochranu považován https protokol, nikoli pouhé spojení http).

Pozitivním trendem je skutečnost, že ohlašovatelé incidentu téměř ve všech důvodných případech učinili kroky k nápravě a zamezení nežádoucích účinků. V drtivé většině případů vyhodnotil Úřad charakter a způsob řešení incidentů a přijatá opatření na základě zaslaných ohlášení (případně jím vyžádaných doplnění podkladů) za dostačující bez nutnosti uplatnění dozorových pravomocí a v tomto duchu se správci komunikoval, v rámci čehož poskytoval také odborné rady a odkazy na bližší informace.

Za pozitivní trend lze též považovat úbytek ohlášení, která neobsahovala skutečnosti, jež vyžaduje obecné nařízení.

DOZOROVÁ ČINNOST V OBLASTI ŠÍŘENÍ OBCHODNÍCH SDĚLENÍ

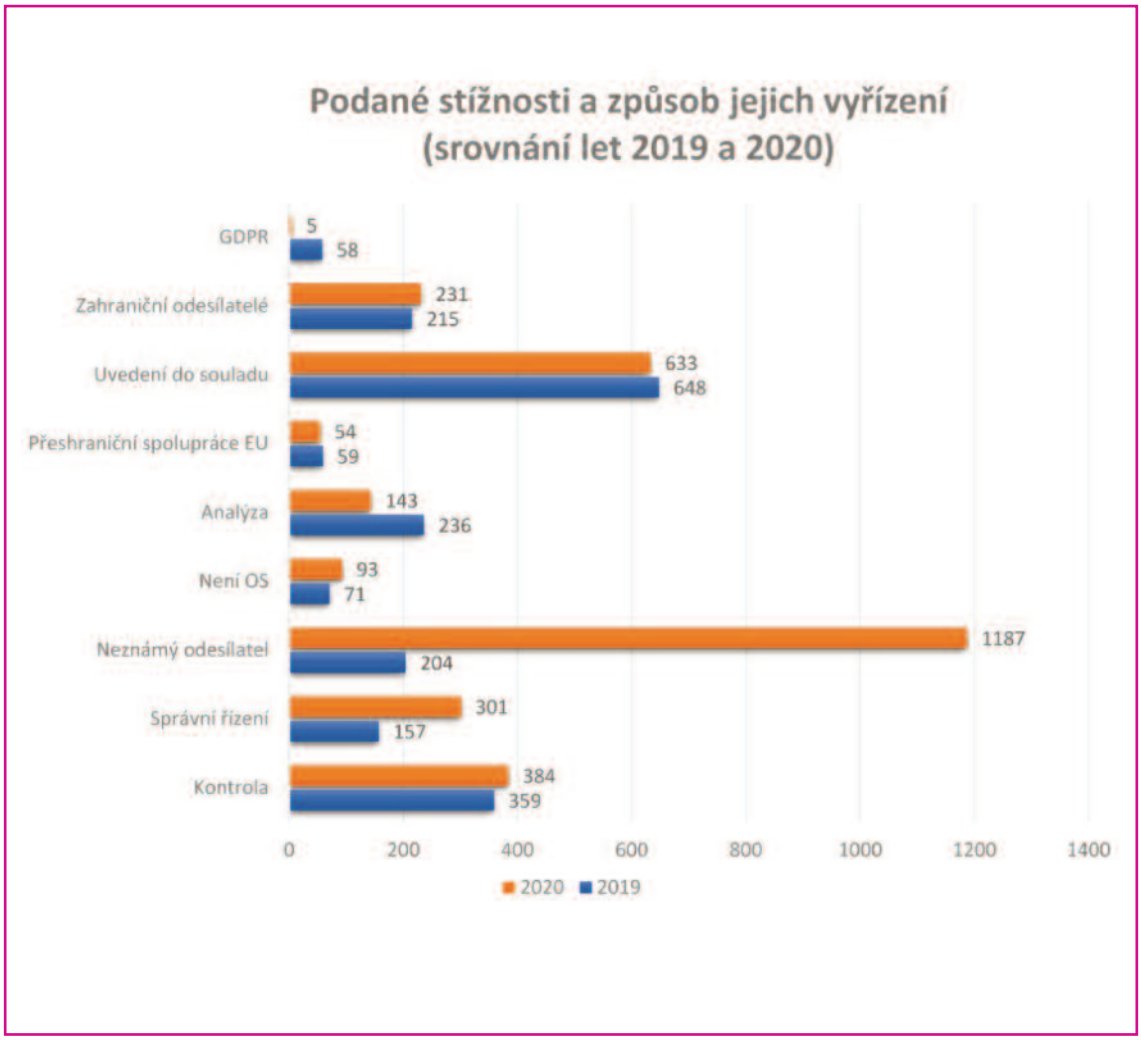
Rok 2020 byl pro oblast šíření obchodních sdělení významným, soudními rozsudky byly potvrzeny některé důležité závěry ze správních řízení, došlo též k uložení prozatím nejvyšší sankce za zasílání nevyžádaných obchodních sdělení ve výši 6 000 000 Kč, ale také došlo i k nárůstu počtu stížností na zasílání nevyžádaných obchodních sdělení zhruba o třetinu oproti předchozímu roku.

Rozsudek NSS 1 As 136/2019-38 z 16. června 2020 se mimo jiné týkal výkladu pojmu obchodní sdělení a rozsudek Městského soudu v Praze č.j. 14 A 242/2018-40 ze dne 7. dubna 2020 byl velice důležitým zejména pro kontrolní praxi Úřadu, jelikož potvrdil dlouho zastávaný výklad Úřadu ve vztahu k odpovědnosti za šíření obchodních sdělení.

O obou rozsudcích Úřad informoval na svých webových stránkách a v této výroční zprávě se jim více věnuje v kapitole Poznatky ze soudního přezkumu na straně 30.

Oproti předchozímu roku došl k výraznému nárůstu v počtu podaných stížností, který může zřejmě souviset i s pandemickou situací v roce 2020, kdy se nabídka zboží a služeb přesunula více do online prostor a tomu odpovídalo i zvýšení online propagace jednotlivých internetových obchodů, včetně šíření obchodních sdělení. Oproti loňskému roku bylo též podáno více stížností na obchodní sdělení, u kterých se však nepodařilo zjistit ani odesílatele, ani subjekt, v jehož prospěch bylo obchodní sdělení šířeno. Často se jednalo o případy, kdy byla obchodní sdělení zasílána přes zahraniční servery. V této souvislosti je třeba odkázat i na Českou obchodní inspekci, která se těmito praktikami zabývá a pravidelně na svých webových stránkách na tyto podezřelé weby upozorňuje. Dále je třeba zmínit, a to opět ve vztahu k předchozímu roku, že v roce 2020 bylo potrestáno více rozesílatelů nevyžádaných obchodních sdělení.

Následující grafy znázorňují počet podaných stížností a způsob jejich vyřízení v roce 2019 a v roce 2020. V roce 2019 bylo Úřadu doručeno 2007 stížností, v roce 2020 to bylo 3031 stížností.



Úřad v roce 2020 vedl 16 kontrolních řízení z této oblasti, přičemž několik kontrol bylo velice složitých. Jednalo se o kontroly společností, které byly v různých ohledech vzájemně provázány, neposky-tovaly v průběhu kontroly žádnou součinnost, naopak se snažily své aktivity při rozesílání nevyžádaných obchodních sdělení skrývat tím, že obchodní sdělení zasílaly z různých neustále se měnících e-mailových adres. Měnili se i provozovatelé internetových obchodů, v jejichž prospěch byla

předmětná obchodní sdělení šířena a faktičtí odesílatelé. Několikrát byl zaznamenán i zánik společnosti s likvidací a následné založení nové, která šířila stejná obchodní sdělení, stejným způsobem. Provázanost mezi těmito odpovědnými subjekty byla zjištěna také v osobách jednatelů či osob nebo společností figurujících jako společníci a taktéž v místě jejich sídel. Ovšem právě ve světle výše uvedeného rozsudku Městského soudu v Praze č.j. 14 A 242/2018-40 ze dne 7. dubna 2020 bylo možno postihnout jak toho, kdo fakticky obchodní sdělení šířil, tak také toho, v čí prospěch bylo odesláno. Na tyto kontroly pak navazovala správní řízení, která byla často vedena formou společných řízení s několika společnostmi. K tomuto je třeba uvést, že díky soustavně a intenzivně prováděným kontrolním a správním řízením s nimi, ale i díky spolupráci v rámci součinnosti dalších orgánů, byl od léta 2020 patrný jistý úbytek podávaných stížností na tyto společnosti, kdy nebyly podávány v takové intenzitě, jako v období několika měsíců předtím.

Úřad dále využívá také možnosti upozornit subjekt na možné porušení zákona, kdy v případě podání jedné či několika málo stížností je patrné, že nedochází k závažnému porušování v oblasti zasílání obchodních sdělení, případně došlo jen k neúmyslnému opominutí či jednorázové chybě při rozesílce. Součástí takového upozornění je i náležité poučení o tom, jak obchodní sdělení zasílat v souladu se zákonem a vždy je požadována odpověď obeslaného subjektu. V nemalé míře bylo tímto způsobem také zjištěno, že chyba může být i na straně stěžovatele, kdy si tento již nepamatuje, že například udělil danému subjektu souhlas se zasíláním obchodních sdělení nebo je jeho zákazníkem a zasílání obchodních sdělení neodmítl. Tímto způsobem bylo v roce 2020 upozorněno celkem 402 společností.

Ke kontrolním řízením je třeba uvést, že v případě neposkytování náležité součinnosti při kontrole bylo vedeno správní řízení o uložení pořádkové pokuty. Těch bylo v roce 2020 vedeno celkem 15 a celková výše uložených sankcí za nesoučinnost činila 933 000 Kč.

Správní řízení ve věci zasílání obchodních sdělení byla vedena celkem v 21 případech a ve 20 případech byla uložena sankce. Celková výše sankcí, které byly pravomocně uloženy za neoprávněné šíření obchodních sdělení, činila 7 684 000 Kč, přičemž v případě jednoho řízení byla uložena doposud nejvyšší sankce v historii Úřadu v souvislosti se zasíláním nevyžádaných obchodních sdělení.

Nejvyšší sankci uložil Úřad společnosti, u které došlo k porušení zákona tím, že rozesílala nevyžádaná sdělení velkému počtu adresátů, kterých bylo například v rámci jedné kampaně osloveno více jak 450 tisíc. Tento subjekt prokázal pouze právní titul postavený na zákaznickém vztahu, což při aplikaci vzorku (kdy bylo požadováno pouze jedno procento, tedy 4 600 adresátů) na celou kampaň, činilo pouze něco přes pět procent oslovených adresátů. Ve zbytku pak bylo konstatováno porušení § 7 odst. 2 zákona o některých službách informační společnosti. Dalším porušením, kterého se tato společnost dopustila, bylo zasílání obchodních sdělení v postavení šiřitele-zadavatele rozesílek obchodních sdělení, kdy předmětná obchodní sdělení byla ve prospěch této společnosti zasílána jinými subjekty. V tomto případě byl konstatován dokonce opakovaný prohřešek, jelikož za stejné porušení byla této společnosti uložena sankce již v roce 2017. Správní orgán se opíral především o závěry z kontrolního řízení, v rámci kterého byly prováděny i zkušební registrace, zkušební ověřování zadávání údajů do systému kontrolovaného, přičemž bylo zjištěno systémové pochybení, nikoli pouze pochybení v jednotlivých případech. K výši této sankce je třeba uvést, že správní orgán přihlédl zejména k vysokému počtu adresátů nevyžádaných obchodních sdělení, k systémovému pochybení a k opakovanému porušení. Míru škodlivosti pak zvyšoval také fakt, že tato společnost je považována za profesionála v oboru, kde dochází k rozsáhlému zpracování osobních údajů. Správní orgán vycházel též z toho, že sankce má mít nejen represivní funkci, ale i odstrašující a preventivní charakter, přičemž vycházel též z účetních záznamů této společnosti uvedených na portálu www.justice.cz. Proti vydanému rozhodnutí byl společností podán rozklad, který byl druhoinstančním rozhodnutím zamítnut a prvoinstanční rozhodnutí bylo potvrzeno. Uloženou pokutu pak společnost zaplatila, nicméně využila ještě svého práva podat žalobu k Městskému soudu v Praze.

Přeshraniční spolupráce v oblasti šíření obchodních sdělení byla ovlivněna tím, že dne 17. ledna 2020 nabylo účinnosti nařízení Evropského parlamentu a Rady (EU) č. 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.

Ministerstvo průmyslu a obchodu vydalo k nařízení i metodiku, jejímž cílem je poskytnout správním úřadům užitečné informace pro jeho praktickou aplikaci. V předchozích letech používaný systém CPC (Consumer Protection Cooperation) byl napojen či včleněn do systému IMI (Internal Market Information System), který je používán předně pro oblast obecného nařízení. Prostřednictvím systému IMI byly v rámci přeshraniční spolupráce osloveny příslušné dozorové úřady v Polsku, Německu, Maďarsku, na Slovensku a ve Velké Británii.

Do systému IMI tak bylo vloženo celkem 54 stížností na zasílání nevyžádaných obchodních sdělení, které byly odeslány ve prospěch některého ze zahraničních internetových obchodů v rámci EU, aby příslušné zahraniční dozorové úřady provedly nezbytná nápravná (donucovací) opatření.

SPRÁVNÍ TRESTÁNÍ

Správní trestání bylo v roce 2020, stejně jako řada dalších činností Úřadu, výrazně ovlivněno pandemií COVID-19, kvůli které muselo dojít při jarní a podzimní vlně epidemie k přizpůsobení vedení správních řízení s obviněnými. To se projevilo například v podobě prodlužování lhůt na žádosti obviněných, kterým správní orgán prvního stupně vyhověl. Úřad zároveň ve zmíněném období ve výzvách či žádostech o podání vysvětlení stanovoval delší lhůtu než obvykle.

Celkově bylo za rok 2020 vedeno 59 správních řízení o přestupcích za porušení obecného nařízení.

K případům správních řízení s veřejnými subjekty je třeba předeslat, že Úřad je v rámci své rozhodovací činnosti vázán platnou právní úpravou, představovanou především obecným nařízením . Ovšem také zákonem o zpracování osobních údajů, jehož ustanovení § 62 odst. 5, vydané k adaptaci obecného nařízení, Úřadu ukládá, aby upustil od uložení správního trestu, jde-li o orgány veřejné moci a veřejné subjekty usazené v daném členském státě. Zákonodárcem zvolené řešení zakládá rozdílné postavení různých skupin, správců a zpracovatelů osobních údajů. Uložit správní trest nelze např. ministerstvům a dalším správním úřadům.

Správní řízení bylo zahajováno ve vztahu k závažnějším přestupkům, zatímco u méně závažných přestupků správní orgán prvního stupně přistupoval k aplikaci ustanovení § 65 zákona o zpracování osobních údajů. To dává správnímu orgánu možnost věc usnesením odložit, aniž by došlo k řízení o přestupku, jestliže bylo vzhledem k významu a míře porušení nebo ohrožení chráněného zájmu, který byl činem dotčen, způsobu provedení činu, jeho následku, okolnostem, za nichž byl čin spáchán, nebo vzhledem k chování podezřelého po spáchání činu zřejmé, že účelu, jehož by bylo možno dosáhnout provedením řízení o přestupku, bylo dosaženo nebo jej lze dosáhnout jinak.

Shora uvedené možnosti bylo typicky využíváno v případech, kdy fyzická osoba nadměrným způsobem kamerovým systémem zaznamenávala veřejné prostranství a po výzvě Úřadu záběr upravila. Nebylo proto důvodné v takových případech zahajovat správní řízení o přestupku, jelikož účel, tj. ochrana veřejného zájmu nebýt monitorován na veřejném prostranství, byl dosažen.

Zmiňované ustanovení zákona o zpracování osobních údajů bylo využito také například v případě zaměstnavatele, který ponechal po rozvázání pracovního poměru se zaměstnankyní její pracovní e-mailovou adresu aktivní, přičemž na základě jejího upozornění jí deklaroval, že provedl deaktivaci. Bývalá zaměstnankyně však zjistila, že se tak nestalo, proto se obrátila na Úřad. Na základě výzvy Úřadu provedl zaměstnavatel nápravu a vysvětlil, že z důvodu technické chyby nebyla náprava zjednána již při žádosti bývalé zaměstnankyně. I v této věci správní orgán prvního stupně usoudil, že po zjednané nápravě, kdy zaměstnavatel navíc doložil, že se již pokoušel deaktivovat adresu bývalé zaměstnankyně na základě její žádosti, nebylo nutné zahajovat formální správní řízení.

V závažnějších případech však Úřad již k vedení správních řízení přistupoval. Správní orgán prvního stupně se v rámci vedených správních řízení na základě obdržených stížností opakovaně věnoval problematice dodržování práv subjektů údajů jednotlivými správci, zejména pak dodržování práva na

přístup k osobním údajům dle čl. 15 obecného nařízení a práva na výmaz osobních údajů dle čl.17 obecného nařízení.

Nutno zdůraznit, že v některých případech se jednalo o situace, kdy ani na základě dřívějšího upozornění ze strany oddělení podnětů a stížností nedošlo u správce ke zjednání nápravy, tj. poskytnutí informací na žádost nebo provedení výmazu osobních údajů (resp. zdržení se jejich využití pro účely, u kterých svědčilo subjektu údajů právo na výmaz). Správní orgán za porušení těchto práv uložil správcům osobních údajů zpravidla pokuty v závislosti na jednotlivých okolnostech, zejména s přihlédnutím k délce trvání porušení, k počtu dotčených subjektů údajů a k míře spolupráce správce s dozorovým úřadem.

Jako příklad z rozhodovací praxe Úřadu lze uvést případ stěžovatelky, které společně s objednaným zbožím přišla faktura od jiné společnosti, než u které zboží objednávala. Stěžovatelka se proto s odkazem na čl. 15 obecného nařízení obrátila na společnost, která zboží dodala, s žádostí o sdělení informací, z jakého zdroje má její osobní údaje, jakým způsobem a na základě jakého právního titulu je zpracovává, a kdo jsou příjemci těchto údajů.

Jelikož společnost na její žádost nereagovala, obrátila se stěžovatelka na Úřad, který společnost na její povinnosti upozornil a vyzval ji k neprodlenému poskytnutí vyžádaných informací subjektu údajů, o čemž stěžovatelku vyrozuměl.

Společnost nereagovala ani na toto upozornění, proto s ní správní orgán zahájil řízení o přestupku podle § 62 odst. 1 písm. c) zákona o zpracování osobních údajů, a za porušení práva subjektu údajů v tomto případě uložil pokutu ve výši 50 000 Kč, přičemž při stanovení výše pokuty mimo jiné zohlednil své předchozí, nijak nereflektované, upozornění.

Na konci roku 2020 Úřad zahájil 11 řízení se subjekty, které zneužily nouzový stav, resp. možnosti zasílat datové zprávy zdarma, a šířily adresátům nevyžádané obchodní nabídky či sdělení, pro podezření z porušení ustanovení čl. 6 odst. 1 a čl. 14 obecného nařízení. Ve formě příkazů byla těmto subjektům uložena kumulativně pokuta ve výši 3 111 000 Kč.

Správní orgán se v rámci své činnosti zabýval rovněž porušením povinnosti správce vyplývající z čl. 32 odst. 1 obecného nařízení, tedy povinnosti správce s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření k zajištění úrovně zabezpečení odpovídající danému riziku.

Jednalo se například o situaci, kdy správce – statutární město – zpřístupnil neoprávněnému příjemci databázi osobních údajů svých dlužníků, a to v rozsahu jméno, příjmení, rodné číslo a údaj o existenci dluhu po splatnosti. K uvedenému došlo tak, že správce měl v adresáři elektronické spisové služby zavedeného jednoho z adresátů duplicitně, a jeden z těchto záznamů obsahoval nesprávný údaj o ID datové schránky. Správce tak v daném případě zjevně neprovedl vhodná technická opatření k zajištění úrovně zabezpečení, a zároveň nedostatečně poučil svou pracovnici o nezbytnosti ověřit správnost kontaktních údajů adresáta před odesláním zprávy. Správní orgán konstatoval, že došlo ke spáchání přestupku podle § 62 odst. 1 písm. a) zákona o zpracování osobních údajů, přičemž podle § 62 odst. 5 téhož zákona ve věci upustil od uložení správního trestu, neboť se jednalo o správce uvedeného v čl. 83 odst. 7 obecného nařízení, konkrétně o orgán veřejné moci.

K upuštění od potrestání bylo na základě ustanovení § 62 odst. 5 zákona o zpracování osobních údajů přistoupeno celkem ve třech případech.

V rámci správního trestání se Úřad v roce 2020 věnoval také projednávání přestupků podle § 61 odst. 1 zákona o zpracování osobních údajů spočívajících v porušení zákazu zveřejnění osobních údajů stanovených jiným právním předpisem. Bylo to celkem v osmi případech. Nejčastěji se jednalo o oznámení přestupku ze strany Policie ČR. Správní orgán se však setkal i se stížnostmi zaslanými ze strany dotčených osob.

Ve většině případů se jednalo o neoprávněné zveřejnění osobních údajů osob zúčastněných na trestním řízení, zejména formou zveřejnění úředních záznamů o podání vysvětlení na Policii ČR, ať již prostřednictvím sociálních sítí, webových stránek, e-mailové pošty nebo zaslaných poštou. V této souvislosti je nutné odkázat na znění ustanovení § 8b odst. 1 zákona č. 141/1961 Sb., o trestním

řízení soudním (trestní řád), ze kterého vyplývá, že: *„Osoby, kterým byly orgány činnými v trestním řízení poskytnuty informace, na které se vztahuje zákaz zveřejnění podle § 8a odst. 1 věty druhé, pro účely trestního řízení nebo k výkonu práv nebo plnění povinností stanovených zvláštním právním předpisem, je nesmějí nikomu dále poskytnout, pokud jejich poskytnutí není nutné k uvedeným účelům. O tom musí být tyto osoby poučeny."* Této povinnosti pak odpovídá skutková podstata přestupku stanovená v § 61 odst. 1 zákona zákona o zpracování osobních údajů, dle které se fyzická osoba *„dopustí přestupku tím, že poruší zákaz zveřejnění osobních údajů stanovených jiným právním předpisem."*

Z celkového počtu osmi podnětů jich Úřad šest odložil, a to z důvodu, že ze shromážděné spisové dokumentace nevyplýval důvod pro zahájení řízení o přestupku.

Ve dvou případech pak uložil pokutu. V prvním případě se obviněný dopustil porušení zákazu zveřejnění osobních údajů tím, že prostřednictvím mobilní aplikace zaslal fotokopii usnesení Policie ČR o zahájení trestního stíhání své osoby nezúčastněným osobám na tomto řízení, a následně jej poskytl k nahlédnutí další osobě. V daném usnesení byly uvedeny osobní údaje účastníků trestního řízení (svědků). Obviněnému byla za toto jednání uložena pokuta.

Ve druhém případě se obviněný dopustil porušení zákazu zveřejnění osobních údajů tím, že pod smyšleným jménem zaslal na adresu zaměstnavatele dopisy obsahující informace o probíhajícím trestním řízení s popisem, z jakého trestného činu je daná osoba obviněna. Tyto anonymní dopisy obsahovaly osobní údaje obviněného v rozsahu jméno, příjmení, titul, pracovní pozice a informace týkající se trestního stíhání. I tomuto obviněnému byla za toto jednání uložena pokuta.

VYŘIZOVÁNÍ STÍŽNOSTÍ PODLE § 175 SPRÁVNÍHO ŘÁDU

Správní řád umožňuje těm, kteří nejsou spokojeni s výstupy správních orgánů, podat stížnost podle § 175 zákona č. 500/2004 Sb., správní řád. Na správní orgány se lze obracet se stížnostmi na nevhodné chování úředních osob nebo se stížnostmi na postup 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 v roce 2020 obdržel celkem 53 podání podle § 175 zákona č. 500/2004 Sb., a to 38 stížností a 15 žádostí o přešetření vyřízení stížnosti. 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. Přibližně jednou pětinou se na celkovém počtu podílely stížnosti směřující do nové agendy svobodného přístupu k informacím.

Ve stejném období Úřad vyřídil celkem 57 podání podle § 175 zákona č. 500/2004 Sb., a to 40 stížností a 17 žádostí o přešetření vyřízení stížnosti. Z tohoto počtu byly čtyři stížnosti vyhodnoceny jako částečně důvodné, jedna jako důvodná a jedna žádost o přešetření stížnosti vyhodnocena jako částečně důvodná. Typickým opatřením je podle povahy věci v takových případech následné nové posouzení původního podnětu a uplatnění dozorových postupů. Dvěma žádostmi o přešetření z roku 2020 se bude Úřad zabývat v roce 2021.

Stejně jako v předchozích letech ani v roce 2020 nesměřoval žádný podnět proti nevhodnému chování úředních osob.

POZNATKY ZE SOUDNÍHO PŘEZKUMU

Stejně jako v předchozích letech i v roce 2020 byla některá rozhodnutí Úřadu předmětem soudního přezkumu. Pokud jde o konkrétní poznatky z předmětné soudní praxe, lze poukázat na několik významných rozsudků, týkajících se zejména:

- odpovědnosti za šíření nevyžádaných obchodních sdělení,
- prodeje databází pro účely zasílání obchodních nabídek,
- zabezpečení osobních údajů pacientů.

1. Ze smyslu § 7 zákona č. 480/2004 Sb., o některých službách informační společnosti, vyplývá, že za subjekt, který šíří obchodní sdělení, nelze považovat pouze přímého odesílatele tohoto sdělení, nýbrž i subjekt, který jeho odeslání inicioval a jehož jménem došlo k jeho šíření.

Městský soud v Praze ve svém rozsudku č. j. 14 A 242/2018–40 ze dne 7. dubna 2020 zamítl žalobu společnosti Widder Gilde s.r.o. (dále jen „žalobce") a ve shodě s právním názorem Úřadu vyjádřeným v rozhodnutí předsedkyně Úřadu č. j. UOOU-05291/17-44 ze dne 27. září 2018 konstatoval, že za osobu, jež šíří obchodní sdělení elektronickými prostředky, nelze považovat pouze jejich přímého odesílatele, nýbrž i osobu, která jeho odeslání iniciovala, dala k němu příkaz či z něj také profitovala. Městský soud v Praze dále uvedl, že: „*Jestliže cílem zákonodárce byla především ochrana adresátů obchodních sdělení před obtěžujícími marketingovými akcemi, musí výklad dotčených právních norem odpovídat tomuto záměru. Opačný výklad, tedy že za šíření odpovídá pouze faktický odesílatel, by činila předmětné právní normy ve své podstatě neúčinnými, neboť v současném digitálním světě by se skutečný šiřitel obchodního sdělení mohl velmi snadno zbavit své odpovědnosti tím, že by odesláním obchodních sdělení pověřil jinou osobu, typicky tu, která by se nacházela mimo dosah českých orgánů veřejné moci. Navíc nelze odhlédnout od faktu, že zákon o některých službách informační společnosti nehovoří o povinnostech toho, kdo rozesílá obchodní sdělení, nýbrž toho, kdo jej šíří. A takto je nezbytné považovat za šiřitele obchodních sdělení elektronickými prostředky nikoli jen subjekt, který fakticky ‚klikem na myš' rozešle daná obchodní sdělení, nýbrž i subjekt, který dal podnět k jejich šíření ke konečným adresátům.*"

Jak Městský soud v Praze dále uvedl, „*žalobce je tedy odpovědný za nedodržení povinností vztahující se k šíření obchodních sdělení elektronickými prostředky v posuzovaných případech, přičemž jeho odpovědnost za nedodržení zákonných povinností nelze vztahovat pouze k uzavření smlouvy, nýbrž k celému procesu šíření obchodních sdělení elektronickými prostředky. Bylo povinností žalobce zajistit, aby obchodní sdělení elektronickými prostředky byla šířena pouze s předchozím souhlasem adresátů a zároveň byla jasně a zřetelně označena jako obchodní sdělení, a pokud tak neučinil, je odpovědný za porušení povinností vyplývajících ze zákona o některých službách informační společnosti.*" Žalobce proto svou odpovědnost nemůže přenášet na svého smluvního partnera.

K tomu Městský soud v Praze dodal, že odpovědnost právnických osob za přestupek dle § 11 zákona o některých službách informační společnosti je odpovědností objektivní. „*Jestliže tedy bylo objektivně zjištěno, že došlo k porušení zákonných povinností, nemůže se žalobce odpovědnosti za jejich porušení zprostit odkazem na smluvní ujednání či odkazem na porušení povinností ze strany smluvního partnera.*"

2. Strukturace osobních údajů v databázích dle požadavků klientů, pro které jsou tyto databáze vytvářeny, nemění nic na postavení subjektu, který určil účel a prostředky zpracování osobních údajů v rámci své podnikatelské činnosti, jako správce osobních údajů.

Rozsudkem Městského soudu v Praze č. j. 11 A 164/2018–48 ze dne 17. září 2020 byla zamítnuta žaloba společnosti SOLIDIS s.r.o. (dále jen „žalobce") proti rozhodnutí předsedkyně Úřadu č. j. UOOU-09774/17-25 ze dne 18. dubna 2018. Tímto rozhodnutím byl zamítnut rozklad žalobce a potvrzeno

prvostupňové rozhodnutí Úřadu ze dne 15. ledna 2018, č. j. UOOU-09774/17-19 ve věci zpracování osobních údajů v databázích a jejich další prodej třetím osobám.

Podle závěru Městského soudu v Praze v projednávané věci Úřad prokázal jak získání předmětných osobních údajů žalobcem, tak i jejich uchovávání žalobcem, což také v odůvodnění obou relevantních správních rozhodnutí v projednávané věci argumentačně podložil. Na str. 4 žalobou napadeného rozhodnutí Úřadu je uvedeno, že *„(o)bviněná (tedy žalobce) byla v postavení správce těchto osobních údajů, neboť určila účel a prostředky zpracování osobních údajů v rámci své podnikatelské činnosti. Strukturace osobních údajů dle požadavků klientů, pro které byly databáze (obviněnou) vytvářeny, nemění nic na postavení obviněné jako správce osobních údajů.*"

Městský soud v Praze se proto bezvýhradně připojil k právnímu posouzení Úřadu vztahujícímu se k postavení žalobce jako správce osobních údajů a dodal, že: *„V projednávané věci tak bylo evidentní, že žalobce současně nemohl být zpracovatelem osobních údajů, byť, jak tvrdil v žalobě, osobní údaje zpracovával do databáze pro daného správce osobních údajů (tj. klienta). Tak se ovšem dělo plně v rámci podnikatelské činnosti žalobce, když mu jeho klienti nepředávali osobní údaje ke zpracování, naopak je pro ně původně do následně předávané databáze zpracovával sám žalobce.*" K tomu Městský soud v Praze dodal, že: *„Kdyby totiž bylo pravdou, jak tvrdí žalobce, že právě jeho klienti, jimž na základě licenčních smluv (objednávek) předával předmětné osobní údaje, byli správci předaných osobních údajů, musel by být tím spíše již sám žalobce správcem osobních údajů, neboť sám předtím v postavení klienta převzal osobní údaje od třetích osob na základě jím dříve uzavřených licenčních smluv.*" Městský soud v Praze v této souvislosti rovněž, opět ve shodě s Úřadem, konstatoval, že zákon č. 101/2000 Sb., o ochraně osobních údajů, s termínem *„dílčího zpracovatele*" sám výslovně nepočítal.

Městský soud v Praze se mimo jiné dále vyjádřil i k žalobcově námitce nedostatečného vymezení skutku Úřadem, a to v bodě 43 svého rozsudku, kde uvedl, že *„na začátku přestupkového řízení samozřejmě nelze po správním orgánu požadovat zcela konkrétní či snad už finální vymezení skutku, neboť od toho zde je právě následné řízení, jehož výsledkem je potom rozhodnutí, kterým je pachatel přestupku uznán vinným. Povinnost zachovat totožnost skutku totiž rozhodně neznamená, že správní orgán musí rozhodnout na základě totožného popisu skutku, který byl uveden v oznámení o zahájení řízení. Řízení slouží právě k tomu, aby konkrétní okolnosti charakterizující daný skutek byly zjištěny a ověřeny (srov. např. rozsudek Nejvyššího správního soudu ze dne 9. listopadu 2016, č. j. 1 As 46/2016–24).*"

Ohledně uložené pokuty Městský soud v Praze konstatoval, že pokuta ve výši 800 000 Kč již z podstaty věci nepředstavuje výjimečný exces. Ta, i přes její nezanedbatelnou výši, dosahovala jen přibližně jedné šestiny horní hranice zákonné sazby, která činila 5 000 000 Kč. Městský soud v Praze přitom neshledal, že by se tato pokuta excesivně vymykala ostatním sankcím Úřadu.

3. Vynaložení veškerého úsilí, které bylo možno požadovat, neznamená jakékoliv úsilí, které právnická osoba vynaloží, ale musí se jednat o úsilí maximálně možné, které je právnická osoba objektivně schopna vynaložit. Pokud právnická osoba v dostatečné míře nepřijme dostatečné mechanismy určené na kontrolu přístupu do elektronické zdravotní dokumentace, nelze než dospět k závěru, že maximální úsilí k zabránění přestupku nevynaložila. Pouhé přijetí interních předpisů nemůže představovat liberační důvod dle § 21 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky. Tím spíše, pokud jejich dodržování ve své podstatě nebylo důsledně kontrolováno.

Městský soud v Praze svým rozsudkem č. j. 14 A 26/2019–37 ze dne 20. května 2020 zamítl žalobu Nemocnice Tábor, a.s. (dále jen „žalobce") proti rozhodnutí předsedkyně Úřadu ze dne 13. prosince 2018, č. j. UOOU-08001/18-14, kterým bylo co do výše uložené pokuty změněno a jinak potvrzeno prvoinstanční rozhodnutí Úřadu ze dne 12. října 2018, č. j. UOOU-08001/18-8. Tím byl žalobce shledán vinným ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů, spočívajícího v porušení ustanovení § 13 odst. 1 tohoto zákona, neboť nepřijal nebo neprovedl opatření pro zajištění bezpečnosti zpracování osobních údajů.

Tohoto přestupku se žalobce jako správce osobních údajů podle § 4 písm. j) zákona o ochraně osobních údajů dopustil v souvislosti s vedením elektronické zdravotní dokumentace tím, že auditní záznamy (logy) v nemocničním informačním systému neumožňovaly určit a ověřit, z jakého důvodu bylo do elektronické zdravotní dokumentace nahlíženo, a také tím, že neprováděl pravidelné kontroly přístupů k elektronické zdravotní dokumentaci.

Městský soud v Praze odmítl argumentaci žalobce a v souladu s rozhodnutími Úřadu v dané věci konstatoval porušení § 13 odst. 1 zákona o ochraně osobních údajů, konkrétně povinnosti dle § 13 odst. 4 písm. c) s tím, že ji přitom nelze bagatelizovat, *„..neboť na jedné straně přispívá k zamezení nedůvodného přístupu k osobním údajům (v případě zdravotnické dokumentace dokonce k citlivým osobním údajům) a na straně druhé dává správci osobních údajů možnost řádně a bez dalšího kontrolovat, zdali nedochází již jen k neoprávněnému čtení či jinému zacházení s osobními údaji (viz § 13 odst. 3 zákona o ochraně osobních údajů).“* Jak dále uvedl Městský soud v Praze: *„A toto pochybení je navýsost závažné i s ohledem na rozsah a předmět osobních údajů, které žalobce zpracovává (především údaje o zdravotním stavu pacientů), aniž by to subjekty osobních údajů mohly jakkoli ovlivnit.“*

Jak rovněž uvedl Městský soud v Praze: *„Ustanovení § 13 odst. 4 písm. c) zákona o ochraně osobních údajů přitom jednoznačně stanovilo, že již v samotném elektronickém záznamu (logu) musí být obsažen důvod zaznamenání či zpracování osobních údajů. Poukaz žalobce na možnost provést následně pohovor se zaměstnancem, jenž přistupoval do databáze, a takto zjistit důvod jeho přístupu neobstojí, neboť zjevně nerespektuje znění citovaného ustanovení zákona. A stejně tak nectí cíle přijaté právní úpravy, kterými je, jak bylo shora rozvedeno, především možnost snadné průběžné i následné kontroly, zdali nedochází k neoprávněnému přístupu do databáze. A v předmětné věci navíc bylo prokázáno, že žalobce ani tuto průběžnou či následnou kontrolu neprováděl dostatečně, respektive že takováto kontrola nepřinesla průkazné závěry, jak ukázal případ stěžovatelky.*

Na odpovědnosti žalobce pak nemůže nic měnit, že není vývojářem předmětného informačního systému, neboť bylo jeho povinností zajistit, aby jím využívaný systém splňoval zákonné požadavky. Jak přitom vyplynulo z provedené kontroly, doposud fungující systém umožňoval zadat důvod přístupu, uživatel systému však nebyl povinen vždy a za všech okolností tento důvod před přístupem k citlivým údajům uvést. Úpravu systému, aby se tato možnost stala povinností, nelze dle soudu považovat za nesplnitelný technický požadavek.“

Poradenská a konzultační činnost

Výjimečnost uplynulého roku se promítla i do konzultační agendy zcela novým tématem, které ukázalo, jak úzce je ochrana osobních údajů spojena s každodenním životem. V souvislosti s pandemií koronaviru totiž vyvstaly zejména otázky, zda a do jaké míry je zaměstnavatel oprávněn zjišťovat a případně dále zpracovávat informace o aktuálním zdravotním stavu zaměstnance, resp. jakým způsobem má přitom spolupracovat s orgány ochrany veřejného zdraví.

Stěžejním tématem covidové problematiky však byly konzultace s Ministerstvem zdravotnictví o realizacích aplikací eRouška, užívaných k trasování nakažených osob. Hlavním, do konce roku přetrvávajícím, problémem se ukázala být absence právní úpravy tohoto nového typu zpracování, která by dala odpovídající záruky uživatelům těchto aplikací, že jejich údaje nebudou zneužity k jiným účelům. Řešení tohoto širokou veřejností citlivě vnímaného tématu komplikuje z hlediska mezinárodní interoperability i rozdílnost přístupu v jednotlivých zemích EU, a to jak s ohledem na rozsah zpracovávaných údajů, tak s ohledem na právní základ, na němž je zpracování postaveno.

Z celkového počtu 1571 písemných dotazů však stejně jako v předchozích letech nejvíce, přibližně čtvrtinový podíl, zaujímala problematika sledování prostřednictvím kamerových systémů. Frekventovanost tématu dokládá, jak je při provozování těchto systémů často obtížné sladit oprávněný zájem na příležitostné identifikaci pachatele protiprávního jednání se zákazem neoprávněného pořizování záznamů o soukromém životě člověka, stanoveného občanským zákoníkem.

K dalším častým tématům písemných dotazů veřejnosti patřilo:

- zpracování osobních údajů v činnosti obcí včetně informování veřejnosti o jednání rady a zastupitelstva obce,
- zpracování osobních údajů v prostředí internetu včetně zveřejňování na sociálních sítích,
- dlužnické registry vedené na základě zákona o ochraně spotřebitele,
- problematika distanční výuky ve školách,
- oblast klinického hodnocení léčiv a
- zpracování osobních údajů členů různých spolků či společenství vlastníků.

Jen přibližně pět procent dotazů zaslali pověřenci pro ochranu osobních údajů.

Na Úřad se často obracejí veřejné subjekty jako obce či úřady prostřednictvím starostů, tajemníků či vedoucích organizačních úvarů, i přestože by kontaktní osobou v takovém případě měl být pověřenec pro ochranu osobních údajů.

To může ukazovat i na rozdílnou odbornou úroveň pověřenců a obtížnost při jejich velkém počtu u veřejnoprávních subjektů dostát požadavku znalostí a praxe v oblasti ochrany údajů stanoveného obecným nařízením. Příčinou může být i snížená dostupnost pověřence způsobená tím, že současně působí i u několika desítek místně vzdálených správců.

Pandemická situace umožnila během roku pouze osm osobních konzultací se správci osobních údajů v sídle Úřadu, převážně v letních měsících, z toho tři s ústředními orgány státní správy, jeden s městským úřadem a čtyři se soukromými subjekty.

Ani v roce 2020 Úřad neobdržel žádnou žádost o předchozí konzultaci, která by splňovala náležitosti článků 35 a 36 obecného nařízení včetně posouzení vlivu na ochranu osobních údajů podle Úřadem doporučených postupů. Jedním z důvodů může být to, že mnozí správci zaměňují posouzení vlivu na ochranu osobních údajů jako riziko pro práva a svobody subjektů údajů, které vyplývají i z operací prováděných samotným správcem, za riziko z hlediska zabezpečení před únikem dat.

Pracovníci oddělení konzultací se zúčastnili několika akcí týkajících se ochrany osobních údajů pořádaných jinými institucemi. Jednalo se o:

- setkání pověřenců ve státní správě uspořádané v budově ČSSZ,
- jednání k právní úpravě zákona č. 185/2020 Sb., o některých opatřeních ke zmírnění epidemie koronaviru, na Ministerstvu pro místní rozvoj,
- porady odboru veřejné správy, dozoru a kontroly Ministerstva vnitra s orgány státní správy,
- jednání s veřejným ochráncem práv a jeho zástupkyní,
- kulatý stůl k problematice rozhodování o své národnosti a
- jednání na Českém statistickém úřadu ke sčítání lidu v roce 2021.

Společně s pracovníky dalších útvarů Úřadu byl v Pardubicích v září uspořádán seminář pro pověřence na téma Veřejné subjekty v ČR po dvou letech s obecným nařízením.

Ve spolupráci s tiskovým oddělením byly na webových stránkách průběžně doplňovány jednotlivé rubriky o odpovědi na aktuální často kladené otázky.

Pracovník oddělení konzultací rovněž zabezpečoval provoz na telefonické informační lince.

Oddělení také umožnilo praxi třem studentům práv se zájmem o oblast ochrany osobních údajů. V rámci oboustranně prospěšné spolupráce jejich pomoc využilo především při psaní odpovědí na písemné dotazy.

ANALYTICKÁ ČINNOST

Analytické oddělení se podobně jako v minulých letech podílelo na řešení komplexních otázek ochrany osobních údajů, které často zahrnují jak poměřování více práv, tak definování zásad a podmínek potřebných pro soulad s pravidly ochrany osobních údajů v obecném nařízení. Různorodá činnost v roce 2020 zahrnovala například monitorování ochrany osobních údajů na evropské úrovni či

zpracování srovnávacích analýz. Z těchto činností vystoupila do popředí již v březnu 2020 činnost spojená s ochranou dat během pandemie.

Analytická činnost Úřadu během pandemie

Ochrana osobních údajů představovala důležité téma během pandemie COVID-19. Důvodem je to, že orgány státu (Ministerstvo zdravotnictví, hygienické stanice, krajské úřady) odpovědné za prosazování či monitorování hygienických opatření jsou povinny během pandemie provádět řadu činností založených na zpracování osobních údajů s cílem zajišťovat veřejné zdraví. V těchto situacích je třeba nalézt vhodnou rovnováhu mezi prováděním nezbytných opatření a ochranou osobních údajů, na kterou nelze rezignovat ani v době pandemie. Jako příklad lze uvést aplikace v rámci Chytré karantény včetně trasovací aplikace eRouška, které mohou být doplněny o rozměr interoperability, vedení zdravotních registrů či registrační systémy pro nahlašování očkování obyvatel. Zdravotní údaje přitom představují zvláštní kategorii osobních údajů, jejichž zpracování je omezené na výjimky podle čl. 9 obecného nařízení. Při řešení těchto otázek Úřad poskytoval maximální součinnost. Zvláštní pozornost vyžadovalo používání mobilních trasovacích aplikací, kterým se věnuje i další text.

Pandemie jako evropské téma

Rovněž v Evropské unii (EU) byla ochrana základních práv během pandemie nastolena jako důležité téma. K tomuto cíli se členské státy EU nehlásily jen slovně, ale ihned po propuknutí pandemie spolupracovaly na různých pracovních úrovních,[2] a tato činnost stále pokračuje. Vznikly dokumenty, které mohly být využity i jako metodické návody, například při nastavení sledovacích a trasovacích aplikací. Pro oblast ochrany osobních údajů byla relevantní zejména stanoviska, pokyny a odpovědi Sboru pro ochranu osobních údajů (EDPB). Řada užitečných dokumentů byla přijata rovněž pro oblast zdravotnictví. Byť zde není výlučná působnost EU, byla zřejmá potřeba koordinace, jejímž nástrojem byla síť pro přeshraniční spolupráci eHealth.[3] Pracovní materiály sloužily k nalezení rovnováhy mezi hodnotami, jíž je na jedné straně ochrana zdraví v době pandemie, na druhé straně demokratické hodnoty právního státu včetně práva na soukromí a ochranu osobních údajů. Ačkoli výše zmíněné dokumenty nejsou právně závazné, jde o materiály užitečné, praktické a návodné.

V tomto ohledu lze upozornit na Pokyny EDPB 4/2020 k používání lokalizačních údajů a nástrojů k vysledování kontaktů v souvislosti s rozšířením onemocnění COVID-19 a některá další stanoviska EDPB,[4] která později mohla být využita i v rámci Evropské federační brány.[5] Jde o novou službu, kterou zřídily členské státy spolu s Evropskou komisí (EK) za účelem umožnění vzájemné přeshraniční komunikace vnitrostátních aplikací v Evropě. Cílem bylo, aby uživatelé mohli používat i v zahraničí jen jednu aplikaci, která je bude varovat, pokud se dostanou do kontaktu s někým, kdo měl pozitivní test na COVID-19. Potenciální varování mohou být zvlášť užitečná pro uživatele v příhraničních oblastech, zejména pokud pravidelně cestují do práce. Na projektu interoperability se již začalo pracovat, ale bude se zavádět postupně.

Aplikace principů ochrany osobních údajů při posuzování mobilních aplikací

Při posuzování trasovacích mobilních aplikací je z pohledu ochrany osobních údajů vždy třeba aplikovat platnou právní úpravu na konkrétní aplikaci, což prakticky znamená potřebu zohlednit jak zásady, tak další povinnosti vyplývající z obecného nařízení, z nichž lze zejména zmínit:

---

[2] Na nejvyšší úrovni se jednalo o Evropskou rada a Radu EU, Evropskou komisi a Sbor pro ochranu osobních údajů. K výčtu lze pro úplnost přiřadit doporučení ENISA, které se zabývá metodikou kyberbezpečnosti.

[3] Takovým dokumentem je například „eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps" – v překladu "Pokyny Sítě pro digitální zdravotnictví členským státům EU a Evropské komisi ke specifikacím interoperability přeshraničních řetězců předávání mezi schválenými aplikacemi".

[4] Prohlášení o zpracování osobních údajů v souvislosti s výskytem onemocnění COVID-19
Prohlášení o dopadu interoperability aplikací pro trasování kontaktů na ochranu osobních údajů

[5] https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_cs.

— **Transparentnost**. Tento princip je z pohledu ochrany osobních údajů klíčovým. Uživatelé musí vždy rozumět tomu, jakých osobních údajů se zpracování týká, musí dostat srozumitelnou a jednoznačnou informaci o zpracování jejich osobních údajů a musí jim zůstat kontrola nad jejich údaji. Nejpozději v okamžiku získání osobních údajů musí být uživatelé informováni o podmínkách a rozsahu zpracování dat. Vhodným návodem v tomto směru jsou pokyny EDPB týkající se transparentnosti.[6]
— **Právní základ**. Obecně platí, že v případě trasovacích aplikací může existovat více právních důvodů zpracování pro účel varování před nakaženými osobami. Nicméně nejčastěji přichází v úvahu jako právní základ zpracování právní důvod podle čl. 6 odst. 1 písm. e) obecného nařízení, tj. zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo čl. 6 odst. 1 písm. a) obecného nařízení, tj. zpracování na základě souhlasu.[7] Členské státy EU využívají oba právní důvody. Každý z těchto důvodů však vyžaduje splnění odlišných podmínek. V případě použití veřejného zájmu je potřebné přizpůsobit vnitrostátní právo tak, aby takový úkol ve veřejném zájmu nebo při výkonu veřejné moci jednoznačně stanovilo. V případě souhlasu zase musí být splněny požadavky pro zpracování osobních údajů ve smyslu pokynů EDPB o souhlasu.[8] To znamená, že souhlas musí vyjadřovat svobodné, konkrétní, informované a jednoznačné svolení subjektu údajů ke zpracování osobních údajů. Musí být také splněna podmínka, že souhlas lze kdykoli odvolat.
— **Minimalizace dat**. Obecně platí, že shromažďování osobních údajů se nesmí uskutečňovat nad rámec nezbytnosti. Rovněž nastavení doby uchovávání telekomunikačních údajů nesmí vést k jejich shromažďování na dobu delší, než je nezbytné. Nedoporučuje se přitom shromažďovat lokalizační údaje, jako je tomu u *data retention*, protože k dosažení účelu sledovanému trasovacími aplikacemi postačují anonymizované údaje zaznamenávající přiblížení se k pozitivně testované osobě na určitou vzdálenost. V každém případě by měla být předem stanovena minimální nezbytná data a doba jejich uchovávání. Tyto údaje by měly být sděleny uživateli před zahájením zpracování jeho dat.
— **Určení správce**. Velice důležité je stanovení role jednotlivých aktérů v procesu zpracování údajů. Pro každé zpracování musí být určen správce, případně společný správce a zpracovatel. Tyto role musí být definovány a sděleny subjektu údajů. Pokud údaje zpracovává zpracovatel, správce s ním uzavře zpracovatelskou smlouvu, jejíž podmínky blíže upravuje čl. 28 obecného nařízení.
— **Posouzení vlivu (DPIA)**. Pokud zpracování osobních údajů může mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob, je správce povinen provést před zamýšleným zpracováním posouzení vlivu na ochranu osobních údajů.[9] Posouzení vlivu je nástroj, který předem mapuje zpracovávání osobních údajů, a nastavuje je tak, aby bylo v souladu se zásadami ochrany osobních údajů. V případě eRoušky a Chytré karantény bylo podle čl. 35 obecného nařízení zpracování posouzení vlivu pravidlem.
— **Uplatňování práv subjektů údajů**. Rozšíření práv subjektů údajů je třeba považovat za největší přínos obecného nařízení, pokud jde o fyzické osoby. Mezi tato práva patří právo na přístup k osobním údajům, právo na informace o jejich zpracování, právo na výmaz a právo na podání námitek. Výkon těchto práv musí být umožněn i v případě mobilních trasovacích aplikací.

Interoperabilita mobilních aplikací z pohledu ochrany osobních údajů

V rámci EU je považováno za žádoucí umožnit fungování interoperabilních trasovacích aplikací, přičemž na tomto úkolu se začalo pracovat od podzimu 2020 a stále se pokračuje.[10] Interoperabilita kontaktních trasovacích aplikací v EU má být založena na národních aplikacích, aby tak byla zvýšena

[6] Pokyny k transparentnosti podle nařízení 2016/679/ES (WP260rev01).

[7] Pokyny 04/2020 k používání lokalizačních údajů a nástrojů k vysledování kontaktů v souvislosti s rozšířením onemocnění COVID-19 ze dne 21. dubna 2020.

[8] Pokyny k souhlasu podle nařízení 2016/679.

[9] Více v Pokynech k posouzení vlivu na ochranu údajů a stanovení, zda je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko pro účely Nařízení 2016/679.

[10] Pro úplnost je však třeba uvést, že některé státy se k této iniciativě nepřipojily. Jedná se o Bulharsko, Francii a Maďarsko.

efektivitatrasování prostřednictvím již existujících opatření. Dozorové úřady obecně nebrání zavedení interoperability, požadují však, aby nastavení trasovacích aplikací bylo v souladu s pravidly ochrany osobních údajů.[11]

Rovněž v ČR se při zadaní úkolu zpracování osobních údajů v rámci interoperabilní eRoušky ČR vycházelo z toho, že Interoperabilita je žádoucím cílem v rámci EU. Je definována jako *„schopnost vyměňovat si minimální nezbytné informace uživateli individuálních aplikací bez ohledu na to, kde se v EU nachází, a být v určitém období varováni, pokud se nachází v blízkosti jiného uživatele, který rovněž používá aplikaci a byl testován jako pozitivní na COVID-19."*

V různých členských státech EU existují kontaktní trasovací aplikace s různými přístupy, přičemž zajištění interoperability různých implementací je technicky náročné a vyžaduje dodatečné finanční a technologické zajištění. Za účelem zajištění zpracování minimálního množství dat, jak to požaduje obecné nařízení, se vývojáři kontaktních trasovacích aplikací musí dohodnout na společném protokolu a kompatibilních datových strukturách a vytvořit společný rámec, naopak rozdílné přístupy mohou v praxi zavedení interoperability znemožnit. V praxi je třeba věnovat pozornost jak obecným požadavkům, tak řadě konkrétních opatření chránících osobní údaje, z nichž na některé lze upozornit:

— Postupy a pravidla týkající se interoperability musí být jak v souladu s pravidly určenými orgány ochrany veřejného zdraví, tak musí zvažovat potenciální dopady do oblasti soukromí a bezpečnostních implikací a v tomto ohledu přijmout vhodné záruky. V oblasti ochrany osobních údajů lze v podrobnostech u těchto otázek odkázat na obecné nařízení a již zmíněné pokyny EDPB 4/2020 (požadující transparentnost a zákonnost zpracování, minimalizaci dat, určení správce, posouzení vlivu a další kritéria, viz výše). Taková opatření jsou součástí komplexní strategie veřejného zdraví pro boj s pandemií.
— Obecně platí, že aplikace pro vysledování kontaktů a varování se používají výlučně dobrovolně, jsou založeny na technologii detekce blízkých zařízení (zpravidla *Bluetooth*), respektují soukromí uživatelů a neumožňují sledování polohy osob.[12] Cíl interoperability přitom nesmí být používán jako argument pro rozšiřování shromažďování osobních údajů nad to, co je skutečně nezbytné.
— Pokud se zavádí interoperabilní aplikace nad rámec dřívější národní aplikace, jde o dodatečnou funkcionalitu, která povede k dalšímu zpracování a zveřejnění dat dalším subjektům. V případě takového rozšíření aplikace je nezbytné informovat subjekty údajů o dodatečném zpracování jejich dat.
— Důležitou otázkou je, zda údaje zpracovávané v rámci mobilních trasovacích aplikací jsou anonymizované či pseudonymizované. I když by bylo žádoucí, aby tyto aplikace pracovaly s anonymizovanými údaji (potom už by se o osobní údaje nejednalo), obvykle pracují s pseudonymizovanými osobními údaji. Prakticky to znamená, že musí splňovat požadavky pro ochranu osobních údajů stanovené obecným nařízením.

Závěrem lze shrnout, že zajištění požadavků souvisejících s ochranou osobních údajů v době pandemie není jednoduchým úkolem, jde o úkol komplexní a náročný. Pokud ovšem má veřejnost s důvěrou využívat nástroje, jako je mobilní trasovací zařízení, je nutné věnovat zpracování osobních údajů náležitou pozornost. Vzhledem k vývoji pandemie se stále jedná o aktuální úkol, na němž bude Úřad připraven spolupracovat.

[11] EDPB dokonce vyzval ke vzniku interoperabilního rámce, který byl přijat sítí eHealth dne 13. května 2020. Dokument „eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps" – v překladu „Pokyny Sítě pro digitální zdravotnictví členským státům EU a Evropské komisi ke specifikacím interoperability přeshraničních řetězců předávání mezi schválenými aplikacemi".

[12] Nemusí být využívány lokalizační údaje, ale postačí anonymní údaje o blízkosti pozitivně testované osoby.

Legislativa

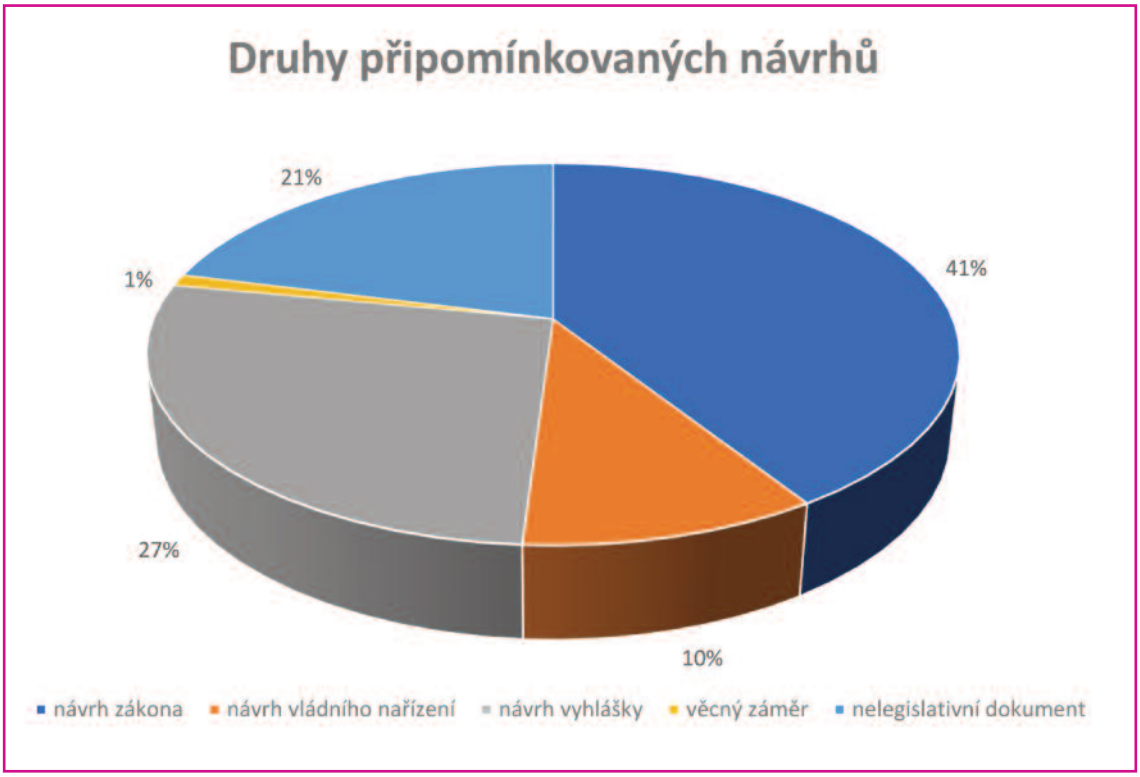
V roce 2020 v souvislosti s pandemií COVID-19 byla řešena potřeba přizpůsobit právní řád boji proti šíření SARS-CoV-2, a to především prostřednictvím dvou předloh právních předpisů, konkrétně návrhem zákona o mimořádných opatřeních při epidemii onemocnění COVID-19 [v roce 2020] (dále jen „zákon o covidu", známý též pod názvem „pandemický zákon") – sněmovní tisk 859 a návrhem zákona, kterým se mění zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a další související zákony, který mimo jiné předpokládá vytvoření ústředního orgánu – Státní hygienické služby, jež má být nástupnickou organizací pro krajské hygienické stanice a hygienickou stanici hlavního města Prahy (dále jen „zákon o SHS").

Zákon o covidu nebyl s Úřadem projednán v rámci standardního připomínkového řízení.[13] Ocenit však lze, že uzákoněním eRoušky a call center tato zpracování osobních údajů dostávají řádný právní základ – článek 6 odst. 1 písm. e) obecného nařízení – nutno ale podotknout, že absentují dostatečné záruky ochrany osobních údajů.

[13] Poslanecká sněmovna se jím nezabývala ani v I. čtení. Vláda nicméně předložila sněmovně návrh zákona dne 15. února 2021, který byl rozeslán jako sněmovní tisk 1158 a který byl až na detaily shodný se sněmovním tiskem 859. Následně po jeho projednání v legislativním procesu byl zákon vyhlášen dne 26. února 2021 ve Sbírce zákonů v částce 38 pod číslem 94/2021 Sb., o mimořádných opatřeních při epidemii onemocnění COVID-19 a o změně některých souvisejících zákonů.

Rovněž v zákoně o SHS absentují vhodné záruky ochrany osobních údajů Státní hygienickou službou, což je důsledek nedostatečného posouzení vlivu na ochranu osobních údajů (DPIA).

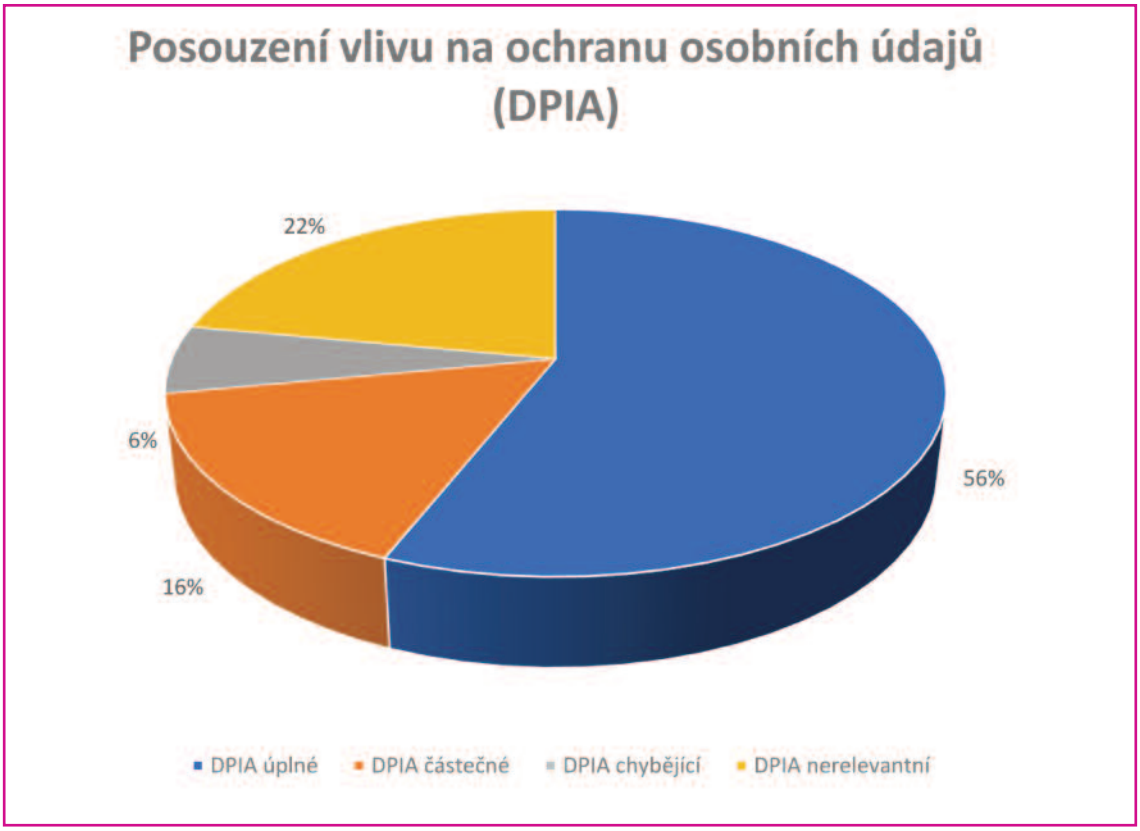
Naproti tomu návrh zákona o elektronizaci zdravotnictví (angl. *eHealth*), který ÚZIS jako autor předlohy s Úřadem od srpna 2018 aktivně projednával, byl sice nadmíru redukován, ale i tak postaví, bude-li schválen Parlamentem ČR, dobré základy pro identifikaci pacientů, zdravotníků a poskytovatelů v reálném čase, a tím i infrastrukturu pro zaručené sdílení zdravotní dokumentace.



Úřad aktivně spolupracuje se Sdružením místních samospráv ČR. Na jeho žádost se zabýval komplikovanými intertemporálními účinky nálezu Ústavního soudu č. 149/2020 Sb. ve věci zveřejňování oznámení místních veřejných funkcionářů o majetku a střetu zájmů. Ministerstvu spravedlnosti bylo doporučeno přijmout opatření k ochraně osobních údajů ještě před účinností nálezu Ústavního soudu. Podstata problému spočívala v tom, že ÚS jako negativní zákonodárce sice zrušil protiústavní ustanovení zákona o střetu zájmů, ale účinnost tohoto rozhodnutí odložil o téměř 11 měsíců a nedal přitom žádná vodítka, jak v mezidobí postupovat. Úřad proto doporučil Ministerstvu spravedlnosti jako správci registru oznámení podmínit přístupy do něj, například poskytnutím funkční e-mailové adresy, či je jinak omezit, například znemožněním hromadného stahování dat.

Legislativní posouzení vlivu na ochranu osobních údajů (DPIA)

Jedním z nejdůležitějších úkolů Úřadu v legislativní oblasti je dbát na kvalitu posouzení vlivu na ochranu osobních údajů podle čl.35 obecného nařízení, v dikci legislativních pravidel vlády od 1. ledna 2013 „zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů" v návrzích právních předpisů.



Jak vyplývá z grafu, u šesti procent návrhů DPIA absentuje zcela, ačkoliv připraveno být mělo. U celých 16 procent návrhů, které Úřad připomínkoval, jsou větší či menší vady. Jedním z největších nešvarů jsou apodiktická (nezdůvodněná) tvrzení. Jindy předkladatel chce za každou cenu dostat absolutorium, že má vše v pořádku, ačkoliv podstatou DPIA není výrok, nýbrž přezkoumání rizik pro subjekty údajů a popis nástrojů použitých k jejich umenšení či úplné eliminaci.

Za příklad dobré praxe lze považovat DPIA u návrhu zákona o elektronizaci zdravotnictví jako vzor zhodnocení dopadu na ochranu osobních údajů, které je konkrétní, a DPIA u návrhu *re-use* novely zákona o svobodném přístupu k informacím jako vzor abstraktního zhodnocení dopadu na ochranu osobních údajů.

Ostatní významné návrhy

Úřad byl osloven s žádostí o stanovisko ohledně povinnosti exekutora plošně nahrávat telefonní hovory v návrhu novely občanského soudního řádu a exekučního řádu (sněmovní tisk 545). Původní pozměňovací návrh považoval Úřad za rozporný s ochranou osobních údajů. Proto byl požádán, aby vypracoval alternativní. Úřad tak učinil a navrhl tyto záruky ochrany osobních údajů: zabezpečení nahrávek před neoprávněným přístupem, omezení oprávnění na přístup, ochranu soukromí třetích osob a zákonné stanovení konkrétní přiměřené doby uchování záznamů.

Zásadní změnou je návrh zcela nového zákona o občanských průkazech.[14] Návrh zákona přináší řadu významných změn, mezi něž patří zejména přehodnocení obsahu údajů uvedených v občanských

[14] Sněmovní tisk 1043.

průkazech (upouští od možnosti vedení titulu nebo vědecké hodnosti v občanském průkazu, neboť titul ani vědecká hodnost nepředstavují údaje, kterými by občan prokazoval svoji totožnost) a např. zavedení biometrických údajů do občanských průkazů podle nařízení Evropského parlamentu a Rady (EU) 2019/1157 ze dne 20. června 2019 o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie a jejich rodinným příslušníkům, kteří vykonávají své právo volného pohybu. Cílem nové právní úpravy je též reagovat na potřebu zajištění rozvoje eGovernmentu, tedy na nutnost zajistit co nejširší dostupnost prostředku pro elektronickou identifikaci a autentizaci vzájemně uznatelného podle nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Na nových občanských průkazech nebude rodné číslo. Úřad podporuje jeho postupné vyřazení jako všeobecného identifikátoru. Rodné číslo má být v soukromém sektoru nahrazeno bezvýznamovým směrovým identifikátorem (BSI) v návrhu novely zákona o právu na digitální služby.

Neméně významné jsou chystané změny zákona o svobodném přístupu k informacím. Ministerstvo vnitra vedle návrhu novely, kterou projednává Poslanecká sněmovna, připravilo návrh transpozice směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru (angl. *re-use*). Jeho součástí je na návrh BIS a KPR omezit působnost Úřadu. Ministerstvo vnitra tomuto návrhu vyhovělo a navrhuje vyloučit působnost Úřadu u Kanceláře Poslanecké sněmovny, Kanceláře Senátu, Kanceláře prezidenta republiky, Kanceláře Veřejného ochránce práv, Ústavního soudu, Nejvyššího soudu, Nejvyššího správního soudu, Nejvyššího státního zastupitelství a zpravodajských služeb. Jedná se o hlubší promítnutí principu dělby moci, který ve stávajícím znění není zcela respektován, a to ve vztahu k moci soudní, zákonodárné a hlavě státu. Další výjimky mají opodstatnění podle povahy činnosti vykonavatele veřejné správy nebo ohrožení jeho nezávislosti.

Další příprava a implementace unijního práva

Mimořádně významný je návrh novely zákona o elektronických komunikacích, který by vedle transpozice evropského kodexu pro elektronické komunikace měl opravit spornou transpozici směrnice o soukromí a elektronických komunikacích. Návrh nařízení o respektování soukromého života a ochrany osobních údajů v elektronických komunikacích (ePR), který Evropská komise navrhla 10. ledna 2017, totiž nebyl schválen ani za německého předsednictví EU. Za zřejmě nejvíce významné lze považovat, že návrh novely v regulaci *cookies* odstraňuje spory o tom, zda se jejich režim i v českém právním řádu řídí režimem „přihlášení" (angl. *opt-in*), tj. předchozího aktivního souhlasného projevu vůle, změnou dikce právní normy.

Ačkoliv Úřad německou podobu ePR podpořil, s podporou členských států EU se nesetkala. Nejspornějšími otázkami ePR zůstává: zadržení údajů (angl. *data retention*), zpracování metadat, zákaz *cookie walls* a přílišný rozsah věcné působnosti ePR – na rozdíl od původní idey upravit pouze přenos dat. Vzhledem k množství nevyřešených otázek a složitosti vyjednávání byla velká očekávání, s jakým návrhem textu přijde portugalské předsednictví na počátku roku 2021.[15]

Úřad se zároveň intenzivně zabýval návrhem nařízení Evropského parlamentu a Rady o dočasné odchylce od některých ustanovení směrnice Evropského parlamentu a Rady 2002/58/ES, pokud jde o používání technologií poskytovateli interpersonálních komunikačních služeb nezávislých na číslech ke zpracování osobních a jiných údajů pro účely boje proti pohlavnímu zneužívání dětí na internetu (CSAMR). Jeho podstatou je automatické plošné prověřování veškeré elektronické komunikace, včetně chatu. Ačkoliv Úřad plně podporuje boj proti pohlavnímu zneužívání dětí na internetu, v českém kontextu jako jeden z mála upozornil na to, že plošné prověřování veškeré elektronické komunikace je v rozporu s listovním tajemstvím a CSAMR tedy nepodpořil. Shodný názor měl Evropský inspektor ochrany údajů a klíčový výbor Evropského parlamentu – pro občanské svobody, spravedlnost a vnitřní věci (LIBE).

[15] Výbor velvyslanců členských států EU (COREPER) 10. února 2021 schválil mandát pro jednání s Evropským parlamentem.

Zahraniční spolupráce

Zahraniční činnost Úřadu, jejíž těžiště spočívá ve členství v Evropském sboru pro ochranu osobních údajů (EDPB), byla ovlivněna situací související s COVID-19. Došlo k technické změně ve způsobu práce, kdy se osobní schůze a jednání od začátku března 2020 přesunuly do virtuálního světa (telefonické konference a videokonference). Celkem bylo v roce 2020 svoláno 27 plenárních zasedání, ve valné většině formou videokonference. Zasedání odborných skupin EDPB, ve kterých má Úřad své delegáty, dosáhla souhrnného počtu 108, z převážné části opět distančně. V porovnání s minulými lety tak po přechodu na vzdálená zasedání došlo k podstatnému nárůstu jejich četnosti.

Změn doznalo i zaměření činnosti EDPB. Bylo totiž třeba operativně určit a popsat, jaké dopady do ochrany osobních údajů a soukromí mohou mít nejrůznější opatření postupně přijímaná v rámci boje s pandemií, a následně nabídnout řešení ve formě zásad a vodítek pro správce osobních údajů shromažďovaných během uplatňování zmíněných opatření.

EDPB tak vydal řadu dokumentů:

- Prohlášení o zpracování osobních údajů v souvislosti s výskytem onemocnění COVID-19 (19. března 2020) představovalo první rychlou reakci na vzniklou situaci.
- Dopis Evropské komisi ohledně návrhu Pokynů k aplikacím podporujícím boj proti pandemii COVID-19 (14. dubna 2020). Ten vznikl na žádost Evropské komise o stanovisko k návrhu jejího dokumentu. EDPB sestavil soubor doporučení pro soulad aplikací s principy ochrany dat implikující důležitý apel, aby po odeznění pandemie byla data takto získaná smazána nebo anonymizována.

- Pokyny 03/2020 ke zpracování údajů o zdravotním stavu pro účely vědeckého výzkumu v souvislosti s rozšířením onemocnění COVID-19 (21. dubna 2020).
- Pokyny 04/2020 k používání lokalizačních údajů a nástrojů k vysledování kontaktů v souvislosti s rozšířením onemocnění COVID-19 (21. dubna 2020).
- Prohlášení o omezení práv subjektů údajů v souvislosti se stavem nouze v členských státech (2. června 2020) – apel na dodržování zásad ochrany dat i za mimořádných podmínek.
- Prohlášení o dopadu interoperability aplikací pro trasování kontaktů na ochranu osobních údajů (16. června 2020).
- Prohlášení o zpracování osobních údajů v souvislosti se znovuotevřením hranic schengenského prostoru po rozšíření onemocnění COVID-19 (16. června 2020). EDPB v něm připomněl základní zásady ochrany dat, na které by členské země měly v daném procesu pamatovat.

Na pozadí vzniklé situace pokračovala za aktivní účasti Úřadu činnost EDPB podle pracovního plánu. Z řady schválených materiálů stojí za zmínku například:

- Pokyny 03/2019 ke zpracování osobních údajů prostřednictvím videotechniky (29. ledna 2020). Na vypracování tohoto dokumentu se Úřad podílel jako člen řešitelského týmu.
- Pokyny 05/2020 k souhlasu podle nařízení 2016/679 (4. května 2020). Jedná se o revizi staršího dokumentu, ještě z dílny bývalé Pracovní skupiny podle článku 29 (WP29).

Úřad vystupoval prostřednictvím svých zástupců v tematicky specializovaných expertních skupinách EDPB v celkem devíti případech jako člen řešitelského týmu při práci na materiálech, jež mají napomáhat správcům a zpracovatelům dosahovat souladu se zásadami ochrany osobních údajů a jednotlivcům pak posilovat povědomí o svých právech.

Nadále se podílel na činnosti Poradního výboru k Úmluvě 108 (T-PD) při Radě Evropy, kde má svého delegáta. Předmětné aktivity však byly poněkud utlumeny vzhledem k pandemické situaci a realizovaly se výhradně prostřednictvím výměny e-mailové korespondence a videokomunikace. Z věcného hlediska se pokračovalo v předchozích tématech, jako je ochrana osobních údajů v rámci vzdělávacího procesu, digitální identita a také problematika evaluace naplnění podmínek Úmluvy 108.

Další, specificky zaměřené informace o činnostech s mezinárodním rozměrem, jsou podrobně popsány v dalších kapitolách.

V rámci přeshraniční spolupráce Úřad obdržel 105 žádostí ve smyslu čl. 61 obecného nařízení. Šlo především o případy dožádání či výměny informací ke konkrétním případům a stížnostem. Řada z nich byla legislativního a výkladového charakteru. Úřad sám poté odeslal tři takové žádosti.

Pokud jde o případy mechanismu jediného kontaktního místa (one-stop-shop), inicioval Úřad na základě obdržených stížností celkem čtyři procedury podle čl. 56 obecného nařízení, v jejichž rámci navrhl příslušnost některého ze zahraničních dozorových úřadů jakožto vedoucího dozorového úřadu.

Do role vedoucího dozorového úřadu byl naopak navržen v devíti případech, přičemž doposud přijal pouze jeden z nich. Na základě provedeného šetření totiž dospěl k závěru, že prováděné zpracování svou charakteristikou nenaplňuje přeshraniční zpracování, stížnost byla zjevně nedůvodná nebo nebylo o vedoucím dozorovém úřadu dosud rozhodnuto.

V případech, kdy se nejednalo o přeshraniční zpracování ve smyslu čl. 4 odst. 23 obecného nařízení, byly tyto stížnosti prošetřeny na národní úrovni mimo režim tzv. one-stop-shop mechanismu, kdy Úřad zůstává taktéž během svého šetření v kontaktu se zahraničním úřadem postoupivším stížnost, avšak tato komunikace probíhá v méně formalizované podobě a zahraniční úřad nepožívá některých práv jako v případech skutečného one-stop-shop.

Úřad se též podílel (prostřednictvím delegátů v několika expertních skupinách a v plénu) na přijetí prvního závazného rozhodnutí EDPB (čl. 65 obecného nařízení).

KODEXY CHOVÁNÍ

Dodržování kodexů chování je vedle certifikačních mechanismů dalším z dobrovolných nástrojů pro správce nebo zpracovatele osobních údajů pro zajištění souladu s obecným nařízením.

Úřad v listopadu 2019 odeslal návrh požadavků pro akreditaci subjektů pro monitorování kodexů chování EDPB, ale kvůli určitým nejasnostem v přístupu k řešené problematice a požadavkům ze strany expertní podskupiny Compliance, eGovernment and Health při EDPB bylo nutno text upravit, což bylo uskutečněno v průběhu prvního pololetí 2020.

Úřad zároveň započal s přípravou vyhlášky k požadavkům pro akreditaci a až poté, co EDPB zahájí další kolo připomínkového řízení, mu ji předá ke stanovisku. Zároveň byly v roce 2020 zaslány připomínky ke dvěma návrhům kodexů chování původem z Francie a Belgie, týkající se cloudových služeb.

Právní úprava pro oblast kodexů a certifikace vyžaduje vydání dvou vyhlášek, úpravu zákona o zpracování osobních údajů a zákona o správních poplatcích, které Úřad v současné době připravuje.

OSVĚDČENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (CERTIFIKACE)

Vydání osvědčení je jedním z nástrojů pro správce nebo zpracovatele osobních údajů pro prokázání souladu jimi prováděných zpracování osobních údajů s obecným nařízením.

V říjnu 2019 Úřad vypracoval a následně předal materiál Kritéria pro vydávání osvědčení k posouzení EDPB, a to v rámci zajištění mechanismu jednotnosti. Na základě žádosti expertní podskupiny Compliance, eGovernment and Health, která materiál posuzuje, byly odděleny obě součásti materiálu, tj. požadavky na akreditaci subjektů pro vydávání osvědčení o ochraně osobních údajů a kritéria pro vydávání osvědčení s tím, že oba materiály budou posuzovány odděleně.

Upravené požadavky na akreditaci subjektů pro vydávání osvědčení o ochraně osobních údajů byly znovu v lednu 2020 odeslány k vypracování stanoviska, které Úřad obdržel v květnu, a ještě v tomto měsíci připomínky v něm uvedené zpracoval a odeslal EDPB. Následně došlo k upřesňování textu akreditačních požadavků na základě stanoviska a požadavků na plnění stanoviska od příslušné pracovní skupiny.

Právní úprava pro oblast certifikace vyžaduje vydání vyhlášky.

POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (DPIA)

Obecné nařízení předpokládá vypracování posouzení vlivu na ochranu osobních údajů v případech, kdy zpracování osobních údajů má za následek vznik vysokého rizika pro práva a svobody fyzických osob, a to s přihlédnutím k povaze, rozsahu, kontextu, účelům zpracování a využitím nových technologií. Obecné nařízení poskytuje v čl. 35, odst. 1 a odst. 3 několik vodítek k určení úrovně vysokého rizika a zároveň v odst. 4 a 5 ukládá povinnost dozorovým úřadům sestavit a zveřejnit seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu, případně (dobrovolně) vytvořit seznam druhů operací zpracování, u nichž není posouzení vlivu nutné provádět.

Úřad na svých webových stránkách zveřejnil již v roce 2019 dokument Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů. Oba seznamy, tedy pozitivní i negativní, byly předloženy a následně schváleny EDPB, jak ukládá obecné nařízení.

Pozitivní seznam vychází z materiálu *WP 248 Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování osobních údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679* a dále je pro potřeby správců rozpracovává. Pro hodnocení rizikovosti operací zpracování bylo možné buď sestavit přímo seznam vysoce rizikových zpracování (což by předpokládalo seznam neustále udržovat a aktualizovat) nebo zařadit operace zpracování mezi vysoce rizikové na základě kriteriální analýzy. Úřad zvolil druhou možnost a sestavil celkem deset kritérií. Pro hodnocení rizikovosti operací je tedy důležité, aby správce vyjádřil povahu zpracování osobních údajů pomocí charakteristik zpracování osobních údajů, které umožní každé zpracování popsat a následně pomocí těchto charakteristik zařadit mezi zpracování s vysokou mírou rizika pro práva a svobody subjektů údajů nebo ostatní zpracování.

Doporučený postup pro správce

Správce by měl ověřit, zda se jím zamýšlené zpracování osobních údajů nachází na seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů. Nejdříve tedy určit, zda nemá výjimku ze zpracování posouzení vlivu (například při zpracování osobních údajů orgánem veřejné správy, který tak činí na základě právního přepisu, by se mohlo stát, že bude zařazeno mezi zpracování s vysokou mírou rizika, nicméně při předkládání návrhu právního předpisu mohlo být součástí materiálu plnohodnotné posouzení vlivu a správce nemusí posouzení vlivu zpracovávat). Pokud správce výjimku nemá (nenalezne zpracování osobních údajů v negativním seznamu), potom by měl provést analýzu zpracování osobních údajů na základě Úřadem vytvořeného návodu v pozitivním seznamu. Jestliže správce dojde k závěru, že zpracování vykazuje vysokou mírou rizika pro práva a svobody subjektů údajů, musí přistoupit k provedení posouzení vlivu na ochranu osobních údajů (stanovit rizika, pravděpodobnost, zvolit technická a organizační opatření k jejich omezení).

Metodika obecného posouzení vlivu na ochranu osobních údajů

Samotné posouzení vlivu není snadnou záležitostí a pro jeho provedení by si měl správce zvolit metodiku, aby bylo zřejmé, na základě jakých postupů dosáhl stanoveného výstupu či cíle. Pro usnadnění plnění povinností správce podle obecného nařízení v oblasti posuzování rizik publikoval Úřad na konci roku 2019 k veřejné diskuzi Metodiku obecného posouzení vlivu na ochranu osobních údajů. Na základě připomínek a návrhů byla vypracována nová verze, která byla konzultována rovněž s Národním úřadem pro kybernetickou a informační bezpečnost a v listopadu 2020 uveřejněna na webových stránkách Úřadu.

Metodika je primárně určena pro potřeby správců, mohou ji však využívat i zpracovatelé (např. v rámci dodávky předloží typové posouzení vlivu pro jimi dodávané produkty), dále zpracovatelé legislativních návrhů i další odborníci na ochranu osobních údajů. Minimální obsah posouzení vlivu upravuje obecné nařízení. Metodika upřesňuje možný způsob provádění (a obsah) posouzení vlivu, který je rozdělen na čtyři etapy:

- 1. etapa – shromáždění informací o zpracování osobních údajů, včetně správcem uplatněných mechanismů pro doložení souladu s obecným nařízením.
- 2. etapa – analýza, zda je nezbytné provést posouzení vlivu,
- 3. etapa – provedení posouzení vlivu včetně posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
- 4. etapa – monitorování dodržování opatření a pravidelné revize posouzení vlivu.

Pokud k provedení posouzení vlivu dojde, správce získá dostatečné podklady pro to, aby mohl zavést přiměřená technická a organizační opatření. Tedy, aby jím uplatněná opatření nebyla nedostatečná (a tedy nezajišťující dostatečnou ochranu osobních údajů) nebo naopak nepřiměřeně silná (a tedy většinou i zbytečně drahá).

Posouzení vlivu je důležitým nástrojem zajištění principu odpovědnosti, protože pomáhá správcům plnit příslušné povinnosti. Na něj navazuje předchozí konzultace podle čl. 36 obecného nařízení. Tzv. konzultační povinnost správce je úzce spjata s povinností provedení posouzení vlivu. Cílem je poskytnout

efektivnější mechanismus dohledu nad zpracováními, která mohou představovat vysoké riziko. Doposud Úřad neregistroval žádnou žádost správce o předchozí konzultaci podle čl. 36 obecného nařízení.

Poznatky z praxe

V rámci výkonu konzultačních agend a legislativy bylo po účinnosti obecného nařízení shledáno, že jednotliví správci dostatečným způsobem a správně neprovádějí posouzení vlivu na ochranu osobních údajů. Často ani netuší, že v případě vysoce rizikového zpracování je provedení posouzení vlivu nezbytnou podmínkou pro samotnou realizaci zamýšleného zpracování.

Povinnost zpracovat DPIA je v obecném nařízení dána ve dvojí formě, jak soukromoprávním správcům, tak státu v rámci návrhu právních předpisů. Ve druhém (legislativním) případě se jedná o zásadní náležitost zpracování, protože podle § 10 zákona o zpracování osobních údajů mají subjekty (orgány veřejné moci), pokud je jim zpracování osobních údajů uloženo zákonem, udělenu výjimku z povinnosti zpracovat DPIA. Kvalitní a podrobné DPIA zpracované v rámci návrhu právních předpisů je tak od okamžiku účinnosti nového zákona jediným a nezbytným návodem pro instruování správců a zpracovatelů a vodítkem pro poznání, jaká rizika při zpracování osobních údajů hrozí, jaké jsou dopady do soukromí a jaká technická a organizační opatření mají při zpracováních uložených zákonem tyto subjekty přijmout.

V rámci připomínkových řízení k návrhům právních předpisů se ukázalo, že předkladatelé nemají v řadě případů příliš jasno, jak má takové posouzení vypadat.

Při přípravě právních předpisů je DPIA nutno přizpůsobit charakteru zpracování osobních údajů, v zásadě lze říci, že velmi podrobné DPIA by mělo být zpracováno tam, kde by byl i správce povinen ho zpracovat (dle seznamu operací, které mohou podléhat požadavku na zpracování posouzení vlivu na ochranu osobních údajů uveřejněnému na webu Úřadu) nebo tam, kde je nutno instruovat další subjekty, jaká technická a organizační opatření musí k ochraně osobních údajů přijmout.

Nejčastějšími problémy, které se vyskytují při návrzích DPIA v rámci právních předpisů, mohou být:

1. nedostatečný nebo nesprávný popis zpracování osobních údajů (chybné vymezení účelů zpracování osobních údajů, nedostatečný popis vazeb na okolní informační systémy nebo zpracování osobních údajů, nedostatečný popis zajištění práv subjektů údajů dle obecného nařízení nebo chybějící zdůvodnění, proč některá práva zajištěna být nemohou, nedostatečný popis toku osobních údajů apod.),
2. chybějící posouzení přiměřenosti/nezbytnosti prováděných operací zpracování (test proporcionality),
3. chybějící nebo nedostatečné posouzení rizik pro práva a svobody subjektů údajů (tj. co ohrožuje zpracování osobních údajů včetně kvantifikace závažnosti/významnosti rizika) a
4. nekonkrétní nebo nedostatečná specifikace technických a organizačních opatření, která mají rizika pro zpracování osobních údajů redukovat na přijatelnou úroveň.

V současné době se návrhy často omezují na slovní vyjádření, které neumožňuje posoudit zpracování osobních údajů v celém komplexu a neposkytuje dostatečné vodítko všem subjektům participujícím na zpracování osobních údajů.

PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO TŘETÍCH ZEMÍ

V režimu obecného nařízení vychází činnost Úřadu v oblasti předávání osobních údajů do třetích zemí z jednak z vlastní rozhodovací činnosti a jednak z výkladové a konzultační činnosti, vázané do značné míry na spolupráci s EDPB, a to především v rámci expertní podskupiny pro mezinárodní transfery, která v průběhu roku 2020 pokračovala v práci na několika zásadních výkladových dokumentech.

Mezi těmito dokumenty je nutné na prvním místě uvést Pokyny EDPB 2/2020 k čl. 46 odst. 3 písm. b) a čl. 46 odst. 2 písm. a) obecného nařízení pro předání osobních údajů ze strany orgánů veřejné moci a veřejných subjektů států Evropského hospodářského prostoru orgánům veřejné moci a veřejným subjektům mimo Evropský hospodářský prostor. EDPB pokyny v průběhu roku 2020 přijal a schválil jejich definitivní znění po vypořádání veřejné konzultace.

Z výkladových dokumentů rozpracovaných podskupinou pro mezinárodní transfery je nutné opětovně zmínit dokument o vzájemné souhře mezi čl. 3 a kapitolou V obecného nařízení, jehož definitivnímu vypracování brání zdlouhavé hledání výkladového konsensu jednotlivých dozorových úřadů.

Dopracovávaly se pokyny EDPB, které vydefinují nezbytné prvky, jež musejí být zahrnuty v těch kodexech chování a certifikačních schématech, které budou určeny dovozcům ve třetích zemích jako nástroj pro vytvoření vhodných záruk pro předávání osobních údajů podle čl. 46 odst. 2 písm. e) a f) obecného nařízení.

Do finální fáze dospěla příprava procedurálních pravidel pro schvalování ad hoc smluvních doložek podle čl. 46 odst. 3 písm. b) obecného nařízení, po jejichž zveřejnění budou moci vývozci osobních údajů, kteří z nějakého důvodu nechtějí použít standardní smluvní doložky, předkládat návrhy svých smluvních doložek, určených pro konkrétní předání osobních údajů, příslušným dozorovým úřadům.

Na základě dosavadních zkušeností s hodnocením návrhů závazných podnikových pravidel koncipovaných již podle požadavků čl. 47 obecného nařízení zahájila podskupina práci na úpravě dokumentů WP 256, WP 257, WP 263, WP 264 a WP 265, upravujících požadavky a proceduru schvalování závazných podnikových pravidel.

Úřad ve třech případech působil v roli spoluhodnotitele konkrétních návrhů závazných podnikových pravidel (Saxo Bank, Fresenius, Vestas) a ve dvou případech se ujal role reportéra přípravy stanoviska EDPB k návrhu konkrétních závazných podnikových pravidel (Iberdrola, Saxo Bank). Navíc Úřad společně s litevským dozorovým úřadem reagoval vstřícně na žádost o pomoc s hodnocením návrhů závazných podnikových pravidel předloženou EDPB ze strany nizozemského dozorového úřadu, který je přetížen množstvím případů, ve kterých si jej skupiny zvolily jako vedoucí dozorový úřad pro svá závazná podniková pravidla.

Rozsudek SD EU ve věci Schrems II

Stěžejní událostí roku 2020 v oblasti předávání osobních údajů do třetích zemí bylo dlouho očekávané rozhodnutí Soudního dvora Evropské unie (SDEU) ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems (tzv. Schrems II), které bylo vydáno dne 16. července 2020. Toto rozhodnutí jednak prohlásilo za neplatné Prováděcí rozhodnutí Komise ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí a jednak podmínilo použití standardních smluvních doložek (a potažmo i ostatních nástrojů pro vytvoření vhodných záruk podle čl. 46 obecného nařízení) testem přiměřenosti přijatých opatření v závislosti na okolnostech předání a zemi dovozce údajů, čímž razantně zvýšilo nároky na legální předání osobních údajů do třetích zemí.

K dopadům uvedeného rozhodnutí do praxe vydal Úřad vyjádření 7. srpna 2020 a na svém webu zveřejnil odpovědi na často kladené otázky K předávání osobních údajů do třetích zemí. V rámci expertní podskupiny pro mezinárodní transfery se Úřad podílel na vypracování několika dokumentů EDPB, které byly završeny zveřejněním Doporučení EDPB 1/2020 k opatřením doplňujícím stávající nástroje předávání osobních údajů pro zajištění EU úrovně ochrany osobních údajů.

V uvedeném doporučení EDPB popsal v několika krocích, jak má postupovat správce (příp. zpracovatel), který hodlá předávat osobní údaje do třetí země s nedostatečnou úrovní ochrany osobních údajů, aby zajistil předaným údajům ve třetí zemi úroveň ochrany „v zásadě rovnocennou" s unijní úrovní ochrany osobních údajů, jak ji vyžaduje ustanovení čl. 46 obecného nařízení, vyložené uvedeným rozhodnutím SDEU:

1. Správce musí předně skutečně znát okolnosti svého předání a uplatnit na předání jako na samostatnou operaci zpracování všechny zásady definované čl. 5 obecného nařízení, tzn. správce musí především vědět komu a do kterých zemí hodlá data předat, musí určit účel předání osobních údajů a vymezit relevantní údaje, které je nezbytné pro naplnění stanoveného účelu předat do třetí země.
2. Správce musí zvolit jeden z nástrojů pro předání vyjmenovaných v čl. 46 obecného nařízení, přičemž, pokud správce není členem skupiny disponující schválenými závaznými podnikovými pravidly, je v současné době stále jedinou schůdnou cestou použití standardních smluvních doložek podle některého z příslušných rozhodnutí Evropské komise.
3. Správce musí v kontextu daného předání, nejlépe ve spolupráci s potenciálním dovozcem osobních údajů, zhodnotit, zda legislativa třetí země nenaruší úroveň ochrany předaných osobních údajů takovým způsobem, že ani použití zvoleného nástroje podle čl. 46 obecného nařízení samo o sobě nezajistí vhodné záruky ochrany předaných osobních údajů. Především se správce musí soustředit na zhodnocení otázky, zda právní řád třetí země umožňuje jejím orgánům veřejné moci přístup k předaným osobním údajům v rozsahu, který jde nad rámec toho, co je obvyklé v demokratické společnosti (hodnocení této otázky je věnováno Doporučení EDPB 2/2020 k zásadním zárukám přiměřeného přístupu k osobním údajům).
4. V případě, že správce dojde k závěru, že pro dané předání do třetí země neposkytuje zvolený nástroj podle čl. 46 obecného nařízení dostatečné záruky pro zajištění „v zásadě rovnocenné" ochrany předaných osobních údajů, musí správce, zpravidla ve spolupráci s dovozcem, přijmout doplňková opatření, která navýší záruky na požadovanou úroveň. V přílohách uvedeného Doporučení EDPB 1/2020 jsou příklady možných technických, smluvních a organizačních opatření. Pokud správce nepřijme nebo nenalezne taková doplňková opatření, nezbude mu nic jiného než předání nerealizovat, resp. v případech již probíhajících předávání toto zastavit, nebo oznámit danou skutečnost příslušnému dozorovému úřadu, který rozhodne o zastavení předávání.
5. Správce musí posléze ve vhodných intervalech znovu zhodnotit, zda v právním řádu dané třetí země nedošlo k nepříznivému vývoji vzhledem k úrovni ochrany předávaných údajů, a zda tedy není nutné nalézt a přijmout ještě jiná doplňková opatření.

Je třeba upozornit, že dané Doporučení EDPB se nevztahuje na předávání osobních údajů jemuž se věnují výše uvedené Pokyny EDPB 2/2020, které otázku dopadů rozsudku SDEU již zohledňují.

V návaznosti na uvedené dlouho očekávané rozhodnutí SDEU vypracovala Evropská komise návrh nových, rovněž dlouho očekávaných, standardních smluvních doložek, který byl předložen EDPB ke stanovisku. Na návrhu stanoviska začala podskupina pro mezinárodní transfery intenzivně pracovat v závěru roku 2020.

Brexit

Se závěrem roku 2020 bylo stále více pravděpodobné, že odchod Velké Británie z Evropské unie bude zakončen bez rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů ve Velké Británii. V rámci dohody o budoucích vztazích uzavřené 24. prosince 2020 se Velká Británie a EU dohodly, že obecné nařízení zůstane v platnosti na území Velké Británie po přechodnou dobu maximálně šesti měsíců. Pro předávání osobních údajů do Velké Británie tak do 1. července 2021 zůstává v platnosti dosavadní režim, který zajistí plnou kontinuitu toků dat mezi EHP a Velkou Británií, aniž by musely společnosti použít jakýkoliv zvláštní nástroj pro přenos údajů. Evropská komise v současné době připravuje návrh rozhodnutí o odpovídající úrovni ochrany ve Velké Británii a předloží jej EDPB ke stanovisku tak, aby do konce přechodného období bylo rozhodnutí platné. EDPB zároveň pracuje na novém informačním dokumentu k předávání osobních údajů do Velké Británie po Brexitu.

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 dozorová činnost vnitrostátních orgánů dozoru spolu s nezbytnými právními úpravami.

Úřad plní v rámci své působnosti v souvislosti se schengenskou spoluprací úlohu vnitrostátního dozorového orgánu, který vykonává dohled nad dodržováním příslušných právních přepisů a dále přispívá k ochraně základních práv osob, jejichž osobní údaje jsou předmětem zpracování v rámci schengenského prostoru.

Evropskými informačními systémy schengenské spolupráce jsou:

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

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 systémům SIS II SCG, VIS SCG, Eurodac SCG a 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. Pověřený zástupce Úřadu se kromě výše zmíněných skupin pravidelně účastní jednání Rady spolupráce pro Europol (ECB) s poradní funkcí, jež byla zřízena v roce 2017, a zasedá minimálně dvakrát ročně.

V rámci činnosti napříč skupinami Úřad mimo jiné sdílí s ostatními příslušnými subjekty své zkušenosti zejména z dozorové činnosti a aktivně přispívá při zpracování podkladů k rozšíření povědomí o ochraně osobních údajů napříč laickou i odbornou veřejností.

S ohledem na epidemiologickou situaci a na navazující omezení pohybu osob na území členských států Evropské unie se veškerá jednání dotčených skupin, vždy i se zastoupením Úřadu, v roce 2020 uskutečnila prostřednictvím videokonference.

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, přičemž jejich počet byl v roce 2020 částečně ovlivněn aktuální pandemickou situací a navazujícími opatřeními. V průběhu roku 2020 Úřad obdržel celkem 30 podnětů týkajících se zpracování osobních údajů v SIS II, přičemž v devíti případech přezkoumával postup spravujícího orgánu, tj. Policie ČR, při zpracování osobních údajů. Ve všech ostatních případech, kdy žadatelé uplatňovali své právo na přístup k osobním údajům, případně právo na jejich opravu či výmaz, byly tyto žádosti, pokud splňovaly nutné náležitosti pro jejich předání, bez prodlení postoupeny věcně příslušnému útvaru Policie ČR k vyřízení.

Úřad dále obdržel celkem 12 podání, v rámci kterých se žadatelé dotazovali na vízovou politiku České republiky či na průběh vyřizování svých vízových žádostí. Vzhledem k tomu, že tato oblast nespadá do zákonem stanovených kompetencí Úřadu, byli jednotliví žadatelé odkázáni na Ministerstvo zahraničních věcí a příslušné zastupitelské úřady v zahraničí. Úřad v této souvislosti průběžně objasňoval kompetence svěřené mu zákonem o zpracování osobních údajů a unijními právními předpisy. Úřad v průběhu roku 2020 neobdržel žádnou stížnost na zpracování osobních údajů ve VIS.

Z uvedeného vyplývá přibližně poloviční pokles počtu přijatých podnětů týkajících se zpracování osobních údajů v SIS II oproti předchozímu roku, přičemž počet dotazů k vízové politice a vyřizování vízových žádostí zůstal ve srovnání s rokem 2019 téměř na stejných hodnotách.

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 které patří Schengenský informační systém, vízová politika, policejní spolupráce, vnější hranice, návraty a ochrana osobních údajů.

Hodnotící týmy jsou vždy vytvářeny ad hoc k jednotlivým evaluacím a jsou složeny ze zástupců 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.

Schengenské hodnocení České republiky bylo uskutečněno v roce 2019. Úřad proto v roce 2020 pokračoval v implementaci doporučení, která ze schengenského hodnocení vyplynula, konkrétně se jednalo o zahájení kontroly národní součásti VIS.

JUDIKATURA SOUDNÍHO DVORA EU K „DATA RETENTION"

Soudní dvůr Evropské unie vydal 6. října 2020 dva důležité rozsudky týkající se uchovávání a dalšího poskytování provozních a lokalizačních údajů o elektronické komunikaci. Konkrétně se jedná o rozsudek *Privacy International v. UK* (C-623/17) a spojený rozsudek *La Quadrature du Net a další v. Francie a Belgie* (C-511/18, C-512/18 a C-520/18).

Oba rozsudky navazují a utvrzují dřívější judikaturu v předmětné záležitosti. Jedná se konkrétně o rozsudek ve věci *Digital Rights Ireland Ltd* (C-293/12) z 8. dubna 2014, rozsudek ve věci *Tele2 Sverige AB* (C-203/15) z 21. prosince 2016 a rozsudek ve *věci Ministerio Fiscal* (C-207/16) z 2. října 2018. Kromě toho rozšiřují působnost unijního práva na zadržení údajů zpravodajskými službami.

Za zvláštní pozornost potom stojí především výroky 1 a 2 rozsudku *La Quadrature du Net a další v. Francie a Belgie* a výrok 2 rozsudku *Privacy International v. UK*. Jimi se obecně zakazují národní legislativní opatření založená ustanovením čl. 15 směrnice 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, pokud preventivně ukládají plošné a nerozlišující uchovávání provozních a lokalizačních údajů. Nicméně se zároveň za blíže určených podmínek povoluje nařídit:

- plošné a nerozlišující uchovávání provozních a lokalizačních údajů v případě reálné a vážné hrozby národní bezpečnosti;
- cílené uchovávání provozních a lokalizačních údajů buď určitých kategorií osob anebo vymezených podle geografických kritérií, obecné a plošné zadržení IP adresy přidělené zdroji připojení a také uchovávání údajů o totožnosti uživatelů elektronických komunikačních systémů, a to na základě objektivních a nediskriminačních faktorů a za účelem zajištění národní bezpečnosti, boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti;
- provedení urychleného uchovávaní provozních a lokalizačních údajů za účelem zajištění národní bezpečnosti a boje proti závažné trestné činnosti.

Čl. 15 směrnice 2002/58/ES také nebrání národní legislativě, která ukládá poskytovatelům služeb elektronických komunikací automatizovaně analyzovat a shromažďovat zejména provozní a lokalizační údaje v reálném čase. Stejný případ platí i pro národní legislativu, která ukládá zajistit v reálném čase shromažďování technických údajů o umístění používaných koncových zařízení, ovšem pouze pokud je nutno čelit závažné hrozbě pro národní bezpečnost a jsou splněny další stanovené podmínky.

Vyvstává tak otázka, nakolik může ve světle těchto rozhodnutí obstát stávající pojetí představované především ustanovením § 97 zákona č. 127/2005 Sb., o elektronických komunikacích, a souvisejícími předpisy založené na preventivním šestiměsíčním zadržování provozních a lokalizačních údajů. Současně je však třeba mít stále na paměti nález Ústavního soudu č. 161/2019 Sb., kde se v bodech 71 až 82 uvádí, že k zadržování takových dat musí objektivně docházet (především pro samotné zajištění služeb a jejich následné vyúčtování), přičemž absence právního zakotvení této povinnosti by vedla k větším škodám v podobě ztráty veřejnoprávních mezí a kontroly.

Bude proto nutno zvážit, jak naplnit požadavky výslovně uváděné v předmětných rozsudcích Soudního dvora Evropské unie. Úřad by pak považoval za přiměřené individuální stanovení lhůt pro uchovávání dat. Ty by měly být určeny zvláště pro různé účely (cíle) a s největší pravděpodobností rovněž i pro různé komunikační kanály a též individuálně odůvodněny, tak, aby bylo budoucí vytěžování zadržených údajů pro dotčené subjekty předvídatelné a mohlo obstát.

Předmětem dalších úvah pak musí být i otázka, do jaké míry k překlenutí nastíněných problémů postačí pouze určitý eurokonformní výklad, či zda je nutná změna zákona, což by měl však vyřešit především gestor.

Svobodný přístup k informacím

Vyhodnocení nové působnosti Úřadu dle zákona č. 106/1999 Sb.

Základním východiskem pro zahájení výkonu nové agendy Úřadu byla teze, že Listinou zaručené právo na informace v článku 17 je potřeba realizovat i v přiměřeném čase. Smyslem a účelem práva na informace je kontrola činnosti veřejné správy včetně vynakládání veřejných prostředků či hospodaření s veřejným majetkem. Platí, že čím dříve je požadovaná informace žadateli dodána, tím „lépe" je jeho právo naplněno. Včasné naplňování ústavních práv pak nepochybně podporuje demokratické procesy. Žadatel má konkrétní znalost o veřejné správě a na základě včasných a relevantních informací se může věcně správně rozhodovat.

Úřad proto ke své agendě přistoupil s plným respektem k tomuto základnímu právu a vědomím, že je potřeba k poskytování informací přistupovat objektivně. Nejedná se totiž o abstraktní informace ani o právo absolutní, ale konkrétní sdělení vztahující se ke konkrétním povinným subjektům, v určitém čase a nepochybně se zásadními důsledky.

Zároveň si byl vědom, že problém při poskytování informací tkvěl především v tom, že požadované informace byly často poskytnuty až na základě rozhodnutí soudů, ve lhůtách dvou a více let. Zajistil tak přívětivý přístup pro občany, kdy mohl reálně zkrátit zákonnou dobu k poskytnutí informace na několik týdnů namísto let.

V řadě případů však postup povinných subjektů, které informace odmítly poskytnout, potvrdil s tím, že byly dány zákonné důvody a jednalo se o informace chráněné. Svou činností rovněž přispívá k rychlému a nezávislému přezkumu pravomocných rozhodnutí, pokud je žadatel přesvědčen, že informace mu měla být vydána. V řadě případů tak žadatel již nevyužije práva soudního přezkumu rozhodnutí, pokud Úřad po posouzení rozhodnutí o odmítnutí žádosti shledá, že pro odmítnutí informace byl dán zákonný důvod. Touto svojí činností může Úřad přispět k odlehčení náporu na správní soudy, i když činnost soudu bezpochyby nenahrazuje.

Agenda práva na informace není triviální. Kromě zákonných předpisů vyžaduje znalost příslušné judikatury správních soudů a Ústavního soudu ČR, jejich vývojové tendence, změny, odborný kontext a také míru lidské zkušenosti a schopnost objektivního úsudku pro řešení řady situací.

Cíle, s jakými byla novela informačního zákona přijímána, se Úřadu podařilo splnit.

Fakticky od 2. ledna 2020 získal novou působnost v řízeních dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, v následujících oblastech:

- posuzování podnětů k zahájení přezkumného řízení rozhodnutí nadřízených orgánů,
- přijímání opatření proti nečinnosti nadřízených orgánů v řízeních dle uvedeného právního předpisu,
- působnost nadřízeného orgánu pro řízení dle uvedeného právního předpisu u vybraných povinných subjektů.

Popis jednotlivých agend

A. **Opatření proti nečinnosti nadřízených orgánů** – Úřad je příslušným pro přijetí opatření v případě nečinnosti nadřízených orgánů, a to v řízeních o odvolání, rozkladu nebo o stížnosti. Jedná se o méně početnou část agendy, kterou Úřad dosud vyřizuje. V rámci možných opatření v současné době využívá zpravidla přikázání nečinnému orgánu ve věci rozhodnout ve stanovené lhůtě. Je však třeba poukázat na skutečnost, že se touto právní úpravou nestává nadřízeným orgánem dotčených (nadřízených) orgánů.

B. **Přezkumné řízení** – posuzování podnětů na přezkum rozhodnutí nadřízených orgánů je pro zákon č. 106/1999 Sb. zcela nový institut, který nebylo možné do konce roku 2019 využít. Jedná se o možnost přezkoumávat pravomocná rozhodnutí nadřízených orgánů, a to v případě, kdy lze pochybovat o tom, že byla vydána v souladu s platnými právními předpisy. Užití správního řádu je omezené, otázkou tedy je, jaká všechna rozhodnutí nadřízených orgánů je Úřad oprávněn přezkoumávat. V současné době postupuje tak, že přezkoumává pouze rozhodnutí o odvolání nebo rozkladu, jimiž bylo potvrzeno odmítnutí informace povinným subjektem. Rozhodnutí o stížnostech ve smyslu § 16a zákona č. 106/1999 Sb. přezkoumávat dle názoru Úřadu nelze, protože se nejedná o rozhodnutí ve věci.

C. **Úřad jako nadřízený orgán některých povinných subjektů** – jedná se o nejobjemnější agendu, u které bylo třeba vyjasnit řadu otázek a která je zároveň vázána velmi krátkými zákonnými lhůtami. Úřad vždy musí nejprve určit, zda je pro konkrétní subjekt příslušným nadřízeným orgánem. V některých případech je třeba se ještě předtím zabývat otázkou, zda se ve smyslu zákona č. 106/1999 Sb. vůbec o povinný subjekt jedná. Průběžně je doplňován přehled povinných subjektů, u kterých je Úřad nadřízeným orgánem. Výčet není dosud kompletní, na Úřad se obracejí jak povinné subjekty s žádostí o posouzení této otázky, tak i žadatelé o informace se svými podněty.

Oblast informací, o kterých je rozhodováno, zda budou či nebudou poskytnuty, je s ohledem na různorodost povinných subjektů velmi rozmanitá a zasahuje do celé řady oblastí. Níže jsou příklady některých povinných subjektů, u kterých je Úřad nadřízeným orgánem:

- vybrané soudy (Ústavní soud ČR, Nejvyšší správní soud, Nejvyšší soud),
- Nejvyšší státní zastupitelství,
- Akademie věd ČR,
- Česká advokátní komora,
- veřejné vysoké školy (zde je působnost dělená mezi Úřad a MŠMT, podle toho, zda žádost o informace směřuje do samosprávy vysoké školy, nebo do výkonu státní správy),

- obchodní společnosti (zřizované a stoprocentně vlastněné státem nebo samosprávnými celky),
- některé státní organizace (Ředitelství silnic a dálnic, Správa železnic),
- zdravotní pojišťovny.

D. **Žaloby proti rozhodnutím Úřadu, jeho nástupnictví do neukončených soudních sporů** – ke konci roku 2020 začala výraznějším způsobem přibývat agenda soudních sporů. Za uvedený rok eviduje Úřad celkem patnáct žalob, kdy je stranou žalovanou. Ne všechny žaloby směřují proti jeho rozhodnutí. V tomto směru bylo podáno celkem šest žalob, z toho v jednom případě ji vzal žalobce zpět. Jedna žaloba směřovala proti nečinnosti Úřadu, i v tomto případě žalobce svůj krok přehodnotil. Dále je žalobou u Nejvyššího správního soudu řešen negativní kompetenční spor Úřadu s Ministerstvem pro místní rozvoj, kdy se ani jeden z dotčených orgánů nepovažuje za příslušný nadřízený orgán pro státní příspěvkovou organizaci Česká centrála cestovního ruchu – CzechTourism.

Od listopadu 2020 byl Úřad dále v sedmi případech příslušnými soudy informován o nástupnictví v dosud neukončených soudních sporech, kdy žaloby směřovaly proti rozhodnutím o odvolání vydaným do konce roku 2019. V důsledku změny příslušného nadřízeného orgánu byl v těchto soudních řízeních pasivně legitimován, a tedy je nástupcem původního žalovaného, ač ve věci žádné řízení nevedl ani nerozhodoval. Z uvedených soudních sporů byly do konce roku tři ukončeny, kdy v jednom případě bylo řízení zastaveno v důsledku uspokojení žalobce povinným subjektem, jedna žaloba byla zamítnuta, rovněž i kasační stížnost.

Tato agenda nástupnických žalob vyvolává nejen zvýšené personální nároky, ale také nároky finanční. V případě úspěchu žalobce je Úřad totiž povinen uhradit vzniklé soudní náklady v plné výši, aniž by skutečně měl možnost výsledek soudního sporu ovlivnit. Je tak odsouzen uhradit náklady soudního řízení, které v průměru na jednu žalobu čítají 20 000 Kč. S ohledem na délku soudních řízení lze předpokládat, že tato situace bude přetrvávat minimálně do roku 2022, aniž by Úřad mohl počet soudních sporů a jejich výsledek ovlivnit.

Personální zajištění

Zákon č. 106/1999 Sb. upravil zcela nové působnosti Úřadu. Zčásti se jedná o činnosti, které předchozí právní úprava nepřipouštěla, zčásti o činnosti, které byly zajišťovány statutárními zástupci daných povinných subjektů. S ohledem na tuto skutečnost nebylo možné provést delimitaci agend, tedy ani Úřadu nově přiřadit stávající pracovníky vybraných povinných subjektů, kteří dosud tuto činnost zajišťovali. Po dohodě s Ministerstvem financí byla pro tyto účely nově systemizována tři služební místa, Úřad dále ze svých zdrojů poskytl pět systemizovaných služebních míst, která by byl nucen v rámci úsporných opatření k 31. prosinci 2019 zrušit. Ze svých stávajících kapacit dále poskytl jedno systemizované pracovní místo.

Celkem je pro agendu plynoucí ze zákona č. 106/1999 Sb. určeno osm systemizovaných služebních míst a jedno systemizované pracovní místo. Vytvořený odbor práva na informace se skládá ze dvou oddělení.

Pro zajištění spisové služby, administrativních a dalších činností je odboru přidělena jedna pracovnice. Sedm státních zaměstnanců vč. dvou vedoucích oddělení se pak zabývá vyřizováním podání a doručených podnětů. Činnost je zastřešena ředitelkou odboru, která zajišťuje řídicí činnost, proškolení pracovníků, spolupráci s povinnými subjekty a dalšími dotčenými resorty a vyřizuje stížnostní agendu týkající se činnosti zaměstnanců odboru.

Úřad každý měsíc obdrží průměrně 44 podání. Větší část podání řeší jako nadřízený orgán povinných subjektů, rozhoduje o stížnostech a odvoláních. Z celkového počtu 61 stížností na postup povinného subjektu při vyřizování žádostí o informace bylo 27 shledáno jako důvodných, 19 nedůvodných. Z 238 odvolání bylo v 91 případech toto zamítnuto jako nedůvodné nebo opožděné, ve 113 případech bylo rozhodnutí povinného subjektu zrušeno a věc vrácena k novému projednání, resp. ve dvou případech bylo řízení zastaveno a v jednom případě byl vydán informační příkaz.

Úřad obdržel 97 podnětů na zahájení přezkumného řízení. Z tohoto počtu byl v 61 případech shledán podnět nedůvodným, ve 14 případech bylo v přezkumném řízení rozhodnuto, a to včetně vydání

informačního příkazu ve dvou případech. V pěti případech prohlásil Úřad napadené rozhodnutí nicotným. V osmi případech bylo přezkumné řízení zahájeno, dosud nebylo ukončeno.

Celkem 99 podání podání směřovalo proti nečinnosti nadřízeného orgánu, z tohoto počtu bylo 58 podání nedůvodných. Ve 26 případech bylo vydáno opatření proti nečinnosti.

Informovanost o činnosti Úřadu

O své činnosti v rámci nové agendy Úřad informuje prostřednictvím webových stránek. K dispozici jsou jak pro povinné subjekty, tak i pro žadatele o informace. Dotazy jsou vyřizovány telefonicky i písemně. Nejužívanější je telefonická konzultace se zhruba pěti konzultacemi týdně.

Zhodnocení prvního roku činnosti odboru práva na informace

Prioritou při zajištění nové agendy byla a stále je řádné vyřízení doručených podání v zákonných lhůtách. Úřad vyřizuje odvolání a stížnosti do 15 dnů od jejich postoupení povinným subjektem, podněty na přezkumné řízení a žádosti o opatření proti nečinnosti jsou vyřizovány do 30 dnů ode dne jejich doručení. U obou lhůt je pro vyřízení potřeba celá její délka, lhůty však nejsou, až na výjimky v řádu jednotek, překračovány.

Další prioritou bylo a je zaškolení nových zaměstnanců, kteří byli přijati průběžně v prvním pololetí roku 2020. Všichni kolegové se rychle zorientovali a průběžně si doplňují znalosti v oblastech, jichž se agenda poskytování informací dotýká.

Je možné konstatovat, že se podařilo postupně vytvořit tým lidí, kteří mají o řešenou oblast zájem a jsou si vědomi důležitosti i odpovědnosti při vyřizování podání. V rámci podání jsou řešeny složité právní otázky z různých oblastí práva, které mohou mít vliv nejen na respektování práva na informace jednotlivých žadatelů, ale i respektování práv povinných subjektů a dalších dotčených osob.

Prvních rok činnosti byl velmi náročný, Úřad přistoupil k řešení jednotlivých podání zodpovědně s tím, že bylo nezbytné se v celé oblasti, ale i v činnosti jednotlivých povinných subjektů, rychle a podrobně zorientovat.

Za pozitivum nové právní úpravy lze jednoznačně označit objektivní posouzení podání mimo strukturu povinného subjektu, rovněž tak možnost rychlého posouzení rozhodnutí nadřízených orgánů jiným subjektem (Úřadem), který přezkoumá zákonnost rozhodnutí a žadatele písemně informuje o důvodech, proč neshledal rozhodnutí a postup v daném řízení jako nezákonný, či zahájí přezkumné řízení. Žadatelům o informace je tak dána možnost rychle a bez zásadních formalit žádat o znovuposouzení postupu a rozhodnutí ve věci. Povinné subjekty nová právní úprava rovněž motivuje k tomu, aby byla jejich rozhodnutí srozumitelná a řádně odůvodněná.

K vydání informačního příkazu Úřad přistoupil zatím pouze ve třech případech. Jedná se o zcela nový institut pro nadřízené orgány a zároveň je nutné si uvědomit, že celá agenda je pro něj nová. Vydání informačního příkazu přichází v úvahu v případě, že je nepochybné, že povinný subjekt požadovanou informací disponuje (má disponovat) a zároveň neexistuje zákonný důvod pro její odepření. Požadované informace, které mají být součástí postoupených stížností a odvolání, však povinné subjekty ve všech případech nepřipojují, objektivně proto není možné posoudit, zda má být požadovaná informace žadateli poskytnuta.

Úřad přistoupil k řešení nové agendy naprosto zodpovědně i přes minimální počet pracovníků, pro které od Ministerstva financí získal systemizovaná služební místa. Začátek výkonu nové agendy zvládl bez excesů či porušení zákonných lhůt.

POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA č. 106/1999 Sb., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

Také v roce 2020 pokračoval trend, započatý v předchozích letech v souvislosti s účinností obecného nařízení, spočívající ve zvýšeném zájmu o činnost Úřadu ze strany veřejnosti, který se projevil mimo jiné i nárůstem počtu žádostí o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon o svobodném přístupu k informacím"). Níže uvedené údaje se vztahují k postavení Úřadu jako povinného subjektu a jsou zveřejňovány ve smyslu § 18 zákona o svobodném přístupu k informacím. Nezohledňují jeho specifické postavení podle zákona č. 111/2019 Sb., tedy ustanovení § 16b a § 20 zákona o svobodném přístupu k informacím.

Oproti roku 2019, kdy obdržel Úřad 90 žádostí, se v roce 2020 věnoval celkem 99 žádostem.

Z toho:

- v 88 případech byla informace poskytnuta v celém požadovaném rozsahu;
- v osmi případech Úřad částečně odmítl informaci poskytnout;
- ve třech případech Úřad informaci odmítl poskytnout úplně.

Žadatelé tradičně pocházeli z řad laické, ale i odborné veřejnosti, přičemž žádosti se různorodě dotýkaly jak činnosti Úřadu coby dozorového úřadu dle obecného nařízení, tak také dalších informací o Úřadu jako takovém.

Z obsahového hlediska žádostí byl tradičně největší zájem o informace v podobě výstupů ze správních řízení či kontrol, tj. rozhodnutí či kontrolních protokolů z Úřadem provedených správních řízení a kontrol. V případě, kdy žadatelé výslovně nežádali o anonymizované výstupy z dozorové činnosti, muselo být přikročeno k rozhodnutí o částečném odmítnutí poskytnutí informací, jelikož správní rozhodnutí či kontrolní protokoly obsahují typicky některé informace, které nelze dle příslušných ustanovení zákona o svobodném přístupu k informacím poskytovat. Jednalo se např. o informace ke konkrétním bezpečnostním opatřením u kontrolované osoby.

Ve vztahu k dozorové činnosti žadatele zajímaly také obecné a statistické údaje o počtu provedených kontrol či správních řízení za různá časová období nebo informace o výši doposud nejvyšší uložené pokuty za porušení obecného nařízení.

Veřejnost se v rámci práva na svobodný přístup k informacím zajímala též například o vnitřní uspořádání Úřadu ve formě vnitřních předpisů nebo o podrobnosti odměňování jeho zaměstnanců ať už obecně nebo konkrétně.

Poskytnuté informace byly standardně zpřístupňovány způsobem umožňujícím dálkový přístup dle § 5 odst. 4 zákona o svobodném přístupu k informacím na webových stránkách Úřadu.

V roce 2020 nebyly Úřadem poskytnuty žádné licence.

V roce 2020 obdržel Úřad čtyři stížnosti dle § 16a zákona o svobodném přístupu k informacím. Důvodem pro podání první stížnosti mělo být neposkytnutí informace ke všem bodům žádosti, rozhodnutím byla stížnost zamítnuta a předchozí postup potvrzen; důvodem pro podání druhé stížnosti bylo neposkytnutí požadované informace v rozsahu, v jakém žadatel očekával, rozhodnutím byla stížnost zamítnuta a postup potvrzen. Důvodem pro podání třetí stížnosti bylo dle stěžovatele to, že nebyla poskytnuta informace v rozsahu požadovaném žadatelem, rozhodnutím bylo stížnosti vyhověno a povinnému subjektu přikázáno do 15 dnů ode dne doručení rozhodnutí vyřídit původní žádost; a konečně posledním důvodem bylo také rozhodnutím stížnosti žadatele vyhověno a povinnému subjektu přikázáno vyřídit žádost ve lhůtě 15 dnů ode dne doručení rozhodnutí.

V roce 2020 neeviduje Úřad v případech, kdy byl povinným subjektem, podání žádné žaloby ve věci přezkoumání zákonnosti rozhodnutí povinného subjektu o odmítnutí žádosti o poskytnutí informace.

Informační systém ORG v systému základních registrů

Informační systém ORG provozuje Úřad od roku 2012 jako součást systému základních registrů a od roku 2018 jako součást kritické informační infrastruktury státu a součást eGovernmentu České republiky. Jedná se o samostatnou působnost a její naplňování je v Úřadu organizačně odděleno. Informační systém ORG je naprosto nezbytnou bezpečnostně-technickou komponentou základních registrů, jejichž správcem je Správa základních registrů.

Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, byl informační systém ORG určen jako informační systém kritické infrastruktury. Správce takového informačního systému je povinen plnit technická opatření stanovená ve vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Rok 2020 byl mimořádně náročný nejen pro pracovníky oddělení základních identifikátorů, ale celou naši společnost. Při první vlně pandemie koronaviru a zavedení nouzového stavu začalo pro Správu základních registrů, a tím i pro pracovníky IS ORG, platit opatření nastavené pro systémy kritické infrastruktury.

Díky dobrému materiálnímu vybavení lze bezpečně dohlížet na běh IS ORG vzdáleně. Jedná se o komunikaci s dodavatelem, sledování a vyřizování požadavků ze Service desku IS ORG i Service desku základních registrů a kontrolu systému. Pracovníci drželi pohotovosti v pracovní dny, o víkendech a svátcích po celý den. Vzhledem k tomu, že jejich pracovní náplní je také docházení do datových center a provádění případné výměny vadného hardwaru, nebyla zde možná práce z domova.

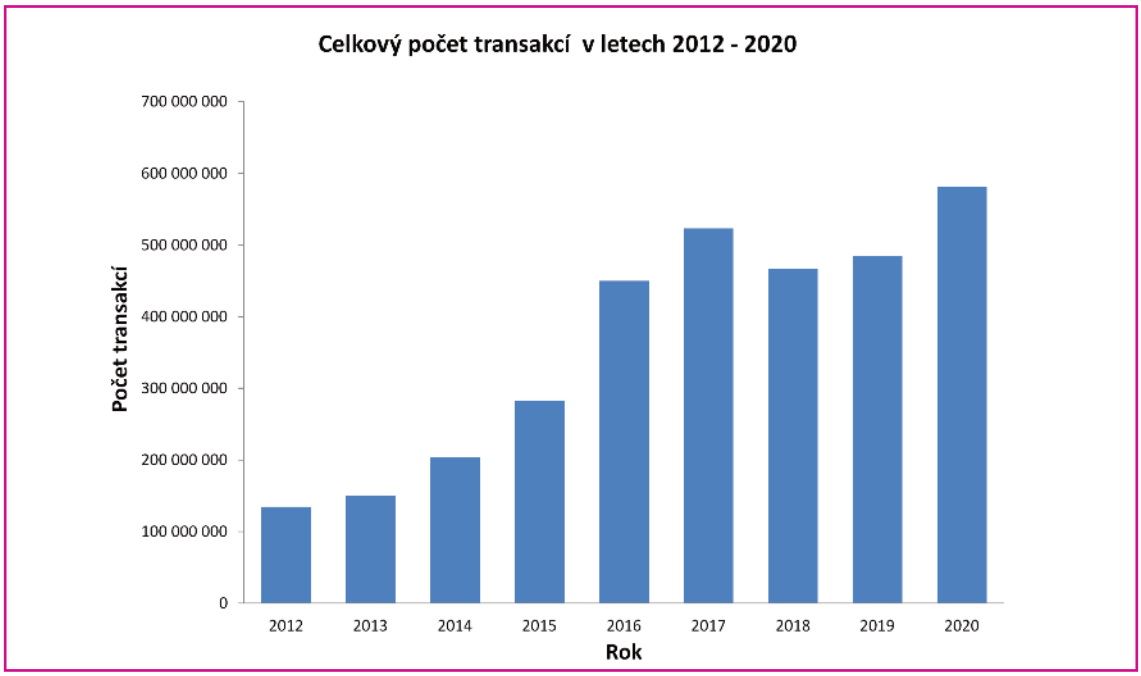
S nástupem druhé vlny pandemie a opětovným vyhlášením nouzového stavu byl takový režim znovu zaveden.

V listopadu byla provedena rozsáhlá obnova původního hardwaru, byla rozšířena disková kapacita a optimalizováno zálohování. Současně s tím byla provedena úprava architektury webových a aplikačních služeb.

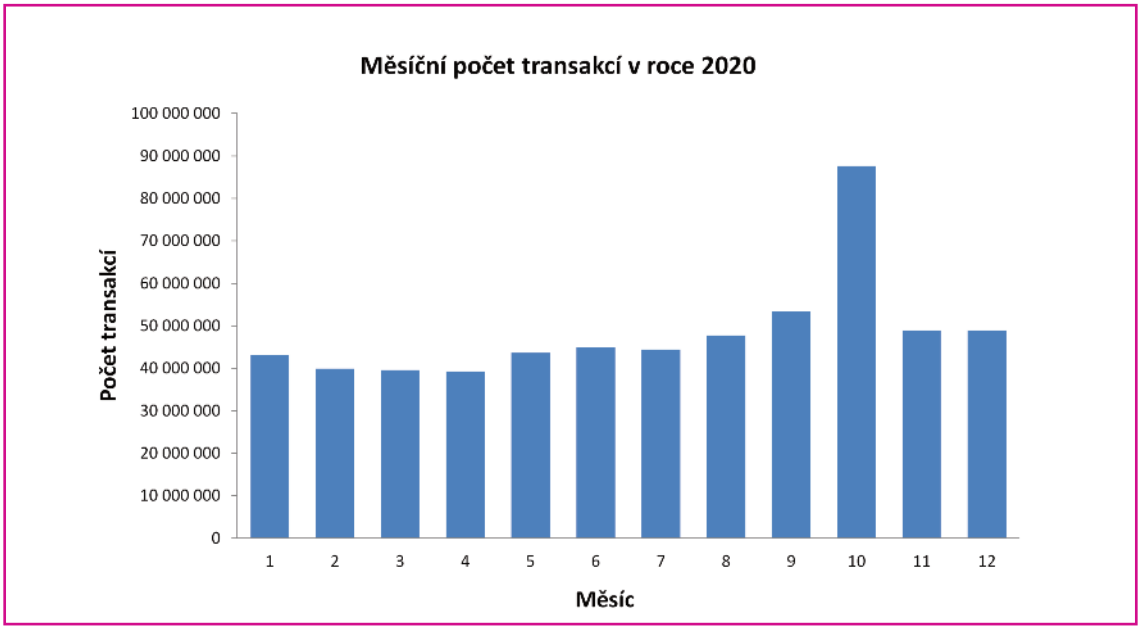
Na doporučení Správy základních registrů je IS ORG certifikován podle ČSN/ISO 27001:2014. Systém IS ORG byl v roce 2020 úspěšně recertifikován bez nálezu dle této normy.

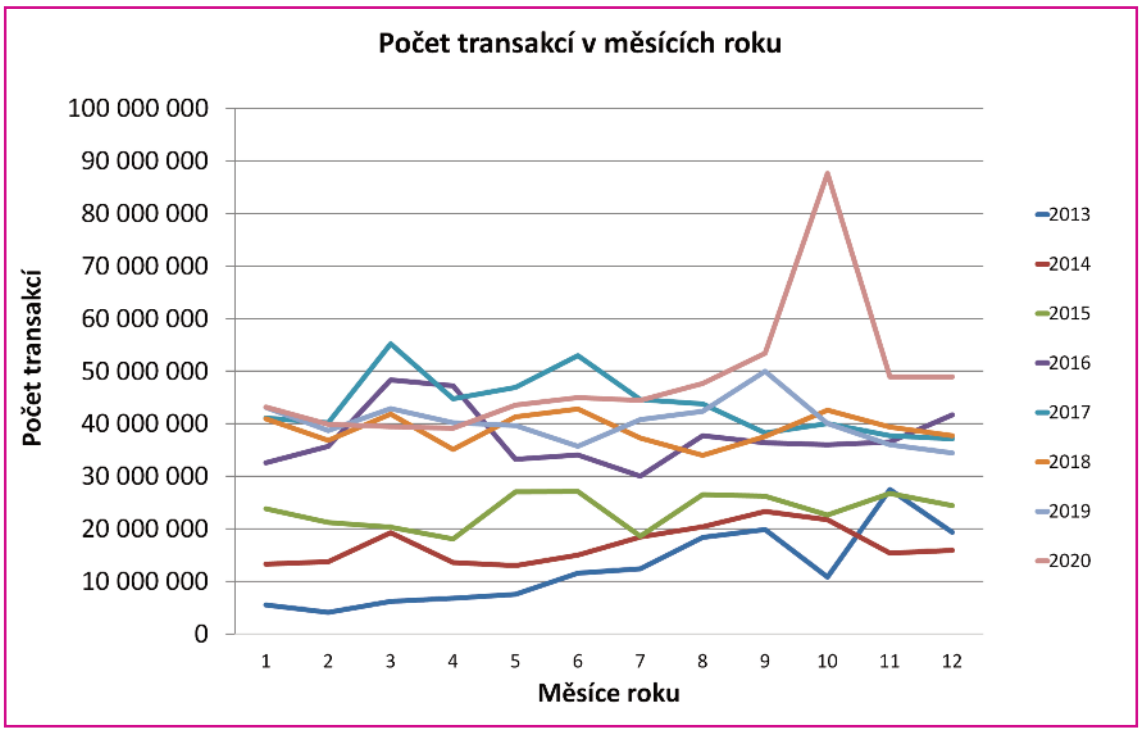
Na rozdíl od předchozích let, kdy byly dvě špičky vytíženosti systému – jarní v březnu a podzimní na přelomu září a října – byla v roce 2020 zaznamenána jen jedna výrazná špička, a to v říjnu. V tomto měsíci proběhlo 87 341 189 transakcí. Z toho bylo 53 585 224 transakcí CtiAIFO a 29 978 557 transakcí ZalozAIFO.

Dá se předpokládat, že tato špička má souvislost s dvěma koly krajských a senátních voleb ve dnech 2. a 3. října a 9. a 10. října 2020. V období od 4. do 14. října 2020 byl denní průměr 4 365 407 transakcí. Během roku transakce CtiAIFO proběhla 270 755 406krát a transakce ZalozAIFO 214 850 924krát. To představuje 91,3 procenta všech transakcí.



V roce 2020 došlo k nárůstu vytíženosti systému o 9,98 procenta oproti předchozímu roku.





Maximum vytíženosti bylo ve čtvrtek 8. října 2020 s hodnotou 4 949 289 transakcí. Minimum bylo v neděli 16. února 2020 s hodnotou 198 488 transakcí.

Sdělovací prostředky a komunikační nástroje

Stejně jako jiné útvary i tiskové oddělení muselo přizpůsobit v roce 2020 svou činnost stavu způsobenému pandemií COVID-19. Zásadní změnou prošla mediální komunikace založená na osobním kontaktu, která byla nahrazena především elektronickou formou.

Přes obtížné podmínky trvající s přestávkami téměř celý rok se Úřad věnoval osvětové činnosti a přinášel novinky z oblasti ochrany dat. Na začátku roku 2020 zveřejnil vlastní shrnutí zásadních částí aktuálních pokynů EDPB provozovatelům kamerových systémů, upozornil na potřebu adaptace sektoru elektronických komunikací na obecné nařízení, ale i na povinnosti spojené s ohlašováním případů porušení zabezpečení osobních údajů v oblasti zdravotnictví. Tématu COVID-19 se věnoval Úřad záhy. Na konci března zveřejnil vlastní překlad stanoviska EDPB ke zpracování osobních údajů v souvislosti s propuknutím nákazy. Vyjádřil se také k mimořádným opatřením Ministerstva zdravotnictví v souvislosti s projektem Chytrá karanténa. Rovněž rozšířil webovou rubriku Často kladené otázky o téma ochrany dat v době koronavirové pandemie. Velmi mediálně sledovaný byl i zveřejněný postoj Úřadu k měření teploty při vstupu na pracoviště kvůli ochraně před COVID-19. Dalšími významnými oblastmi, kterým média v roce 2020 věnovala zvýšenou pozornost, byla otázka shromažďování osobních údajů účastníků soudních řízení v internetových databázích. Nelze nezmínit i od počátku roku mediálně sledovanou novou agendu Úřadu vycházející ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Úřad rovněž informoval o nejvyšší uložené pokutě za nevyžádaná obchodní sdělení ve výši 6 000 000 Kč.

Mediální vrcholy roku představovaly pro Úřad připomenutí výročí 20 let od jeho vzniku, ale také zvolení nového předsedy Senátem PČR, kterým se stal Jiří Kaucký, stejně jako zvolení Petra Jägera do funkce druhého místopředsedy Úřadu.

Ve zvýšené míře se média v roce 2020 věnovala v souvislosti s ochranou osobních údajů oblasti digitálních technologií. Deník N zveřejnil článek *„Kde jsi včera byl? Mobily na nás prozradí úplně všechno"* popisující, co vše o sobě uživatel prozradí během standardního používání mobilního telefonu. Stále více se do popředí zájmu médií, ale i veřejnosti, dostávalo téma systémů na rozpoznávání obličejů. Server Info.cz přinesl v první polovině roku zprávu *„Definitivní konec soukromí? Nová technologie údajně rozpozná obličeje miliard lidí"* o technologii, která je prakticky okamžitě schopna identifikovat jakéhokoli člověka procházejícího na ulici. Kybernetickým útokům i během pandemie COVID-19 se věnovala média v průběhu celého roku. TV Prima upozorňovala ve své reportáži *„Stoupá počet kybernetických útoků na firmy i domácnosti"*, že útočníkům značně usnadňují jejich práci samotní uživatelé. Obdobně informoval portál iDNES.cz o nedostatečném přístupu uživatelů k bezpečnosti na internetu v článku *„Hackeři využili karantény a útočí, zaměstnanci na home office se neumí bránit"*. Dezinformacím, které provázejí boj s pandemií COVID-19, se věnovala v průběhu roku prakticky všechna média. Zpravodajský server BBC News, resp. ČTK, přišly se zprávou, že vyšší stupeň vzdělání nezaručuje, že lidé nepodlehnou dezinformacím. V článku *„Proč i chytří lidé věří koronavirovým mýtům?"* uvádí, že na vině je zejména nekritické myšlení a nedostatečné vyhledávání zdrojů zveřejňovaných informací.

Z čistě tuzemských témat se média v roce 2020 věnovala například kamerovému systému elektronických dálničních známek. V TV Seznam tak v pořadu Výzva mohl k tématu vystoupit místopředseda Úřadu Josef Prokeš. Důležitým tématem bylo rovněž používání mobilních aplikací k boji s epidemií COVID-19. ČTK představila v článku *„Ochránci soukromí EU: data z mobilů používaná proti epidemii by měla být anonymizovaná"* stanovisko EDPB k danému tématu. Významnou část roku přinášela média informace o českém projektu tzv. chytré karantény a aplikaci eRouška. Některých z výše popsaných témat se týkal také rozsáhlý rozhovor *„Co je smazáno, nemůže být zneužito"*, který pro Lidové noviny poskytnula tehdejší předsedkyně Úřadu Ivana Janů. Výhradám Kanceláře prezidenta republiky k zákonu o svobodném přístupu k informacím, který rozšířil pravomoci Úřadu, se věnoval ve svém článku například server iRozhlas *„Hrad prosadil u vnitra změnu práva na informace. O stížnostech má opět rozhodovat kancléř Mynář"*. Mediální zájem vzbudila snaha státu poskytnout seniorům ochranné prostředky v boji s COVID-19. Článek ČTK *„Rozesílání roušek seniorům prověřují ochránci osobních údajů"* byl jedním z mnoha, ve kterém média tuto kauzu opakovaně připomínala.

MEDIÁLNÍ OBRAZ

Ani v roce 2020 nebyl Úřad spojován novináři s žádnou kauzou. Média se po celý průběh roku věnovala převážně tématům spojeným s pandemií. Na Úřad se proto obracela spíše kvůli projektu Chytré karantény a možné povinnosti registrace při vstupu do restaurací. Přesto se Úřad po celý rok snažil, aby i výše popsaná témata byla mediálně zaznamenána.

TWITTER

S aktuálními informacemi ze své činnosti a praxe, stejně jako s novinkami ze světa ochrany osobních údajů, seznamuje Úřad širokou veřejnost také prostřednictvím světově oblíbené sociální sítě Twitter. Oficiální účet Úřadu doplnil v roce 2020 také osobní profil předsedy Úřadu.

WEBOVÉ STRÁNKY

I nadále sloužily webové stránky Úřadu pro primární komunikaci. Využívány byly zejména pro zveřejňování informací určených pro laickou i odbornou veřejnost. Významným způsobem byla nadále rozšiřována a aktualizována rubrika Poradna, zahrnující informace a návody pro řešení řady životních situací.

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 2020 i 31. prosinci 2020 činil 112.

Fluktuace zaměstnanců se v roce 2020 v meziročním srovnání s předchozím rokem snížila z 11,8 procenta na 9,5 procenta.

Plynule pokračoval chod jednotlivých procesů personální správy Úřadu v návaznosti na vývoj legislativy v oblasti státní služby a pracovněprávních vztahů. S účinností od 1. září 2020 byl nově jmenován do funkce předsedy Úřadu Mgr. Jiří Kaucký.

Dne 16. prosince 2020 byl s účinností od 1. ledna 2021 zvolen do funkce místopředsedy Mgr. Petr Jäger, Ph.D.

Ke dni 30. září 2020 ukončila svůj mandát inspektorka PaedDr. Jana Rybínová a k 31. prosinci 2020 inspektor Mgr. Daniel Rovan.

V průběhu čtvrtého čtvrtletí roku 2020 probíhala postupně změna organizační struktury Úřadu do výsledné optimální podoby, která již ve svých základních obrysech zůstane trvalá.

Úřad v průběhu roku 2020 obsadil všechna systemizovaná místa související s novou agendou zákona č. 106/1999 Sb., o svobodném přístupu k informacím, čímž zajistil v souladu s omezeným počtem přidělených míst minimální rozsah personálního krytí výkonu předmětné působnosti. S ohledem na rozsah agendy se jedná o personální obsazení velmi poddimenzované.

Zároveň v rámci jednání o rozpočtu požádal předseda Úřadu o navýšení tří míst pro výkon agendy. Tento požadavek byl podpořen s ohledem na rozsah nové agendy i gesčním petičním výborem Poslanecké sněmovny v rámci projednávání rozpočtu Úřadu pro rok 2021, nicméně se ve schváleném rozpočtu neprojevil, rozpočet Úřadu byl snížen o tři miliony Kč.

V průběhu první i druhé vlny epidemie koronaviru COVID-19 bylo všem zaměstnancům umožněno vykonávat jejich pracovní povinnosti z domova v rozsahu možností stanovených charakterem jejich činnosti.

V Úřadu působí Základní odborová organizace Odborového svazu státních orgánů a organizací na základě oznámení ze dne 30. října 2019. Průběžná komunikace mezi ní a zaměstnavatelem probíhala zejména v elektronické formě. Kontrola provedená Státním úřadem inspekce práce, oblastním inspektorátem v Praze, která se týkala problematiky BOZP a zejména součinnosti zaměstnavatele s odborovou organizací, nenalezla žádná pochybení.

Do služebního poměru bylo nově přijato 14 státních zaměstnanců. Tři státní zaměstnanci služební poměr ukončili. Do pracovního poměru pak byli přijati tři zaměstnanci, přičemž sedm zaměstnanců pracovní poměr ukončilo.

V rámci Úřadem zajišťované zvláštní části úřednické zkoušky pro obor služby 60 – Ochrana osobních údajů bylo vyzkoušeno celkem 22 žadatelů, z nichž 19 složilo zkoušku úspěšně. Tři žadatelé byli hodnoceni jako neúspěšní.

K 1. lednu 2020 činil evidenční stav 101 zaměstnanců, k 31. prosinci 2020 byl pak jejich počet 107.

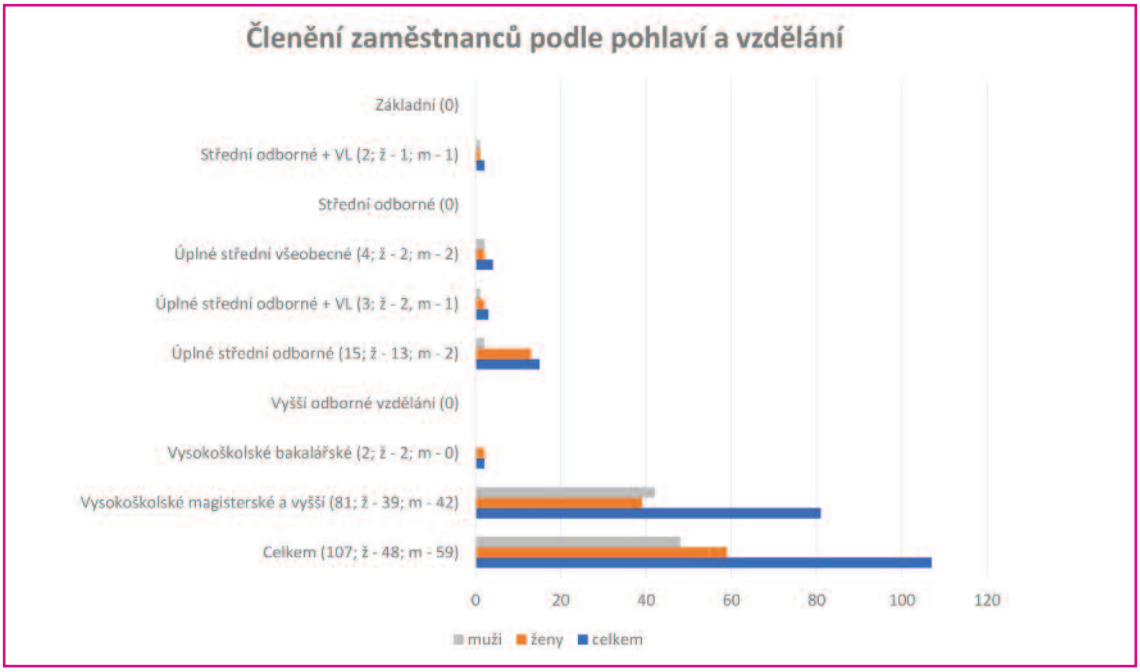
Průměrný evidenční přepočtený počet zaměstnanců za rok 2020 činil 104,95.

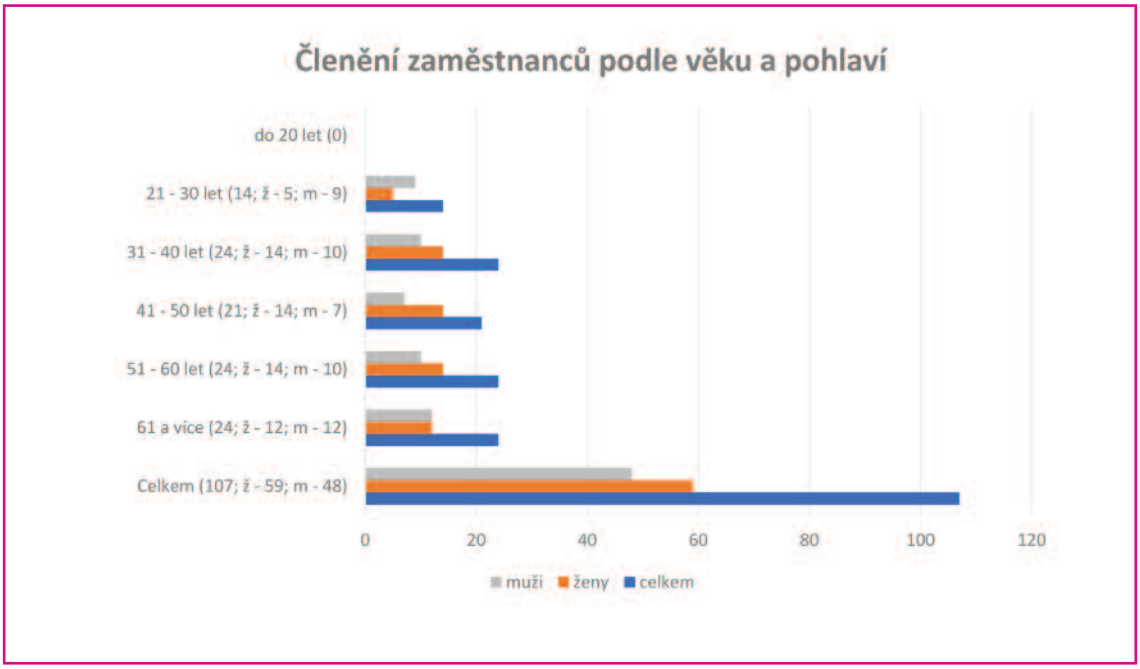
Dalších 41 osob vykonávalo v Úřadu činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr.

Z tabulky „Členění zaměstnanců podle věku a pohlaví" vyplývá, že v Úřadu pracují převážně zaměstnanci ve věku 40 let a výše. Tito zaměstnanci mají kromě odpovídajícího vzdělání i zkušenosti vyplývající z jejich dlouhodobé praxe. Řada z nich zde působí 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. Mohou například navštěvovat kurzy anglického a německého jazyka. Tyto 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, přičemž v roce 2020 vykonávali praxi v Úřadu celkem tři studenti. Tímto Úřad podporuje jejich zájem o problematiku ochrany osobních údajů a zároveň tak vyhledává nové potenciální zaměstnance.





HOSPODAŘENÍ

Rozpočet Úřadu byl schválen zákonem č. 355/2019 Sb., o státním rozpočtu České republiky na rok 2020.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů	v tisících Kč
Souhrnné ukazatele	
Příjmy celkem	7 280,15
Výdaje celkem	179 617,66
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	7 280,15
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	0,00
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	7 280,15
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	179 617,66
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	73 795,39
Povinné pojistné placené zaměstnavatelem*)	24 393,77
Základní příděl fondu kulturních a sociálních potřeb	1 412,34
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	11 105,41
Platy zaměstnanců na služebních místech dle zákona o státní službě	47 092,52

Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	12 418,08
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	19 299,95

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

1. PŘÍJMY

Příjmy pro rok 2020 nebyly schváleným rozpočtem stanoveny.
Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů byl naplněn částkou 7 280,15 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 2019 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2019).

2. VÝDAJE

Čerpání výdajů ve výši 179 617,66 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, ostatní výdaje za provedenou práci a související výdaje, vč. základního přídělu FKSP a náhrady v době nemoci ve výši **99 601,50 tisíc Kč** odpovídá kvalifikační struktuře a plnění plánu pracovníků.
Stav k 31. prosinci 2020 byl **107 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 **19 299,95 tisíc Kč**.

PŘEHLED ČERPÁNÍ ROZPOČTU V ROCE 2020

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2020 v tis. Kč	Konečný rozpočet 2020 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2020 v tis. Kč	Skutečný konečný rozpočet v %
2211, 2212, 2322, 2324, 4132	Ostatní nedaňové příjmy	0,00	0,00	7 280,15	0,00
	PŘÍJMY CELKEM	**0,00**	**0,00**	**7 280,15**	**0,00**
501	Platy	72 397,17	74 587,70	70 616,00	94,68
5011	Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	12 295,94	13 153,73	11 105,41	84,43
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	46 843,63	47 893,63	47 092,52	98,33
5014	Platy zaměstanců v prac. poměru odvoz. od platů úst. činitelů	13 257,60	13 540,35	12 418,08	91,71
502	Ostatní platby za provedenou práci	1 890,91	3 671,29	3 179,38	86,60
5021	Ostatní osobní výdaje	1 890,91	2 405,11	1 913,20	79,55
5024	Odstupné	0,00	215,18	215,18	100,00
5026	Odchodné	0,00	1 051,00	1 051,00	100,00
503	Povin. pojist. plac. zaměstnavatelem	25 109,37	25 109,37	24 393,77	97,15
5031	Povin. pojist. na sociál. zabezpečení	18 423,44	18 423,44	17 893,02	97,12
5032	Povin. pojist. na veřej. zdrav. pojištění	6 685,93	6 685,93	6 500,75	97,23
512	Výdaje na některé úpravy hm. věcí a pořízení některých práv k hm. věcem	20,00	11,00	0,00	00,00
513	Nákup materiálu	1 369,00	2 552,80	2 392,63	93,73
514	Úroky a ost. fin. výdaje	30,00	30,00	5,25	17,50
515	Nákup vody, paliv a energie	1 548,00	1 820,00	1 654,81	90,92
516	Nákup služeb	48 061,82	53 586,22	51 870,78	96,80

517	Ostatní nákupy	3 872,50	3 176,06	1 142,78	35,98	
518	Výdaje na netransfer. převody uvnitř organizace, na převzaté povinnosti a na jistoty	35,00	35,00	0,00	0,00	
519	Výdaje souvis. s neinv. nákupy, příspěvky, náhrady a věcné dary	3 282,10	3 493,90	3 126,90	89,50	
534	Převody vlastním fondům a ve vztahu k útv. bez plné práv. subjektivity	1 447,94	1 447,94	1 412,34	97,54	
5342	Základní příděl FKSP a soc. fondů obcí a krajů	1 447,94	1 447,94	1 412,34	97,54	
536	Ost. neinv. transf. jin. veřej. rozp. platby daní a další povinné platby	1300,00	37,86	16,59	43,82	
542	Náhrady plac. obyvatelstvu	200,00	510,00	506,48	99,31	
5424	Náhrady v době nemoci	200,00	510,00	506,48	99,31	
	Běžné výdaje celkem	**159 276,82**	**170 069,15**	**160 317,71**	**94,27**	
611	Pořízení dlouh. nehmot. majetku	6 000,00	8 309,65	1 834,25	22,07	
612	Pořízení dlouh. hmot. majetku	6 500,00	21 578,86	17 465,70	80,94	
	Kapitálové výdaje celkem	**12 500,00**	**29 888,51**	**19 299,95**	**64,57**	
VÝDAJE CELKEM		**171 776,82**	**199 957,66**	**179 617,66**	**89,83**	

Číselné údaje jsou použity z výkazů zpracovaných k 31. prosinci 2020.

PŘÍPRAVA A SCHVÁLENÍ ROZPOČTU NA ROK 2021 A STŘEDNĚDOBÝ VÝHLED

V rámci projednávání návrhu zákona o státním rozpočtu na rok 2021 došlo ze strany Ministerstva financí ke snížení rozpočtu, resp. celkových výdajů Úřadu o tři miliony Kč, tj. došlo ke snížení rozpočtu z 171 776,819 tisíc Kč v roce 2020 na 168 776,819 tisíc Kč v roce 2021 a další léta.

Vzhledem k tomu, že v souvislosti s tímto snížením rozpočtu schváleným pro rok 2021 je očekáván nedostatek finančních prostředků, které jsou potřebné pro zabezpečení všech zákonných úkolů Úřadu i jeho plánovaných investic, je nutné zajistit opětovné navýšení celkového rozpočtu Úřadu o tři miliony Kč. Tento požadavek Úřadu rovněž koresponduje s usnesením Petičního výboru Poslanecké sněmovny č. 175 z 3. listopadu 2020, které doporučilo zvýšit rozpočet kapitoly o požadované tři miliony Kč.

INTERNÍ AUDIT

Služební místo vnitřního auditora bylo v roce 2020 organizačně odděleno od řídicích a výkonných struktur. Auditor je funkčně nezávislý a je podřízen přímo předsedovi Úřadu.

Základní právní a regulatorní normy upravující činnost interního auditu v roce 2020:

- zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole),
- prováděcí vyhláška č. 416/2004 Sb. k zákonu o finanční kontrole ve veřejné správě.

Cíle vnitřního auditu v roce 2020:

- provádění funkčně nezávislého a objektivního přezkoumávání a vyhodnocování operací ekonomických, provozních a věcných agend Úřadu z pohledu zákona o finanční kontrole,
- provádění funkčně nezávislého a objektivního přezkoumávání funkčnosti a účinnosti vnitřního kontrolního systému zavedeného a udržovaného předsedou Úřadu tak, aby bylo dosahováno jeho zkvalitňování,
- zajišťování konzultační činnosti,
- zvyšování a prohlubování odbornosti auditora.

Roční plán interního auditu na rok 2020, schválený předsedkyní Úřadu dne 16. března 2020, vycházel ze střednědobého plánu, z výsledků předchozích auditů, z požadavků vedoucích zaměstnanců Úřadu a z kapacitních možností interního auditu.

Plnění ročního plánu interního auditu bylo v roce 2020 ztíženo personální změnou na služebním místě interního auditu a vlivem ztížených podmínek v souvislosti s nepříznivou epidemickou situací šíření onemocnění koronavirem COVID-19.

V roce 2020 byly zahájeny tři plánované audity, přičemž byl dokončen jeden mimořádný audit. Ten měl za úkol přezkoumat účelnost, efektivnost a hospodárnost vynaložených nákladů v souvislosti s prezentací Úřadu, jakož i správnost postupů a plnění povinností v souvislosti s prováděním řídicí kontroly. Výsledky tohoto auditu byly projednány s vedoucími zaměstnanci a s předsedkyní Úřadu.

V roce 2020 vnitřní audit nezjistil nedostatky s významným rizikem pro hospodaření s veřejnými prostředky. Zjištěné nedostatky nebyly takového charakteru, aby byly způsobilé zásadně ovlivnit výkon finančního řízení a funkčnost nastaveného vnitřního kontrolního systému. Dále nezjistil nic, co by nasvědčovalo tomu, že by účetní závěrka Úřadu neposkytovala věrný a poctivý obraz předmětu účetnictví, nebo že by došlo k porušení rozpočtové kázně. K nedostatkům střední a nízké významnosti zjištěným při výkonu interního auditu byla přijata adresná a konkrétní opatření a jejich realizace bude sledována a vyhodnocována. Známky korupčního či podvodného jednání nebyly v rámci auditní činnosti zjištěny.

Na základě výsledku auditních šetření lze poskytnout ujištění, že za rok 2020 je ve vybraných dílčích oblastech vnitřního provozního a finančního řízení 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.

Zjištěné nedostatky jsou impulzem pro zvýšení kvality kontrolního prostředí, kvality vnitřních předpisů a systémů dohledu nad jejich dodržováním, pro zvýšení důrazu na efektivní edukaci zaměstnanců a na ochranu práv a oprávněných zájmů Úřadu.

POVĚŘENKYNĚ PRO OCHRANU OSOBNÍCH ÚDAJŮ

Úřad jmenoval v souladu s čl. 37 obecného nařízení pověřence pro ochranu osobních údajů, jehož hlavní úkoly vyplývají z čl. 39 obecného nařízení. Pověřenec Úřadu především monitoruje soulad zpracování prováděného Úřadem s obecným nařízením a poskytuje informace a poradenství zaměstnancům, kteří se na zpracování osobních údajů podílejí. Zároveň zodpovídá dotazy subjektů údajů, jejichž osobní údaje zpracovává sám Úřad.

V roce 2020 v činnosti pověřence převažovala konzultační činnost uvnitř Úřadu spojená především s oblastmi výkonu služby/práce z jiného místa prostřednictvím elektronické komunikace, zabezpečených vzdálených přístupů do využívaných systémů a uživatelských oprávnění, kybernetické bezpečnosti či pandemie COVID-19. Pověřenkyně mj. oslovila zaměstnance ohledně práce z domova a společně s manažerkou kybernetické bezpečnosti provedla kontrolu informačního systému Úřadu.

Ve vztahu k veřejnosti se pak jednalo o otázky k obecným situacím a pojmům ochrany osobních údajů, kterými byly např. práva subjektů údajů, podání stížnosti, nevyžádaná obchodní sdělení či zrušení oznamovací povinnosti.

Zodpovídání tohoto druhu dotazů však do působnosti pověřence nespadá, o čemž je veřejnost informována i prostřednictvím webových stránek Úřadu.

ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2020 a informace o jejím předání proběhne v řádném termínu do 31. července 2021 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 2020
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 březnu 2021 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, 2021

ISBN 978-80-210-9835-0