



Úřad pro ochranu  
osobních údajů

VÝROČNÍ ZPRÁVA

2022





Úřad pro ochranu  
osobních údajů

VÝROČNÍ ZPRÁVA

2022





# ● **Obsah**

(interaktivní)

<b>Slovo předsedy</b>	<b>7</b>
<b>Úřad 2022</b>	<b>10</b>
<b>Milníky roku 2022</b>	<b>11</b>
<b>Ochrana osobních údajů</b>	<b>12</b>
<b>Cookies výzvou roku</b>	12
<b>Závěry z kontrol</b>	14
Osobní údaje poslanců na sociálních sítích	15
Kontrola aplikací Tečka/čTečka	15
Únik rodných čísel do zahraničí	15
Zpracování katastrálních dat	16
Používání trackovacích odkazů v rámci rozesílaných SMS	17
Ztráta spisu stavebním úřadem	18
Kamerový systém v prostorách nemocnice	19
Telefonická nabídka nákupu dluhopisů	20
Zabezpečení osobních údajů	20
Zpracování osobních údajů soudními exekutory	21
<b>Z rozhodnutí předsedy Úřadu</b>	22
Zvýšená ochrana zranitelných osob	22
Identifikace subjektu, jehož jménem jsou rozesílána obchodní sdělení	22
<b>Soudní přezkum vybraných rozhodnutí Úřadu</b>	23
Pokuta nemocnici za nedostatečné zajištění bezpečnosti osobních údajů	23
Odložení věci jako úkon předcházející správnímu řízení	24
<b>Častá témata podnětů a stížností</b>	24
COVID-19	25
Stížnosti na zaměstnavatele	25
Školy	25
Obce	26
Vyhledávače a jiné platformy	26
Kopírování občanských průkazů	26
Obchodní sdělení a neplnění informační povinnosti	26
Zpřístupňování osobních údajů SVJ a bytovými družstvy neoprávněným příjemcům	26
Ztěžování výkonu práv subjektu údajů podle obecného nařízení	27
<b>Ohlášení porušení zabezpečení osobních údajů</b>	27
<b>Závěry z konzultační činnosti</b>	28
Zasílání obchodních sdělení ve zdravotnictví	28
Doložení nepřítomnosti žáka lékařským potvrzením	28

Český jazyk a výkon funkce pověřence pro ochranu osobních údajů	29
Souhlas se zpracováním zvláštní kategorie osobních údajů v online platformě	29
Doručení volebních lístků s uvedením data narození voliče na obálce	29
<b>Závěry z analytické činnosti</b>	30
Problematika právní úpravy DNA z pohledu ochrany osobních údajů	30
<b>Národní legislativa</b>	32
<b>Unijní legislativa</b>	33
<b>Přehled oblastí upravených pokyny EDPB</b>	34
Pokyny 01/2022 k právům subjektu údajů – právo na přístup	34
Pokyny 04/2021 týkající se kodexů chování jakožto nástrojů pro předávání	35
Pokyny 02/2022 k uplatňování článku 60 GDPR	35
<b>Vývoj v oblasti předávání údajů do třetích zemí, kodexů chování a certifikací</b>	35
Předávání údajů do třetích zemí	35
Standardní smluvní doložky	36
Závazná podniková pravidla (BCR)	36
Kodexy chování a certifikace jako bezpečné nástroje předávání	37
Předávání údajů do USA	37
Předávání údajů v rámci využívání různých služeb	37
Osvědčení o ochraně osobních údajů (certifikační mechanismy)	38
Kodexy chování	39
<b>Závazná rozhodnutí podle čl. 65 GDPR</b>	39
Zpracování jako nezbytnost pro splnění smlouvy	39
<b>Nevyžádaná obchodní sdělení</b>	41
Shrnutí dozorové činnosti v oblasti šíření obchodních sdělení	41
Závěry z dozorové činnosti v oblasti nevyžádaných obchodních sdělení	42
<b>Rozhodování Úřadu v oblasti svobodného přístupu k informacím</b>	44
<b>Působnost Úřadu</b>	44
<b>Poznatky z rozhodovací praxe Úřadu a z judikatury</b>	45
Informace o probíhajícím trestním řízení – žádost o poskytnutí textu trestního oznámení	45
Přípustnost přezkumného řízení – aplikace zásady non bis in idem	46
Informace o fakturách za právní služby poskytnuté obci	46
Vyluka z práva na informace z důvodu ochrany autorského práva	46
Poskytnutí kopie výplatní pásky vedoucího zaměstnance	46
Aplikovatelnost ustanovení § 168 odst. 2 stavebního zákona jako speciálního důvodu pro odmítnutí žádosti o informace podané podle zákona o svobodném přístupu k informacím	47
Náklady za mimořádně rozsáhlé vyhledání požadovaných informací nepodléhají dani z přidané hodnoty	47
Soudní exekutor není povinným subjektem dle zákona o svobodném přístupu k informacím	47



Určení nadřízeného orgánu příspěvkové organizace kraje – rozsudek Nejvyššího správního soudu ze dne 16. 2. 2022, č. j. Komp 3/2021-26	47
<b>Organizační zajištění rozhodování Úřadu v oblasti svobodného přístupu k informacím</b>	<b>48</b>
<b>Informační systém ORG</b>	<b>49</b>
<b>O činnosti</b>	<b>52</b>
<b>Společné a koordinované kontroly</b>	52
<b>Schengenská spolupráce</b>	53
<b>Poradenství a konzultace</b>	54
<b>Evropská a zahraniční spolupráce</b>	55
Evropský sbor pro ochranu osobních údajů	55
Mechanismus spolupráce	56
Oblast předávání osobních údajů do třetích zemí a mezinárodním organizacím	56
Oblast osvědčení o ochraně osobních údajů (certifikační mechanismy)	57
Oblast Kodexů chování	57
Světové shromáždění pro ochranu soukromí (GPA)	57
Rada Evropy	57
Jarní konference	58
<b>Poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím</b>	58
<b>Komunikace s médii</b>	60
<b>Vyřizování stížností podle § 175 správního řádu</b>	61
<b>Fungování Úřadu</b>	<b>62</b>
<b>Personální obsazení Úřadu</b>	62
<b>Pověřenec pro ochranu osobních údajů Úřadu</b>	63
<b>Hospodaření úřadu</b>	64
<b>Účetní závěrka</b>	67
<b>Zpráva auditora</b>	67
<b>Úřad v číslech</b>	<b>68</b>
<b>Počet stížností a podnětů</b>	68
Hlavní oblasti stížností	69
<b>Dozorová činnost Úřadu</b>	70
<b>Úřad a poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím</b>	71
<b>Rozhodování předsedy Úřadu</b>	72
Přijatá podání k nadřízenému správnímu orgánu (§ 175 správního řádu)	72
<b>Soudní přezkum rozhodnutí (předsedy) Úřadu</b>	72
<b>Legislativa</b>	72
<b>Komunikace</b>	73
<b>Seznam použitých zkratk</b>	<b>75</b>







## • Slovo předsedy

Vážené dámy, vážení pánové,

ochrana osobních údajů byla v roce 2022 vystavena několika důležitým mezníkům. Doznívající dopady pandemie onemocnění COVID-19 byly zásadním celoevropským tématem pro otevřenou debatu nad způsoby a účely zpracování osobních údajů. V České republice v této souvislosti především rezonovalo zachování respektu k ochraně soukromí. V rámci metodické a dozorové činnosti Úřadu pro ochranu osobních údajů jsme indikovali řadu nestandardních postupů a pochybení, o kterých se dozvíte více v dalších částech této výroční zprávy.

Dynamický rozvoj informačních a komunikačních technologií přesouvá významnou část komunikace do virtuálního prostoru a směřuje tak dominantně k digitální komunikaci. Ta je spojena zčásti nevyhnutelně, zčásti arbitrárně s ohromným a neustálým zpracováním osobních údajů. Zneužití velkého množství osobních údajů jak v důsledku kriminální činnosti, tak samotnými správci těchto údajů, a s tím související skandalizace některých platform v zahraničí, vedly k zásadnímu zintenzivnění ochrany osobních údajů jak na úrovni orgánů Evropské unie, tak i národních dozorových úřadů. Ochrana soukromí a osobních údajů ale paradoxně začala opravdu zajímat i ty, jichž se týká především, tedy subjekty údajů, až v okamžiku, kdy vlivem pandemie onemocnění COVID-19 vzrostl tlak veřejných institucí i soukromých subjektů na objem a kvalitu osobních údajů, včetně osobních údajů zvláštní kategorie, které jsme všichni byli povinni poskytovat nebo jejichž poskytování nám bylo alespoň doporučováno. Úřad si je trvale vědom citlivosti těchto údajů, a proto například provedl hloubkovou kontrolu zabezpečení zpracování osobních údajů v rámci aplikací, které s údaji o očkování pracovaly („Tečka“ a „čTečka“), a požadoval maximální úroveň zabezpečení údajů o zdravotním stavu osob. Zájem jednotlivců i veřejnosti na dostatečné ochraně osobních údajů je také zřejmý z počtu podání adresovaných Úřadu v loňském roce, kdy bylo podáno 1 528 stížností ve vlastní věci a 664 podnětů ve veřejném zájmu.

V naší kontrolní a zejména metodické činnosti jsme se snažili brát maximální ohledy na výjimečnost a – doufejme – i neopakovatelnost

této krizové situace, přesto jsme k některým věcem nemohli mlčet, neboť je naší povinností chránit osobní údaje. Problém je navíc širší: nedostatek věcné informovanosti o některých přijímaných opatřeních, stejně jako hypertrofie zásahů do soukromí i v případech, kdy bylo možné najít méně invazivní řešení, mohly umožnit dílčí úspěch skupin, které v rámci odporu vůči proticovidovým opatřením šířily často zcela anti-systémové postoje. Vysoká míra veřejnoprávní ingerence do soukromí občanů, doprovázená nedostatečným respektem k rozhodovací praxi správních soudů, tak vedla k erozi identifikace části společnosti s Českou republikou a jejími orgány jakožto vlastním státem.

Než se stačila právní situace v České republice navrátit do předcovidového standardu fungování ústavních institucí, rozpoutala ruská agrese na Ukrajině další společenskou krizi. V ní se daří masivním a cíleně distribuovaným dezinformacím, tedy snahám agresora o vnitřní destabilizaci spojeneckých zemí. Jsou podnikány sofistikované hackerské a kybernetické útoky na veřejné i soukromé informační systémy s hlavním motivem podkopat důvěru ve stát. Toto vše je velmi úzce propojeno s dosud nebývalým úsilím o zneužívání osobních údajů. I proto Úřad pro ochranu osobních údajů v řadě konkrétních případů úzce spolupracoval se svými partnery nejen v rámci EU, ale také s domácími institucemi, zejména pak s Národním úřadem pro kybernetickou a informační bezpečnost.

Jakkoli lze doufat, že se nejedná o nevratný stav, skutečnost, že skupiny, které více či méně otevřeně podporují ruskou agresi, mají vůbec nějakou společenskou odezvu, naznačuje, že budování České republiky jako demokratického právního státu, s nímž se bude identifikovat naprostá většina společnosti jako se svojí vlastí, je nyní zásadní výzvou pro všechny osobnosti i subjekty veřejného života a zejména pro orgány veřejné moci. Úřad pro ochranu osobních údajů obnovení důvěry ve stát, prostřednictvím důsledné ochrany osobních údajů, resp. soukromí občanů, bude i nadále považovat za prioritu mezi svými úkoly, a to jak v metodické, tak i ve své kontrolní činnosti.

Rok 2022 kromě COVIDu-19 a hybridní války proti svobodnému světu přinesl v oblasti ochra-

ny osobních údajů také několik zcela „normálních“, ale přesto zásadních výzev. Ať už to byla novela zákona o elektronických komunikacích, která znamenala změnu principu vyjádření souhlasu pro zaslání obchodních sdělení, způsoby a nastavení využívání cloudových služeb ve veřejné správě nebo zahájení implementace klíčových evropských nařízení v oblasti regulace společné digitální agendy, a to včetně dosud na evropské úrovni nevyřešené právní kodifikace předávání osobních údajů do třetích zemí.

S postupující propojeností informací, které o nás ve virtuálním prostoru existují, nabývá stále více na významu skutečnost, že zpracování osobních údajů je přeshraniční. Proto musí být přeshraniční i ochrana osobních údajů. V této souvislosti považuji za nejvýznamnější počín uplynulého roku společné koordinované vymáhání ochrany osobních údajů podle pravidel obecného nařízení (GDPR). Zapojili jsme se společně s dalšími 21 evropskými úřady do první akce svého druhu, kterou inicioval Evropský sbor pro ochranu osobních údajů. Společná akce dozorových úřadů byla věnována využívání cloudových služeb veřejnými subjekty. Volba tohoto tématu vycházela ze zjištění evropské statistické agentury Eurostat, že využívání cloudových služeb se v zemích Evropské unie za uplynulých šest let zdvojnásobilo. Využívání cloudových služeb přitom doprovází nové kybernetické a bezpečnostní výzvy, kterým tak musejí být přizpůsobeny i mnohem vyšší nároky na ochranu osobních údajů a soukromí. K podrobnější informaci velmi doporučuji zalistovat v textu výroční zprávy, kterou máte právě před očima.

Pro další rozvoj ochrany osobních údajů je ovšem také velmi důležité nezapomínat ani na skutečnost, že právní prostředky veřejné moci ke shromažďování osobních údajů jsou na nesrovnatelně vyšší úrovni než v soukromém sektoru. To akcentuje i význam vyšší míry odpovědnosti právě veřejného sektoru za ochranu soukromí jednotlivce a jeho osobních údajů. Není dobré, pokud se – např. při přípravě legislativy s faktickými dopady pro ochranu osobních údajů – toto téma bagatelizuje a obchází. I z tohoto důvodu jsme iniciovali novelu legislativních pravidel vlády, v jejímž důsledku



s účinností od 1. 4. 2023, ve vztahu k ochraně soukromí a osobních údajů, nově obsahují legislativní pravidla vlády obdobné náležitosti jako je posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR. V současné době je k veřejné konzultaci publikována naše metodika a po jejím uzavření budou mít subjekty legislativního procesu, resp. jednotliví legislativci, podle našeho soudu z hlediska ochrany osobních údajů, dostatečný nástroj ke skokovému zkvalitnění návrhů právních předpisů.

Důvodem této naší iniciativy ke změně legislativních pravidel vlády byla skutečnost, že v legislativní i aplikační praxi často registrujeme, že velké zaujetí veřejné správy pro využívání nových informačních a komunikačních technologií je vedeno snahou přiblížit se dynamice obvyklé v privátním prostředí. Zároveň s tím ovšem často abscentuje dostatečné technické povědomí o tom, jak je s osobními daty v takových informačních a komunikačních systémech nakládáno, jakými algoritmy jsou zpracovávány, kam jsou předávány a kdo je může, bez jakýchkoli komplikací, získat a využívat. Nedostatky v této oblasti pak mohou vést k tomu, že osobní údaje nemusejí být vždy zpracovávány výlučně k obecně prospěšným cílům a v zájmu osob, jejichž údaje stát takto spravuje.

Vážené dámy, vážení pánové, výroční zpráva Úřadu pro ochranu osobních údajů za rok 2022 přináší přehled toho nejvýznamnějšího, čím jsme se zabývali, jaká témata jsme řešili a jaké výzvy byly v uplynulém roce spojeny s ochranou osobních údajů a soukromí. Loňský rok se stal dalším potvrzením narůstajícího významu obezřetnosti a zodpovědnosti nejen státu, ale každého z nás při nakládání s osobními údaji. Budu rád, pokud se tato výroční zpráva Úřadu pro ochranu osobních údajů stane vaší inspirací.

S úctou

**MGR. JIŘÍ KAUCKÝ**  
předseda Úřadu

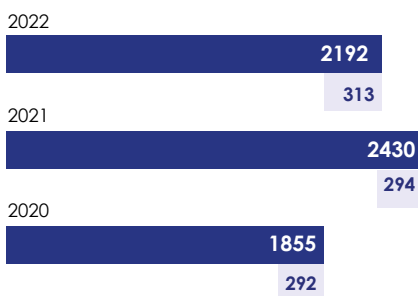
“ Ruská agrese na Ukrajině rozpoutala další společenskou krizi. V ní se daří masivním a cíleně distribuovaným dezinformacím a snahám o vnitřní destabilizaci spojeneckých zemí. Jsou podnikány sofistikované hackerské a kybernetické útoky na veřejné i soukromé informační systémy s cílem podkopat důvěru ve stát. Toto vše je přitom velmi úzce propojeno s dosud nebývalým úsilím o zneužívání osobních údajů. ”



# • Úřad 2022

## Ochrana osobních údajů

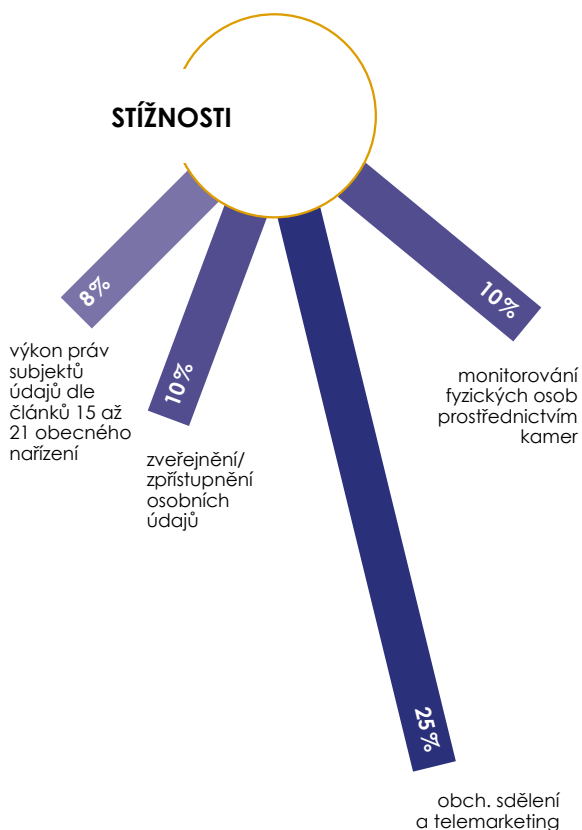
Úřad provádí dozorovou činnost v oblasti ochrany osobních údajů upravenou především obecným nařízením a zákonem č. 110/2019 Sb., o zpracování osobních údajů. Ta spočívá v provádění kontrol, vedení správních řízení o pokutě či o nápravném opatření, případně v komunikaci se správci a zpracovateli, která zahrnuje i dopisy upozorňující na možné porušení právních předpisů.



## PODNĚTY A STÍŽNOSTI

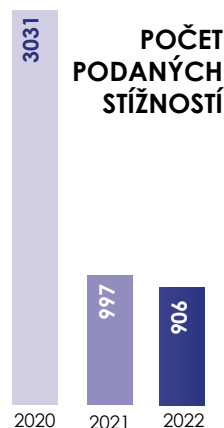
● celkový počet  
● ohlášení porušení zabezpečení osobních údajů (data breach)

## Vybrané oblasti podaných stížností v roce 2022



## Nevyžádaná obchodní sdělení

Úřad vykonává i působnost podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů. Ta spočívá především v dozoru a kontrole šíření nevyžádaných obchodních sdělení elektronickou formou, které je prováděno v rámci podnikatelské činnosti právnických i fyzických osob.

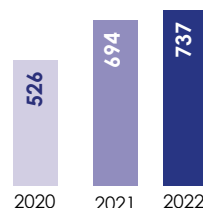


## Svobodný přístup k informacím

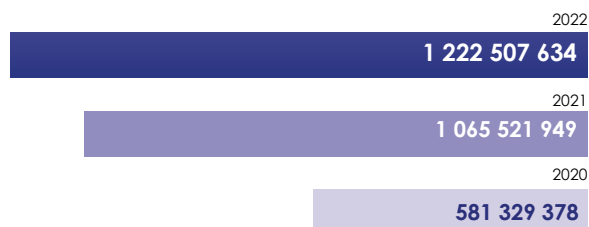
Úřad je nadřízeným orgánem těch povinných subjektů, jejichž nadřízený orgán nelze určit podle § 178 správního řádu. Úřad je v oblasti svobodného přístupu k informacím rovněž přezkumným orgánem oprávněným přezkoumávat pravomocná rozhodnutí nadřízených orgánů vydaná v odvolacím řízení. Úřad je též příslušný k přijímání opatření proti ne-

činnosti nadřízených orgánů v této oblasti.

## SROVNÁNÍ NÁPADU



## POČET TRANSAKČÍ V LETECH 2020–2022



## Zdrojové identifikátory fyzických osob / IS ORG

Úřad je správcem a provozovatelem autonomního informačního systému základních registrů. Ten zajišťuje ochranu osobních údajů občanů uložených v základních registrech České republiky.

## Komunikace

kumulovaný mediální zásah (GRP) s tématem ochrany osobních údajů v ČR v roce 2022





## • Milníky roku 2022

### • VYUŽÍVÁNÍ CLOUDOVÝCH SLUŽEB VEŘEJNOU SPRÁVOU V ZEMÍCH EU

Napříč evropskými dozorovými úřady proběhla koordinovaná kontrolní akce (CEF 2022), jejímž iniciátorem byl Evropský sbor pro ochranu osobních údajů (EDPB). Tematické zaměření bylo orientováno na využívání cloudových služeb. To se v Evropské unii za uplynulých šest let zdvojnásobilo. Přejít na cloudové služby přitom klade vysoké nároky na ochranu osobních údajů a využívání nevhodných produktů či nespolehlivých služeb může znamenat jejich ohrožení. Více v kapitole [O činnosti](#).

### • EVROPSKÁ DIGITÁLNÍ AGENDA

V říjnu vstoupilo v platnost nařízení o digitálních službách (*Digital Services Act, DSA*). To představuje jednu z nejvýznamnějších nových regulací elektronického obchodu. Doprovodným je pak nařízení o digitálních trzích (*Digital Markets Act, DMA*) nastavující pravidla pro přístup k digitální infrastruktuře prostřednictvím nových povinností pro tzv. *gatekeepers* (vyhledávače, sociální média nebo cloudové služby). Dalšími zásadními dokumenty jsou nařízení o správě dat (*Data Governance Act, DGA*) a nařízení o umělé inteligenci (*Artificial Intelligence Act, AIA*). Více v kapitole [Unijní legislativa](#).

### • APLIKACE TEČKA A ČTEČKA

Úřad dokončil v roce 2022 kontrolu, jejímž předmětem bylo dodržování povinností Ministerstva zdravotnictví při zpracování osobních údajů subjektů údajů v souvislosti s elektronickým certifikátem EU COVID-19. Více v kapitole [Závěry z kontrol](#).

### • REZERVAČNÍ SYSTÉM PRO OČKOVÁNÍ A OCHRANA OSOBNÍCH ÚDAJŮ

Zpracovatel osobních údajů jako dodavatel online rezervačního systému očkování porušil zabezpečení ochrany osobních údajů z důvodu chybné funkcionality systému webových stránek. Ta umožnila zobrazení čísla pojištění (a tím také rodného čísla) včetně jeho následného přenosu do USA, a to prostřednictvím nástroje pro získávání statistických dat Google Analytics. Díky tomu došlo k úniku 80 tisíc autentických rodných čísel českých občanů do zahraničí. Více v kapitole [Závěry z kontrol](#).

### • ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ POSLANCŮ

Zveřejnění adres trvalých pobytů poslanců je zpracováním osobních údajů identifikovatelných fyzických osob, a to bez ohledu na to, kdy k jednotlivým adresám není přiřazeno jméno, příjmení nebo jiný další osobní údaj subjektu údajů. Prostřednictvím adresy trvalého pobytu je možné přímo kontaktovat subjekt údajů, což je i samotným účelem zpracování osobních údajů. Takový subjekt je tak dosažitelný a identifikovatelný, a to i bez znalosti jména a dalších identifikátorů. Více v kapitole [Závěry z kontrol](#).

## • Ochrana osobních údajů

### • COOKIES VÝZVOU ROKU

Na základě novely zákona č. 127/2005 Sb., o elektronických komunikacích, která nabyla účinnosti 1. ledna 2022<sup>1</sup>, byl v rámci zpřesnění transpozice Směrnice o soukromí a elektronických komunikacích výslovně upraven pro soubory cookies tzv. režim opt-in (*princip aktivního souhlasu*). Ten v praxi znamená, že každý, kdo hodlá používat nebo používá síť elektronických komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních účastníků nebo uživatelů, získá od těchto účastníků nebo uživatelů předem prokazatelný souhlas s rozsahem a účelem jejich zpracování. Tato povinnost neplatí pro technické ukládání nebo přístup výhradně pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací nebo je-li to nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem.

Pro podporu, správnou orientaci a srozumitelnost novely Úřad pro ochranu osobních údajů připravil a na svých internetových stránkách zveřejnil [informační materiál k vysvětlení předmětného souhlasu s cookies soubory](#) udělovaného prostřednictvím cookie lišt. Téma bylo ve zvýšené míře frekventované hned od počátku roku 2022, a to jak v agendě stížností subjektů údajů (tj. uživatelů/návštěvníků českých webů), tak v agendě konzultací, kam se často obracely subjekty údajů i správci.

V návaznosti na obdržené stížnosti Úřad velmi často upozorňoval na nedostatky poskytovaného souhlasu, které se promítly v obsahu tzv. cookie lišty. Případně byly poskytované informace o využívání cookies chybné, nepřesné či neúplné. V důsledku takové situace nebyly splněny veškeré definiční znaky souhlasu podle čl. 4 bodu 11 nařízení (EU) 2016/679 (GDPR), tedy že se musí jednat o svobodný, konkrétní, informovaný a jednoznačný projev vůle. Šlo o případy, kdy se volba odmítnout využívání cookies

<sup>1</sup> Zákon č. 374/2021 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů a některé další zákony.



nacházela až v dalších vrstvách poskytovaných informací. Uživatel tak neměl možnost využití cookies odmítnout stejně jednoduše jako udělit souhlas. Jakkoliv část správců akceptovala názor Úřadu, někteří správci považovali umístění možnosti odmítnutí využívání cookies v jiné vrstvě webové stránky, než ve které byla umístěna možnost přijmout využívání cookies, za zákonu vyhovující. To však Úřad neakceptuje.

Při poskytování konzultací se často objevovalo téma opakovaného zobrazování cookie lišty. Tato skutečnost může v určitých případech (např. při zobrazování cookie lišty při každém zobrazení webové stránky) vést k nepřímému nátlaku na uživatele k udělení souhlasu (tj. absentovalo by naplnění požadavku na svobodně udělený souhlas, upravený v rámci čl. 4 bodu 11 obecného nařízení). Rovněž z dotazů provozovatelů webových stránek především menšího rozsahu bylo zřejmé, že postrádají bližší vodítka k nastavení četnosti zobrazování předmětné lišty. Na základě uvedeného Úřad doplnil výše uvedený informační materiál ve vztahu k souhlasu s cookies udělenému prostřednictvím tzv. cookie lišty.

Doba, po kterou je platně udělen souhlas se zpracováním osobních údajů prostřednictvím cookies, i doba pro opětovné zobrazení cookie lišty v případě odmítnutí udělit souhlas musí být stanovena správcem s ohledem na účel, ke kterému jsou osobní údaje zpracovávány, a současně s ohledem na očekávání subjektů údajů. Opětovné zobrazení cookie lišty by nemělo narušovat činnosti uživatele při používání webové stránky, ať už souhlas udělil, či odmítl udělit.

Obecně lze za přiměřenou dobu, na kterou byl souhlas s využíváním cookies udělen, považovat 12 měsíců, přičemž v praxi se Úřad zatím neseťkal s případem, kdy by správce odůvodnil delší dobu. V případě, že uživatel odmítl souhlas udělit, nemělo by být jeho udělení znovu vyžadováno alespoň 6 měsíců od posledního zobrazení cookie lišty. Tato doba může být kratší, pokud:

- se významně změnila jedna nebo více okolností zpracování,
- provozovatel není schopen sledovat předchozí souhlas/nesouhlas (např. uživatel smazal cookies uložené ve svém zařízení).

Za významnou změnu zpracování lze považovat zcela nové nastavení cookie lišty a účelu zpracování nebo takovou změnu, u které lze předpokládat, že uživatel, který odmítl udělit souhlas, by jej nově udělit mohl (např. výrazné omezení počtu subjektů – správců a zpracovatelů; nebo např. u analytických cookies dojde ke změně zpracovatele a osobní údaje již nebudou předávány mimo EU). Jelikož souhlas se zpracováním osobních údajů prostřednictvím cookies je udělován ke konkrétnímu účelu a určeným subjektům (správcům), nelze považovat za významnou změnu zpracování jednotlivých cookies.

V této souvislosti je třeba upozornit na to, že dojde-li k významné změně zpracování, která by měla vliv i na uživatele, kteří dříve souhlas se zpracováním osobních údajů udělili, bude nezbytné znovu požádat o udělení souhlasu s tímto novým zpracováním i tyto uživatele.

Úřad pouze nereagoval na obdržené dotazy či stížnosti, ale přistoupil proaktivně a komplexně k celé problematice a v průběhu roku 2022 provedl množství šetření jednak na základě obdržených stížností, jednak na základě vlastních poznatků.

Bylo provedeno 35 hloubkových analýz webů, kdy se mimo nastavení souhlasu a plnění informační povinnosti Úřad zaměřil i na to, aby zjistil, jakým způsobem se chovají cookies používané na jednotlivých webech a zda se chovají způsobem, který správce deklaruje. Na základě těchto šetření Úřad identifikoval typová opakování se porušení obecného nařízení Evropské unie o ochraně osobních údajů (GDPR). V první řadě se jednalo o výše už zmíněné nesprávné nastavení cookie lišty, jejímž prostřednictvím dochází k udělení souhlasu s používáním souborů cookies. Problémem je umístění tlačítka pro odmítnutí udělení souhlasu s využitím souborů cookies do druhé vrstvy cookie lišty, případně podoba tlačítka v první vrstvě, kdy toto bylo ukryto mezi dalšími poskytovanými informacemi. Takovou praxi Úřad pokládá za porušení požadavku na svobodu souhlasu podle čl. 4 odst. 11 GDPR, resp. zásady korektnosti a transparentnosti podle čl. 5 odst. 1 písm. a) GDPR.

V některých případech bylo na předmětných internetových stránkách nepřiměřeně obtížné

(či nemožné) dohledat způsob, kterým lze již udělený souhlas odvolat. Pokud udělení souhlasu a jeho odvolání není stejně snadné, jde o porušení čl. 7 odst. 3 GDPR.

Úřad se setkal také s nastavováním neúměrné doby platnosti souborů cookies vzhledem k jejich účelu. V této souvislosti Úřad narazil na případy, ve kterých byla platnost souborů cookies nastavena na dobu několika desítek, ba i stovek let (tedy, nesrovnatelně déle, než by byla lhůta v daných případech akceptovatelná). Takovou praxi hodnotí Úřad jako v rozporu s čl. 5 odst. 1 písm. e) GDPR, tedy zásadou omezení uložení.

Úřad jako opakující se problém dále identifikoval nepřesnou klasifikaci jednotlivých souborů cookies. Správci internetových stránek v některých případech zjevně zcela rezignovali na sdělení účelu jednotlivých souborů cookies. Též docházelo k nesprávnému zařazení souborů cookies podléhajících nutnosti udělení souhlasu mezi technické cookies, na něž se povinnost získat souhlas (princip opt-in) nevztahuje. V důsledku toho mohlo dojít ke zpracování osobních údajů bez řádného právního titulu. Úřad se setkal rovněž s případy, kdy správce sice správně klasifikoval soubor cookie jako podléhající udělení souhlasu, nicméně i přesto již před jeho udělením docházelo skrze takové cookies ke zpracování osobních údajů. Taková praxe zakládá porušení čl. 6 odst. 1 GDPR.

Návštěvníci internetových stránek v neposlední řadě podle zjištění Úřadu často nebyli správně informováni o předepsaných aspektech zpracování svých osobních údajů, což je minimálně v rozporu se zásadou korektnosti a transparentnosti podle čl. 5 odst. 1 písm. a) GDPR. Někteří správci buď neposkytovali všechny informace předepsané čl. 13 GDPR, případně v rozporu s čl. 12 odst. 1 informovali nedostatečným způsobem – typicky se jednalo o poskytnutí příliš obecných či nepřesných informací, nebo tyto byly poskytnuty pouze v cizím jazyce.

K využití cizího jazyka docházelo i v rámci provedení tlačítek pro souhlas a nesouhlas se zpracováním osobních údajů v rámci cookie lišt, čímž z důvodu nesrozumitelnosti dochází k porušení podmínek souhlasu jakožto pro-



jevu vůle, který musí být svobodný, konkrétní, informovaný a jednoznačný. Ojedinele byla lišta zobrazena tak, že zakrývala část viditelné plochy internetového prohlížeče, přičemž bylo znemožněno číst povinně sdělované informace. Taková praxe může být k návštěvníkům stránek nekorektní a netransparentní a může představovat porušení čl. 5 odst. 1 písm. a) GDPR.

Do budoucna se Úřad pro ochranu osobních údajů samostatně zaměří také na špatné nastavení cookie lišty, která je koncipována tak, že neumožňuje udělit nebo odmítnout souhlas ve stejné vrstvě, a nepřiměřeně časté a obtěžující objevování se cookie lišty poté, co subjekt údajů neudělil souhlas se zpracováním osobních údajů. Na základě výsledků šetření v oblasti cookies Úřad připraví rozšíření svých metodických materiálů.

## ZÁVĚRY Z KONTROL

Jednou z primárních pravomocí Úřadu je provádění kontrol podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), v rámci kterých Úřad vypracovává kontrolní protokoly obsahující zjištěná porušení právních předpisů.





## Osobní údaje poslanců na sociálních sítích

Předmětem kontroly bylo zveřejnění adres trvalého pobytu části poslanců Poslanecké sněmovny Parlamentu České republiky na sociálních sítích politickým hnutím.

Úřad v dané kontrole shledal, že „zveřejnění adres trvalých pobytů poslanců je zpracováním osobních údajů identifikovatelných fyzických osob, lhotejnost že k jednotlivým adresám nebylo přiřazeno jméno, příjmení nebo jiný další osobní údaj subjektu údajů. Prostřednictvím adresy trvalého pobytu bylo možné přímo kontaktovat subjekt údajů, což byl i samotný účel zpracování, určený kontrolovanou osobou, a tento subjekt tak byl dosažitelný, a tedy identifikovatelný, a to případně i bez znalosti jeho jména a dalších identifikátorů, s přihlédnutím ke všem prostředkům, které mohly být rozumně použity jak kontrolovanou osobou jakožto správcem osobních údajů, tak jakoukoli jinou osobou pro identifikaci daného subjektu údajů, například skrze informace přístupné dálkovým nahlížením do katastru nemovitostí“.

Úřad v této souvislosti shledal především porušení čl. 6 odst. 1 GDPR, neboť kontrolovaná osoba nedoložila, že by pro zpracování osobních údajů poslanců disponovala legitimním právním titulem. Nad rámec toho shledal Úřad porušení čl. 14 GDPR, neboť kontrolovaná osoba neplnila informační povinnost vůči subjektům údajů.

Následně bylo v této souvislosti zahájeno správní řízení, jehož předmět zahrnul i později obdržené stížnosti týkající se kontrolované osoby.

Úřad v této souvislosti připomíná, že prvním krokem každého zpracování osobních údajů je stanovení účelu, resp. jak stanoví GDPR ve svém čl. 5 odst. 1 písm. b): „osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.“ Takový účel pak musí být v první řadě legitimní, přičemž jak též vyplynulo z uvedeného případu, ani deklarovaný spekulativní účel nebylo možné hodnotit jako konformní s požadavky GDPR. Nestanoví-li si správce řádný účel, je na něm založené následné zpracování (bez ohledu na zkoumání právního titulu) od počátku stíženo vadou spočívající v porušení jedné ze základních zásad GDPR.

## Kontrola aplikací Tečka/čTečka

Úřad dokončil v roce 2022 kontrolu, jejímž předmětem bylo dodržování povinností Ministerstva zdravotnictví při zpracování osobních údajů subjektu údajů v souvislosti s elektronickým certifikátem EU COVID-19, zpřístupněným na očkovacím portálu [ocko.uzis.cz](https://ocko.uzis.cz), včetně aplikací „Tečka“ a „čTečka“.

V rámci této kontroly se Úřad zejména soustředil na povinnosti podle čl. 32 GDPR, tedy povinnosti týkající se zabezpečení zpracování osobních údajů.

Úřad shledal v rámci kontrolního protokolu, že kontrolovaná osoba „neplní povinnosti podle čl. 32 nařízení (EU) 2016/679, jelikož:

- v souvislosti s vydáváním původních certifikátů docházelo při načtení QR kódu čtečkou v mobilním zařízení ke zpřístupnění údaje o číslu pojištěnce držitele certifikátu;
- v aplikaci čTečka nebylo znemožněno pořízení screenshotu displeje, což je v rozporu se smyslem aplikace, tedy ověření platnosti certifikátů, bez zanechání elektronické stopy s osobními údaji o tomto ověření.“

Podané námitky předseda Úřadu zamítl. Zjištěná porušení kontrolovaná osoba následně napravila, nebyl tedy důvod zahajovat správní řízení o uložení nápravného opatření.

Úřad si je vědom citlivosti údajů o očkování, a proto provedl hloubkovou kontrolu zabezpečení zpracování osobních údajů v rámci aplikací, jež s těmito údaji pracovaly, a požadoval maximální úroveň zabezpečení údajů o zdravotním stavu.

## Únik rodných čísel do zahraničí

Úřad provedl kontrolu zpracovatele osobních údajů, a to dodavatele online rezervačního systému očkování. Předmětem kontroly bylo především porušení zabezpečení spočívající v chybě funkcionality systému webových stránek kontrolované osoby, která umožnila zobrazení čísla pojištěnce (a tím také rodného čísla) a jeho následný přenos do USA prostřednictvím nástroje pro získávání statistických dat Google Analytics.

Úřad provedl rozsáhlé šetření za účelem prověření autenticity udělených pokynů správce vůči zpracovateli (kontrolované osobě), na je-

jichž základě docházelo ke zpracování osobních údajů, včetně pokynů, které se týkaly vzniklého porušení zabezpečení, aby tak mohl spolehlivě určit odpovědnost za jeho vznik.

Úřad především konstatoval, že kontrolovaná osoba, jakožto další zpracovatel, je spolu se správcem odpovědná za porušení ustanovení čl. 32 odst. 1 písm. b) GDPR, neboť jako odborník neupozornila správce na nevhodnost pokynu k vytvoření systému, v rámci kterého URL adresa obsahovala číslo pojištěnce (rodné číslo) a tuto zpracovávala za současného použití služby Google Analytics, přičemž tímto došlo k úniku URL adres včetně čísel pojištěnců v rozsahu cca 80 tisíc subjektů údajů. Ve vymezeném období nebylo zpracování osobních údajů kontrolovanou osobou prováděno v souladu s GDPR, když se toto zpracování řídilo smlouvou, aniž by tato naplňovala atributy čl. 28 odst. 3 GDPR. Dále porušovala také čl. 37 odst. 1 GDPR, neboť pro zpracování nejmenovala pověřence pro ochranu osobních údajů.

Kontrola byla zásadně ztěžována přístupem správce, který po téměř celou dobu trvání kontroly odmítal (a to navzdory opakovaným výzvám Úřadu) potvrdit tvrzení zpracovatele, že pokyny k nastavení systému tak, že došlo k porušení zabezpečení, byly vydány jím. Tyto potvrdil až poté, co kontrolovaná osoba podala námitky proti kontrolním zjištěním. Tento přístup se negativně projevil do délky kontroly, neboť potvrzení pokynu mělo klíčový význam pro určení odpovědnosti (resp. podílu na ní) za porušení zabezpečení. Ve věci bylo zahájeno správní řízení.

V této souvislosti Úřad zdůrazňuje, že je oprávněn kontrolovat i zpracovatele osobních údajů (tedy nejenom správce, který je primárně za zpracování osobních údajů odpovědný), přičemž je to i zpracovatel, který může být spoluodpovědný (a v některých případech i samostatně odpovědný) za porušení GDPR.

### **Zpracování katastrálních dat**

Úřad společně s Českým úřadem zeměměřičským a katastrálním (ČÚZK) provedl kontrolu zpracování osobních údajů v rámci služeb poskytovaných kontrolovanou osobou. Kontrolovaná osoba poskytovala mimo jiné služby zalo-

žené na zpracování katastrálních dat, přičemž na tyto služby se kontrola primárně zaměřila.

Kontrolovaná osoba kategoricky odmítala, že by v rámci služeb, v jejichž rámci zpracovává osobní údaje vlastníků nemovitostí v České republice, byla v pozici správce. Dále kontrolovaná osoba ke konci roku 2021 ze svých serverů vymazala software, který zajišťoval provoz služeb, jež byly předmětem kontroly, a všechna s ním související data.

V rámci kontroly bylo dále v datech extrahovaných od poskytovatele IT služeb pro kontrolovanou osobu nalezeno 427 300 rodných čísel. Argumentace kontrolované osoby, že není v roli správce osobních údajů vlastníků nemovitostí, byla vyvrácena na základě skutečností zjištěných mimo jiné na základě studia dat získaných od poskytovatele IT služeb pro kontrolovanou osobu a na základě dat poskytnutých ČÚZK. Z těchto dat vyplývalo, že kontrolovaná osoba v rámci poskytovaných služeb nevyužívala osobní údaje dostupné skrze oficiální dálkový přístup do katastru nemovitostí, nýbrž musela využívat svoji databázi osobních údajů, čímž se nacházela bez jakýchkoliv pochybností v postavení správce osobních údajů, jež zpracovávala nejméně v rozsahu jméno, příjmení, adresa trvalého bydliště, seznam vlastněného nemovitého majetku. Z této databáze byla následně získávána data pro jednotlivé klienty, kteří předmětné služby kontrolované osoby využívali.

Úřad v rámci kontroly shledal množství porušení, mimo jiné porušení čl. 14 odst. 1 GDPR, protože kontrolovaná osoba nedoložila, že by v souvislosti s databází vlastníků/spoluvlastníků nemovitostí informovala subjekty údajů, jejichž osobní údaje byly zpracovávány, o podmínkách tohoto zpracování. Dále Úřad shledal porušení čl. 24 odst. 1 obecného nařízení, jelikož kontrolovaná osoba v rámci kontroly nepředložila podklady dokládající plnění opatření dle čl. 25 odst. 1 a čl. 32 odst. 1 GDPR, přijatá v souvislosti s provozem této databáze a porušení čl. 30 odst. 1 nařízení GDPR, protože do doby vydání kontrolního protokolu nepředložila záznamy o činnostech zpracování.

V rámci kontrolního protokolu bylo v souladu s ustanovením § 10 odst. 2 zákona č. 255/2012 Sb. o kontrole (kontrolní řád), uloženo kontrolova-



né osobě podání písemné zprávy o odstranění nedostatků zjištěných kontrolou, a to ve lhůtě 30 dnů ode dne formálního ukončení kontroly ve smyslu § 18 zákona č. 255/2012 Sb.

Kontrola byla ukončena marným uplynutím lhůty pro podání námitek. V návaznosti na učiněná zjištění bude v roce 2023 zahájeno správní řízení.

Článek 5 odst. 2 GDPR zakotvuje nejen odpovědnost správce za dodržování povinností podle GDPR, ale upravuje též jeho odpovědnost doložit dodržování tohoto souladu. Správce se tedy nemůže zprostit odpovědnosti například tím, jak se o to pokusila kontrolovaná osoba, že smaže předmětný software a s ním spojené osobní údaje. Správce je stále odpovědný za to, aby doložil soulad jím prováděného zpracování osobních údajů s GDPR, nedoložení tohoto souladu zakládá porušení GDPR a lze jej trestat pokutou.

Dále je třeba uvést, že plnění informační povinnosti, ať již podle čl. 13 či 14 GDPR, je zcela zásadní povinností správce osobních údajů. Pouze řádně informovaný subjekt údajů má možnost se kvalifikovaně rozhodnout, zda své osobní údaje svěří správci, či zda neuplatní některé ze svých práv, jež mu dle GDPR náleží. Pokud subjekt údajů nemá reálnou představu o tom, jak zpracování jeho osobních údajů probíhá, je mu tato možnost odepřena a ve svém důsledku tím může v některých případech až znemožnit právo svobodné volby subjektu údajů stran toho, jakým způsobem může být s jeho osobními údaji nakládáno. Pokud pak Úřad dospěje k závěru, že ze strany správce došlo k takovému jednání proto, že se před subjekty údajů snažil utajit, jakým způsobem nakládá s osobními údaji, může se jednat o přestupek obdobně závažný jako například zpracování osobních údajů bez řádného právního titulu podle čl. 6 odst. 1 GDPR.

### **Používání trackovacích odkazů v rámci rozesílaných SMS**

Předmětem kontroly bylo zpracování osobních údajů v souvislosti s rozesíláním SMS výzvy k instalaci aplikace eRouška. Kontrolovaná osoba byla oslovena ze strany Ministerstva zdravotnictví se žádostí o rozeslání informačních SMS všem svým zákazníkům. Této žádosti kontrolovaná osoba vyhověla, avšak nad rámec této žádosti

do každé SMS přidala unikátní odkaz za účelem evidování prokliků na stránky, kde bylo možné stáhnout aplikaci eRouška. Na základě těchto informací disponovala kontrolovaná osoba informacemi o tom, zda bylo z telefonu konkrétního telefonního čísla odkazu užito. Smyslem tohoto odkazu mělo podle kontrolované osoby být předejít opakovanému rozesílání SMS zákazníkům, kteří si již aplikaci stáhli, a tím do budoucna také minimalizace nákladů v případě potřeby rozesílání dalších SMS s podobným obsahem.

Úřad po provedení kontroly a posouzení všech okolností konstatoval, že zpracování osobních údajů v rozsahu telefonního čísla a informace o prokliku na stránku vedoucí k instalaci aplikace eRouška prováděla kontrolovaná osoba bez řádného zákonného titulu a příjemce SMS zpráv řádně neinformovala o zpracování jejich osobních údajů a neprokázala provedení vhodných technických a organizačních opatření při zpracování osobních údajů, čímž porušila čl. 6 odst. 1 GDPR, čl. 13 GDPR a čl. 32 GDPR.

V dané věci správce rozporoval i skutečnost, že se jedná o zpracování osobních údajů, čemuž Úřad nemohl přisvědčit, neboť kontrolovaná osoba disponovala informací o tom, že došlo z konkrétního telefonního čísla k prokliku na určitou internetovou stránku, což jsou informace, které jsou ve smyslu GDPR osobními údaji.

Zákonnost zpracování postavila kontrolovaná osoba na svém oprávněném zájmu ve smyslu čl. 6 odst. 1 písm. f) GDPR. K tomuto Úřad v kontrolním protokolu shledal:

*„Oprávněný zájem kontrolovaná osoba odůvodnila tak, že účelem pro umístění trackovacího odkazu bylo vedení evidence počtu unikátních prokliků na stránky, kde bylo možné stáhnout aplikaci eRouška, kde smyslem této evidence bylo předejít opakovaní rozesílky na účastníky, kteří si již aplikaci stáhli. Kontrolovaná osoba dále uvedla, že zpracovávala pouze informaci o tom, že uživatel (subjekt údajů) klikl na eRoušku, informaci o tom, zda byla aplikace stažena, kontrolovaná osoba nezjistila.*

*Základem posouzení proporcionality vždy musí být posouzení kritéria vhodnosti, tedy zda zvolený prostředek může sloužit vytyčenému účelu zpracování osobních údajů. Na základě uvedených podkladů pak kontrolující konstatují, že de-*

klarovaného účelu kontrolovaná osoba nemohla zvoleným prostředkem dosáhnout. Kontrolovaná toliko evidovala informaci o prokliku na stránky, kde bylo možné stáhnout aplikaci eRouška, nikoli to, zda došlo ke stažení předmětné aplikace. Z tohoto důvodu tak nemohly být naplněny podmínky titulu pro zpracování osobních údajů podle čl. 6 nařízení (EU) 2016/679, neboť v takovém případě (nevhodnosti použitého prostředku k dosažení deklarovaného cíle) nelze mít za to, že převáží oprávněné zájmy kontrolované osoby nad zájmy a právy subjektů údajů.“

Stran porušení informační povinnosti správce ve smyslu čl. 13 GDPR Úřad uvedl, že jakkoliv kontrolovaná osoba měla na svých webových stránkách v části Zásady zpracování osobních údajů uvedeny informace taxativně vymezené v čl. 13 odst. 1 a 2 GDPR, tyto informace byly dostupné pouze na internetové adrese a subjekt údajů, který klikl na odkaz v přichozi SMS, je neměl v okamžiku získání osobních údajů kontrolovanou osobou k dispozici. Takový postup byl v rozporu s čl. 13 GDPR.

Proti všem kontrolním zjištěním podala kontrolovaná osoba námitky, které byly vypořádány zamítnutím, protože k předmětnému zpracování osobních údajů došlo bez řádného zákonného titulu a kontrolovaná osoba nesplnila informační povinnost. Stran závěrů k právnímu titulu zpracování uvedl předseda Úřadu v rámci vyřízení námitek: „Z žádosti MZČR o rozesílku předmětných SMS nikterak nevyplývá, že by se žádost měla opakovat. Kontrolovaná osoba tak pouze na základě svých úvah předpokládala několik vln rozesílek, ke kterým však nedošlo. Zájem kontrolované osoby byl tedy pouze hypotetický (...) V případě zpracování osobních údajů podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 je třeba vzít v úvahu také to, zda subjekt údajů takové zpracování může důvodně očekávat (viz odst. 47 preambule GDPR.) (...) Mám za to, a to i vzhledem k nedostatečnému informování subjektů údajů (...), že průměrný uživatel (adresát předmětné SMS) zpracování svých osobních údajů prostřednictvím kliknutí na odkaz neočekával.“

Vyhověno bylo pouze námitce směřující proti kontrolnímu zjištění spočívajícímu v neprokázání vhodných technických a organizačních opatření při zpracování osobních údajů.

Ve věci bylo následně zahájeno správní řízení.

Právní titul pro zpracování osobních údajů podle čl. 6 odst. 1 písm. f) GDPR spočívá v tom, že zpracování osobních údajů je zákonné, pokud „zpracování 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 pak musí být poměřován i kritériem vhodnosti. Pokud nemůže zvolený prostředek dosáhnout vytyčeného cíle, nemůže být z povahy věci shledáno naplnění podmínek čl. 6 odst. 1 písm. f) GDPR.

### Ztráta spisu stavebním úřadem

Předmětem kontroly byla ztráta správního spisu stavebním úřadem, přičemž Úřad se zaměřil na možnost systémového pochybení města (kontrolované osoby) při vedení spisové služby, což bylo v rámci kontroly vyloučeno.

Úřad však u ztráty konkrétního spisu vyhodnotil, že toto porušení zabezpečení osobních údajů mělo být městem zadokumentováno (povinnost daná čl. 33 odst. 5 GDPR) a ohlášeno Úřadu (povinnost dle čl. 33 odst. 1 GDPR). Kontrolovaná osoba tyto povinnosti nesplnila, jelikož ztrátu spisu za porušení zabezpečení nepovažovala. Tomu však Úřad nemohl přisvědčit, neboť ani v době kontroly nebylo zřejmé, zda je spis skartován, ztracen v rámci budovy (např. přiřazením k jinému spisu) či došlo k manipulaci se spisem neoprávněnou osobou, která by jej stále mohla mít v držení. Ztráta spisu, který obsahuje též osobní údaje, může v takovém případě nepochybně vést k riziku pro práva a svobody fyzických osob.

Proti kontrolním zjištěním kontrolovaná osoba nepodala námitky, v následném správním řízení byla příkazem shledána vinnou z porušení zjištěných v rámci kontroly, proti čemuž nepodala odpor. Pokuta městu za spáchané přestupky nebyla uložena. Od uložení správního trestu bylo upuštěno ve smyslu § 62 odst. 5 zákona č. 110/2019 Sb., o zpracování osobních údajů. Podle tohoto ustanovení Úřad musí upustit od potrestání orgánů veřejné moci a veřejných subjektů.

Ohlašování případů porušení zabezpečení osobních údajů podléhá ohlašovací povinnos-



ti podle čl. 33 GDPR (ohlášení Úřadu), příp. též dle čl. 34 GDPR (oznámení subjektu údajů). Pro ohlašovací povinnost je rozhodné riziko pro práva a svobody fyzických osob:

- pokud je nepravděpodobné, že by porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob, správce případ porušení zabezpečení zadokumentuje podle čl. 33 odst. 5 GDPR, ohlášení Úřadu nebo subjektu údajů neprovádí,
- pokud je pravděpodobné, že porušení zabezpečení bude mít za následek riziko pro práva a svobody fyzických osob, správce případ porušení zabezpečení zadokumentuje podle čl. 33 odst. 5 GDPR a provede ohlášení Úřadu podle čl. 33 odst. 1, 3 a 4 GDPR,
- pokud je pravděpodobné, že porušení zabezpečení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, správce případ porušení zabezpečení zadokumentuje podle čl. 33 odst. 5 GDPR, provede ohlášení Úřadu podle čl. 33 odst. 1, 3 a 4 GDPR a nadto provede oznámení subjektu údajů podle čl. 34 GDPR.

GDPR počítá s tím, že veškeré informace, které mají být ohlášeny dozorovému úřadu (čl. 33 odst. 3 GDPR), nemusí mít správce okamžitě k dispozici (ohlášení musí být provedeno bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm správce dozvěděl). V takovém případě lze učinit prvotní ohlášení ve stanovené lhůtě a informace postupně doplňovat bez dalšího odkladu (čl. 33 odst. 4 GDPR), jakmile je správce bude mít k dispozici na základě svého dalšího šetření.

### **Kamerový systém v prostorách nemocnice**

Předmětem kontroly bylo zpracování osobních údajů při využívání kamerového systému v prostorách konkrétní kliniky nemocnice.

Zavedení kamerového monitorovacího systému ve vnitřních prostorách kliniky mělo být podle vyjádření kontrolované osoby pouze podpůrným procesem pro detekci vzniku nežádoucích stavů pacientů a nedílnou součástí celkové léčby pacienta. Kontrolovaná osoba založila zpracování osobních údajů na čl. 6 odst. 1 písm. c) GDPR, tj. na zákonném základě (zákon č. 372/2011 Sb., o zdravotních službách, a vy-

hláška č. 98/2012 Sb., o zdravotnické dokumentaci). Zpracování zvláštních kategorií osobních údajů pacientů pak mělo být zdůvodněno výjimkou podle čl. 9 odst. 2 písm. i) GDPR, kdy je zpracování nezbytné z důvodu veřejného zdraví a slouží k zajištění přísných norem kvality a bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických přípravků. Zákon o zdravotních službách ani vyhláška o zdravotnické dokumentaci však nestanoví povinnost provádět sledování stavu pacientů pomocí videokamer. V průběhu kontroly navíc vyplynulo, že v období posledních 10 let nebylo do kamerových záznamů nahlíženo. Úřad konstatoval, že kontrolované osobě pro užití kamerového monitorovacího systému ve vnitřních prostorách kliniky právní titul ve smyslu čl. 6 odst. 1 písm. c) GDPR nesvědčí.

K využití kamerového systému ve vnějších prostorách kontrolovaná osoba prokázala oprávněný zájem dle čl. 6 odst. 1 písm. f) GDPR. Oprávněný zájem spočívá v ochraně majetku nemocnice, prevenci před vandalismem a v ochraně života a zdraví osob vstupujících do prostor nemocnice. Proti kontrolním zjištěním kontrolovaná osoba nepodala námitky.

Je nutno zdůraznit, že konstatované porušení povinnosti dané čl. 6 odst. 1 GDPR (zákonost zpracování) se vztahuje ke konkrétně deklarovaným účelům a skutečností zjištěným při kontrole. V teoretické rovině by kamerový monitorovací systém ve vnitřních prostorách mohl být provozován v souladu s čl. 6 odst. 1 písm. f) GDPR (oprávněný zájem správce nebo třetích stran). Správce osobních údajů by však musel prokázat, že pro konkrétní účely má tento oprávněný zájem přednost před zájmy nebo základními právy a svobodami subjektu údajů.

V obecné rovině je pak třeba zdůraznit, že sama skutečnost, že správcem deklarovaný právní titul, o který opírá předmětné zpracování osobních údajů, nelze užít, neboť nejsou naplněny jeho podmínky, nemusí nutně znamenat, že zpracování osobních údajů je prováděno bez právního titulu, pokud na dané zpracování dopadá správcem nedeklarovaný právní titul. Deklarace nepřiléhavého právního titulu však může mít vliv na porušení těch ustanovení GDPR, jež jsou vázána na specifický právní

titul. Jako příklad lze uvést právo vznést námitku ve smyslu čl. 21 odst. 1 GDPR, jež je spojeno se zpracováním osobních údajů opírajícím se o právní tituly podle čl. 6 odst. 1 písm. e) nebo f) GDPR. Pokud je tedy správce mylně přesvědčen, že předmětné zpracování osobních údajů je opřeno například o čl. 6 odst. 1 písm. c) GDPR, může toto přesvědčení vést v důsledku k tomu, že nedovolí subjektům údajů uplatnit právo vznést námitku.

### Telefonická nabídka nákupu dluhopisů

Kontrolovaná osoba mimo jiné zastávala názor, že vygenerované telefonní číslo není osobním údajem. Tento názor považuje Úřad za rozporný s GDPR a proto v protokolu uvedl: „Náhodně vygenerované telefonní číslo je osobním údajem. Prostřednictvím tohoto čísla je možno daný subjekt v určitém časovém úseku přímo kontaktovat, a tento subjekt je tak dosažitelný a jistým způsobem určitelný, a to případně i bez znalosti jeho jména a dalších údajů. Je totiž spojeno s identifikovatelnou fyzickou osobou jako kontaktní údaj. Fyzickou osobu může bez vynaložení mimořádného úsilí a nákladů s využitím svých legálních a technických možností identifikovat také např. telefonní operátor. V případech, kdy jde o spojení telefonního čísla a dalších identifikačních údajů (např. veřejný telefonní seznam, uvedení kontaktů veřejně na internetu), jsou fyzické osoby identifikovatelné i dalšími subjekty včetně kontrolované osoby bez vynaložení mimořádného úsilí a prostředků.“

V této souvislosti kontrolující shledali, že předmětné zpracování osobních údajů bylo prováděno bez řádného právního titulu.

U kontrolované osoby bylo v souvislosti s jiným zpracováním osobních údajů dále zjištěno, že souhlas se zpracováním osobních údajů udělovaný subjekty údajů není svobodný, neboť spojoval více účelů (zasílání obchodních sdělení; zjištění relevantních potřeb; nabídka a poskytování investičních příležitostí; péče o klienta; nabízení dalších produktů a služeb), pro které měl být udělován vždy samostatný souhlas.

Úřad dále konstatoval porušení čl. 30 odst. 1 GDPR, neboť kontrolovaná osoba jako správce osobních údajů nevedla záznamy o činnostech

zpracování, ačkoli na ni tato povinnost dopadala.

Jak vyplývá i z pokynů Evropského sboru pro ochranu osobních údajů č. 5/2020, služba může zahrnovat několikero zpracování pro vícero účelů. V takových případech by subjekty údajů měly mít možnost si svobodně zvolit, který účel přijmou, a neměly by muset souhlasit se souborem účelů zpracování. Pokud správce sloučil několik účelů zpracování a nepokusil se získat samostatný souhlas pro každý účel, není souhlas dostatečně svobodný.

### Zabezpečení osobních údajů

V nočních hodinách k došlo k neoprávněnému vstupu do prostor kontrolované osoby, během kterého byly odcizeny tři kusy počítačů.

Následnou kontrolou zahájenou na základě podnětu bylo zjištěno, že užívané prostory nebyly zabezpečeny kamerovými systémy ani systémem detekce pohybu. V buňkách uvnitř haly se nacházely počítače, na kterých zaměstnanci kontrolované osoby uskutečňovali registraci klientů. V oddělené místnosti serverovny se původně nacházel odcizený serverový počítač.

Jeden z odcizených notebooků obsahoval hardware s instalovaným přihlašovacím rozhraním do vzdálených databází. Po zjištěném bezpečnostním incidentu přijala společnost opatření v podobě blokace přihlašovacího protokolu do vzdálené databáze. Incident byl společností ohlášen Policii ČR. Při šetření Policií ČR byly odcizené notebooky nalezeny.

Ve spolupráci s Policií ČR Úřad provedl analýzu nalezených počítačů. Dva notebooky nesly znaky reinstalace, nebyly v nich identifikovány soubory s osobními údaji. Ve třetím notebooku bylo velké množství osobních údajů klientů. Tyto bylo možné získat z aktuální databáze i uložených záloh databáze informačního systému. Úřad zjistil, že k souborům, které byly v odcizeném počítači, nebylo vyžadováno ověření uživatele a současně nebyly šifrované. Bylo konstatováno, že přístup k osobním údajům mohl získat každý, kdo měl po odcizení počítačů k zařízení přístup.

O vzniklém bezpečnostním incidentu společnost před provedením místního šetření neinformovala.



movala Úřad ani dotčené návštěvníky centra. Ohlášení porušení zabezpečení ve smyslu čl. 33 GDPR bylo přitom učiněno až v průběhu kontroly.

Úřad dále zjistil, že funkci pověřence pro ochranu osobních údajů u kontrolované osoby vykonával provozní ředitel kontrolované osoby.

Úřad zjistil následující porušení: (1) nebyla přijata vhodná technická a organizační opatření k zabezpečení osobních údajů; (2) ve lhůtě nebylo nahlášeno porušení zabezpečení osobních údajů Úřadu, přičemž nebyl uveden důvod opožděného ohlášení; (3) nebylo ohlášeno porušení zabezpečení dotčeným subjektům údajů; (4) nebyl jmenován pověřenec pro ochranu osobních údajů, byť docházelo ke zpracování zvláštní kategorie osobních údajů, přičemž toto zpracování bylo rozsáhlé; (5) Úřadu nebyly sděleny kontaktní údaje na pověřence pro ochranu osobních údajů; (6) nebylo zajištěno, aby jmenovaný pověřenec pro ochranu osobních údajů nebyl ve střetu zájmů ve spojitosti s úkoly, které plní u kontrolované osoby.

Kontrolovaná osoba podala námitky proti kontrolnímu protokolu v celém rozsahu. Všechny námitky byly Úřadem shledány jako nedůvodné a ve věci bylo zahájeno správní řízení.

V této souvislosti předně Úřad doplňuje, že ačkoliv není jeho cílem trestat oběti útoků, které vynaložily adekvátní úsilí k zabezpečení osobních údajů, je jeho úkolem stíhat porušení povinností nahlásit mu bezpečnostní incidenty.

Pokud dopadá na správce povinnost jmenovat pověřence pro ochranu osobních údajů, je tento povinen mimo jiné zajistit, aby byl pověřenec náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů, aby měl k dispozici zdroje nezbytné k plnění úkolů pověřence tak, aby jiné povinnosti a úkoly mu uložené nevedly ke střetu zájmů pověřence. Není-li tomu tak, může se jednat o porušení minimálně čl. 38 odst. 1, 2 a 6 GDPR.

## **Zpracování osobních údajů soudními exekutory**

V roce 2022 Úřad dokončil kontrolu dvou soudních exekutorů.

První kontrolou bylo zjištěno, že nejméně po dobu jednoho měsíce chyběly na webo-

vých stránkách kontrolované osoby jako správce osobních údajů transparentní informace, sdělení a postupy pro výkon práv subjektů údajů podle čl. 12 GDPR.

Podle sdělení kontrolované osoby informace pro subjekty údajů chyběla pouze po dobu úpravy jejích webových stránek, z důvodu změny informační povinnosti o nahrávání telefonických hovorů. V průběhu kontroly uvedené porušení napravila, vložila na webové stránky kompletní informace včetně postupů pro výkon práv subjektu údajů a přijala vhodná opatření, aby poskytla subjektům údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článku 12 obecného nařízení.

Kontrola byla ukončena marným uplynutím lhůty pro podání námitek. Kontrolovaná osoba přijala vhodná opatření k nápravě zjištěného nedostatku. Proto již nebylo třeba ukládat kontrolované osobě opatření k odstranění zjištěného nedostatku ze strany Úřadu.

Předmětem druhé kontroly byla stížnost, jež se týkala doručení písemnosti stěžovateli a jeho nesouhlasu s rozsahem osobních údajů uvedených na výzvě vyvěšené na vstupních dveřích bytového domu v bydlišti stěžovatele.

V této souvislosti Úřad oslovil Exekutorskou komoru ČR, od které si vyžádal její pokyny či metodická doporučení týkající se postupu při doručování písemností exekutory podle zákona č. 99/1963 Sb., občanský soudní řád, a zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů. Exekutorská komora ČR ve vyjádření popsala způsoby doručování s odkazem na občanský soudní řád, podle kterého jsou exekutoři povinni postupovat.

Kontrolou bylo zjištěno, že exekutor při doručování výzvy k převzetí písemnosti povinné osobě (stěžovateli) v probíhajícím exekučním řízení uvedl na této výzvě nadbytečný osobní údaj, a to datum narození povinné osoby. V případě, že povinný neměl v místě bydliště označenou domovní schránku a nemohlo být doručeno osobně, měla být tato výzva k dobrovolnému plnění vrácena odesílajícímu soudu a v místě bydliště zanecháno adresátovi pouze

oznámení o uložení zásilky podle § 49 odst. 2 zákona č. 99/1963 Sb.

Kontrola byla ukončena marným uplynutím lhůty pro podání námitek.

Kontrolovaná osoba již v průběhu kontroly přijala opatření, zaměstnanec exekutora, soudní vykonavatel, který doručování prováděl, byl náležitě poučen. Vzhledem k tomu, že se jednalo o ojedinělé pochybení, nebyl důvod zahajovat řízení o odstranění zjištěných nedostatků.

## Z ROZHODNUTÍ PŘEDSEDY ÚŘADU

Předseda Úřadu rozhoduje o rozkladech, tedy opravných prostředcích proti rozhodnutí Úřadu, jako ústředního správního úřadu.

### Zvýšená ochrana zranitelných osob

Na základě podnětu stěžovatelky řešil Úřad neoprávněné předání osobních údajů mezi společnostmi, které zajišťují pro své klienty uzavření smlouvy na dodávku energií na základě výsledku aukce energií, a následné zpřístupnění údajů zpracovateli.

Stěžovatelka uzavřela v místě svého bydliště se společností A, a později i s obviněnou (společnost B, která byla se společností A propojena osobou jednatele), smlouvu o zajištění slev na dodávkách energií. Od obou smluv stěžovatelka následně řádně odstoupila, což bylo za obě společnosti akceptováno zákaznickým centrem obviněné. Přesto společnost A postoupila výše zmíněnou (tj. již ukončenou) smlouvu se stěžovatelkou obviněné. Přestože obviněná o ukončení smlouvy se společností A věděla a věděla tedy, že nedisponuje právním titulem pro zpracování osobních údajů stěžovatelky, předala tyto osobní údaje zpracovateli (obchodnímu zástupci), aby stěžovatelku kontaktoval za účelem uzavření nové smlouvy.

Za zpracování osobních údajů bez právního titulu a za neoprávněné zpřístupnění osobních údajů zpracovateli uložil Úřad obviněné pokutu ve výši 80 000 Kč. Jako k přitěžující okolnosti přihlédl Úřad k tomu, že obviněná spáchala svým jednáním více přestupků a tyto přestupky byly spáchány na osobě vysokého věku.

Předseda Úřadu měl za to, že stěžovatelku lze, vzhledem k jejímu věku (přes 80 let) a s ohledem

na skutečnost, že k hájení svých práv vůči správci využila pomoc svého příbuzného, považovat za zranitelnou osobu. Pojem „zranitelná osoba“ není ve vnitrostátním ani mezinárodním právu jednotně definován. Podle odst. 75 preambule GDPR jsou za zranitelné osoby považovány především děti. Blížší vymezení lze najít v Pokynech pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679 ze dne 4. dubna 2017, v aktualizovaném znění (WP 248 rev. 01 str. 12). Z uvedených pokynů vyplývá, že posouzení, zda dochází ke zpracování údajů týkajících se zranitelných subjektů údajů, je podstatné „kvůli větší nerovnováze moci mezi subjekty údajů a správcem údajů, což znamená, že pro jednotlivce může být nemožné snadno vyslovit souhlas, případně nesouhlas se zpracováním svých údajů, nebo vykonávat svá práva. Mezi zranitelné subjekty mohou patřit děti (u nichž lze mít za to, že nejsou schopny vědomě nebo promyšleně vyslovit nesouhlas, popřípadě souhlas se zpracováním svých údajů), zaměstnanci, zranitelnější skupiny obyvatelstva, které vyžadují zvláštní ochranu (osoby s duševní chorobou, žadatelé o azyl nebo starší osoby, pacienti atd.) a všichni ti, v jejichž případech je možné stanovit nerovnováhu ve vztahu mezi postavením subjektu údajů a správce“. Neoprávněným zpracováním stěžovatelčiných osobních údajů tak byly vyšší měrou ohroženy její základní práva a svobody.

### Identifikace subjektu, jehož jménem jsou rozesílána obchodní sdělení

Předseda Úřadu rozhodoval o rozkladu podaném obchodní společnosti proti rozhodnutí Úřadu, jímž byla tomuto podnikatelskému subjektu uložena pokuta ve výši 250 000 Kč za spáchání přestupku podle § 11 odst. 1 písm. a) bod 1 a bod 3 zákona č. 480/2004 Sb., o některých službách informační společnosti, kterého se dopustil tím, že rozeslal obchodní sdělení více než 266 tisícům adresátů, aniž by k tomu disponoval jejich souhlasem, a dále i tím, že předmětná obchodní sdělení neuváděla osobu, v jejíž prospěch se komunikace uskutečnila.

Předseda Úřadu prvostupňově rozhodnutí potvrdil, v odůvodnění pak především zdůraz-





nil, že odesílatel a subjekt, v jehož prospěch se obchodní sdělení odesílá, mohou být různé osoby. Ustanovení § 7 odst. 4 písm. b) zákona č. 480/2004 Sb. pak obsahuje podmínku, podle níž ze zaslání obchodního sdělení má být patrná totožnost odesílatele, jehož jménem se komunikace uskutečňuje. Tímto je právě podnikatel, resp. osoba, jejíž zboží, služba či image se propaguje, kterou je nutno v rámci rozesílky obchodních sdělení identifikovat, a nikoli ten, kdo pouze uskutečňuje vlastní rozesílku. Tento výklad podporuje i korespondující ustanovení čl. 6 písm. b) směrnice 2000/31/ES<sup>2</sup>, které vyžaduje, aby fyzická nebo právnická osoba, na jejíž objednávku obchodní sdělení probíhá, byla jasně rozeznatelná. Stejně tak lze odkázat na dosavadní výklad Úřadu a také připomenout rozhodnutí Městského soudu v Praze čj. 14 A 242/2018 ze dne 7. dubna 2020.

Z uvedených důvodů proto byl odmítnut názor dotčeného podnikatelského subjektu, podle něhož Úřad nepřípustně rozšířil skutkovou podstatu přestupku podle § 11 odst. 1 písm. a) bod 3 zákona č. 480/2004 Sb. Pro úplnost je pak nutno dodat, že v textu předmětných obchodních sdělení byly uváděny pouze odkazy na webové stránky nabízeného produktu, facebookové stránky, telefonní kontakt či e-mailová adresa třetí strany. Neobsahovaly však konkrétní identifikaci této třetí strany, v jejíž prospěch bylo obchodní sdělení šířeno.

## ● SOUDNÍ PŘEZKUM VYBRANÝCH ROZHODNUTÍ ÚŘADU

V roce 2022 bylo několik rozhodnutí Úřadu podrobena soudnímu přezkumu v rámci správního soudnictví. Pokud jde o ukončená soudní řízení, lze poukázat na tyto rozsudky:

- uložení pokuty nemocnici za nedostatečné zajištění bezpečnosti při zpracování osobních údajů ve vazbě na vedení elektronické zdravotní dokumentace,

- zamítnutí kasační stížnosti a institut odložení věci jako úkon předcházející správnímu (přestupkovému) řízení.

### Pokuta nemocnici za nedostatečné zajištění bezpečnosti osobních údajů

Nejvyšší správní soud (NSS) svým rozsudkem čj. 10 As 190/2020–39 ze dne 25. února 2022 potvrdil pokutu ve výši 40 000 Kč, uloženou v řízení vedeném Úřadem pod sp. zn. UOOU–08001/18 nemocnici – akciové společnosti za nedostatečné zajištění bezpečnosti při zpracování osobních údajů v souvislosti s vedením elektronické zdravotní dokumentace. NSS v tomto přelomovém rozhodnutí také konstatoval, že nemocnice – akciová společnost není z pohledu zákona č. 110/2019 Sb., o zpracování osobních údajů, veřejným subjektem, přestože je financována převážně z prostředků veřejného zdravotního pojištění.

NSS především odmítl aplikaci § 62 odst. 5 zákona č. 110/2019 Sb., o zpracování osobních údajů, který neumožňuje uložení sankce veřejnému subjektu. V této souvislosti konstatoval, že tento zákon definici veřejného subjektu neuvádí. Z povahy věci je ovšem zřejmé, že takový subjekt bude zpravidla zřízen zákonem a určen k plnění úkolů ve veřejném zájmu (jinak by totiž nebyl označován jako veřejný). Zároveň by neměl disponovat vlastním majetkem, protože finance bude čerpat z veřejných rozpočtů.

Naopak, zásadně bude nerozhodné, zda je veřejnou institucí ve smyslu zákona o svobodném přístupu k informacím či veřejným zadavatelem podle zákona o zadávání veřejných zakázek, a také to, zda vede zdravotnickou dokumentaci.

Dotčená nemocnice pak je akciovou společností s vlastním majetkem a hospodařením. Je financována převážně z prostředků veřejného zdravotního pojištění, což však nelze brát jako čerpání peněz z veřejných rozpočtů. Nemocnice jakožto akciová společnost totiž nedostává peníze na svůj provoz a fungování přímo z veřejných rozpočtů. Získává je jako protiplnění za konkrétní úkony a pacienty, které „vykáže“ zdravotním pojišťovnám. Shodným způsobem je ostatně financován jakýkoli jiný poskytovatel lékařské péče (soukromá nemocnice či soukromý lékař).

<sup>2</sup> Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)

Byť tedy dotčená nemocnice poskytuje zdravotní péči, která jistě je ve veřejném zájmu, je akciovou společností, která nečerpá finance z veřejných rozpočtů. Není tak veřejným subjektem, u něhož by mělo být podle § 62 odst. 5 zákona č. 110/2019 Sb., o zpracování osobních údajů rozhodnuto o upuštění od potrestání.

Dále, jak NSS uvedl, ačkoli čl. 32 GDPR vykazuje oproti někdejšímu ustanovení § 13 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů, jisté drobné formulační rozdíly, nelze dovozovat, že by GDPR oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů, kladlo, co se týká zabezpečení osobních údajů, na správce či zpracovatele nižší požadavky, a to i v souvislosti s vedením elektronické zdravotní dokumentace. Pořizování tzv. logů, které umožní následně určit a ověřit, z jakého důvodu bylo do předmětné dokumentace nahlíženo, tak zůstává důležitou součástí příslušných opatření. Proto již v samotném logu musí být obsažena nejen informace o tom, kdo a kdy osobní údaje zpracovával, ale i důvod tohoto zpracování. Nelze tedy spoléhat na možnost následného pohovoru s osobou, která přistupovala do databáze, jelikož takto není možno provést řádnou průběžnou ani následnou kontrolu, zda nedocházelo k neoprávněnému přístupu.

### **Odložení věci jako úkon předcházející správnímu řízení**

NSS svým rozsudkem čj. 5 As 128/2021–38 ze dne 18. května 2022 zamítl kasační stížnost a potvrdil usnesení Městského soudu v Praze čj. 15 A 70/2020–51 ze dne 8. dubna 2021, podle něhož odložení věci bez dalších opatření je úkonem, který předchází zahájení správního (přestupkového) řízení. Zároveň implikuje skutečnost, že řízení zahájeno nebude, přičemž ze zákona neplyne veřejné subjektivní právo jednotlivce na to, aby správní orgán toto řízení zahájil, ať již na základě podnětu, oznámení či jiné formy sdělení skutečností, o kterých je jejich oznamovatel přesvědčen, že jsou pro zahájení přestupkového řízení relevantní.

Žalobkyně podala u Městského soudu v Praze proti Úřadu žalobu na ochranu před nečinností, ve které brojila proti tomu, že Úřad na základě jejího podnětu nezahájil žádné řízení.

Poté, co Městský soud v Praze žalobu odmítl, obrátila se s kasační stížností na NSS. Jak NSS uvedl, v projednávané věci bylo podstatné, že žádné řízení, v němž by mělo být vydáno rozhodnutí, zahájeno nebylo. V první řadě tak bylo třeba zabývat se tím, zda zahájeno být mělo. V případě, kdy je možno správní řízení zahájit jen z moci úřední a kdy mohou osoby k zahájení takového řízení dát pouze podnět, což nastalo v projednávané věci, je postup správního orgánu (Úřadu) upraven v § 42 správního řádu. Správní orgán v souladu s tímto ustanovením stěžovatelce sdělil, že neshledal důvody k zahájení řízení z moci úřední, a věc odložil. Stěžovatelka nebyla v postavení účastníka řízení, nemohla být tedy ani zkrácena na žádných svých procesních právech, jak tvrdila. Na tom nic nemění ani skutečnost, že jí Úřad umožnil nahlédnout do spisu, byť nebyla účastníkem řízení (neboť žádné neprobíhalo), jelikož ve spise, do něhož nahlížela, se nacházela výhradně její korespondence.

Dále NSS také konstatoval, že nezbytnou podmínkou úspěšnosti žaloby na ochranu před nečinností je zahájené správní řízení, neboť tímto okamžikem počíná plynout lhůta pro vydání rozhodnutí ve věci samé. Tato podmínka však splněna nebyla. Na základě podnětu stěžovatelky Úřad správní řízení nezahájil a stěžovatelka se tedy nemůže v rámci ochrany proti nečinnosti domáhat vydání rozhodnutí ve věci. Stejně tak se podanou žalobou nelze domáhat toho, aby soud správnímu orgánu nařídil správní řízení zahájit.

### **ČASTÁ TÉMATA PODNĚTŮ A STÍŽNOSTÍ**

Aby byla zajištěna náležitá ochrana osobních údajů, je mimo jiné nutné umožnit subjektu údajů, aby kromě práv podle čl. 12 až 22 obecného nařízení o ochraně osobních údajů a § 27 až 29 zákona č. 110/2019 Sb., o zpracování osobních údajů, měl možnost obrátit se na dozorový úřad se stížností podle čl. 77 GDPR a § 31 zákona č. 110/2019 Sb., o zpracování osobních údajů, na nedostatky při zpracování jeho osobních údajů. Úřad se zabývá rovněž jinými podněty, aby ověřil zákonnost zpracování osobních údajů.



## COVID-19

V první polovině roku se Úřad ještě zabýval podáními v souvislosti s povinnostmi podle protiepidemických opatření. Jednalo se zejména o ověřování certifikátů při vstupu například do restaurací či sportovišť. Další podání se vztahovala k povinnosti vyplňovat příjezdový formulář. V těchto případech obvykle nebylo shledáno pochybení správce, podatelé namítali pouhé ověření splnění podmínek pro vstup do provozoven.

Byl řešen podnět upozorňující na jednání vysoké školy, která nařídila studentům nahrávat potvrzení prokazující očkování proti nemoci COVID-19, testování či informace o prodělání nemoci do školního systému. Správce se domníval, že takové zpracování osobních údajů je povinen realizovat s ohledem na mimořádné opatření Ministerstva zdravotnictví MZDR 14600/2021-20/MIN/KAN, podle kterého byla vysoká škola povinna kontrolovat, zda studenti splňují jednu z podmínek uvedených v článku II. Opatření. Shromážděné osobní údaje dále uchovával, a to z důvodu schopnosti prokázat plnění povinností podle opatření. Úřad správce upozornil, že povinnost vést evidenci předmětných osobních údajů o zdravotním stavu studentů za účelem ubytování studentů uložena vysoké škole předmětným opatřením není. Naopak evidence v rozsahu např. jméno studenta a datum ověření (případně neověření) požadované skutečnosti pro ubytování bylo zcela v souladu s opatřením, a tedy i GDPR. Správce po upozornění Úřadu příkaz ke vkládání předmětných údajů do systému zrušil a uložené údaje vymazal.

## Stížnosti na zaměstnavatele

V této kategorii správců je velmi častým pochybením nevyřízení žádosti zaměstnance/bývalého zaměstnance související s výkonem jeho práv podle nařízení, typicky žádosti o výmaz. Správci po upozornění Úřadu na porušení obecného nařízení odpověď dotčené osobě poskytli, obvykle vysvětlili i původní absenci reakce a zaměstnanci se omluvili. V návaznosti na rychlou nápravu vzniklého pochybení ze strany správce Úřad řízení nezahájil. Úřad opakovaně řešil stížnosti na nezrušení pracovní e-mailové schránky

v případě ukončení pracovního poměru se zaměstnancem, a tedy další zpracování e-mailové adresy, která v rozsahu jméno, příjmení zaměstnance a doména správce jsou osobními údaji vlastníka schránky. V některých případech se jednalo o nedbalost, jindy byl však e-mail cíleně přesměrován na jiného pracovníka a dále monitorován, docházelo tak i k porušení listovního tajemství. Úřad správce upozorňoval na možné pochybení a ti to schránku zrušili. Dotčení bývalí zaměstnanci byli informováni o svém právu na náhradu případné újmy.

## Školy

Nejčastěji se Úřad zabýval stížnostmi a podněty souvisejícími se zpřístupňováním a zveřejňováním osobních údajů žáků, ale i pedagogů. Po upozornění Úřadem správci obvykle zveřejněné údaje odstranili. Nicméně vzhledem k nevratnému zásahu do soukromí subjektů údajů byly tyto subjekty informovány o jejich právu domáhat se náhrady újmy od správce, a to i prostřednictvím soudu. V případě stížnosti, podle které škola předala osobní údaje pedagoga jeho bývalému partnerovi, kdy se mj. jednalo i o informace o výkonu pracovní činnosti, absencích a ukončení pracovního vztahu pedagoga, tedy o osobní údaje týkající se zaměstnaneckého vztahu, se Úřad věcí dále zabývá, neboť pro takový postup správce nebyl shledán právní důvod.

Zpočátku roku se objevovala ještě podání související s výukou v období protiepidemických opatření. Jednalo se například o nahrávání třídních schůzek. Podle správce nahrávání spustil jeden z rodičů prostřednictvím aplikace MS Teams. Záznam byl následně automaticky v této aplikaci uložen. Škola uvedla, že pořizování videozáznamů v MS Teams v případě online výuky bylo znemožněno, v případě třídních schůzek takové jednání ze strany zákonných zástupců žáků předpokládáno nebylo, a proto zůstala možnost pořizování záznamu aktivována. Škola Úřadu sdělila, že k systematickému zpracování osobních údajů v podobě pořizování videonahrávek z třídních schůzek ze strany školy běžně nedochází. Na základě upozornění Úřadu škola přijala technická opatření spočívající v podobě změny nastavení v aplikaci MS

Teams, a to za účelem znemožnění pořizování videonahrávek z třídních schůzek realizovaných online jejich účastníky.

Stížnostmi týkajícími se zabezpečení osobních údajů, jež jsou zpracovávány v souvislosti s využíváním školního informačního systému, používání cookies a využívání Google Analytics, se Úřad dále zabývá. V případě, že dochází ke zpracování osobních údajů prostřednictvím Google Analytics, dochází k předání osobních údajů společnosti Google Inc. se sídlem v USA. Práva a povinnosti při předávání osobních údajů do třetích zemí jsou upraveny především v čl. 44 a násl. obecného nařízení. K jakémukoli předání osobních údajů, které jsou předmětem zpracování nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci, může dojít pouze tehdy, splní-li správce a zpracovatel podmínky podle obecného nařízení. USA na základě platné legislativy realizují plošný přístup státních orgánů k osobním údajům a nezajišťují dostatečnou ochranu předávaným údajům ani účinnou právní ochranu subjektům údajů. Podle rozhodnutí Evropské komise o standardních smluvních doložkách je zřejmé, že pokud vývozce a dovozce údajů dojdou k závěru, že standardní smluvní doložky nemohou být ve třetí zemi dodrženy, měly by být doplněny o další opatření, nebo přenos údajů bude zastaven.

## Obce

Podstatná část podání směřujících proti obcím se týká zveřejňování osobních údajů občanů obce na webových stránkách obce. Jedná se o případy, kdy jsou např. zveřejňovány dokumenty bez jakékoliv úpravy včetně osobních údajů či anonymizace nebyla provedena důsledně, případně byla zvolena chybná metoda, která umožnila následné zobrazení osobních údajů. Správci po upozornění Úřadu pochybení napravili, nicméně tato podání se stále opakují. Úřad v těchto případech stěžovatele informoval o jejich právu domáhat se náhrady újmy od správce, a to i prostřednictvím soudu.

Podatelé se na Úřad obraceli i ve věci zpracování osobních údajů v souvislosti s parkovacími systémy obcí, obvykle namítali rozsah požadovaných osobních údajů. V jednom případě vyžaduje město pro účely elektronické žádosti o vydání

parkovací karty od žadatele zaslání kopie občanského průkazu, které mají být dále uchovávány, byť má město přístup do registru obyvatel.

## Vyhledávače a jiné platformy

V této oblasti jsou častá podání týkající se ověřování totožnosti a věku (prostřednictvím kopie OP, bankovní identity či bankovního převodu). Obvykle nebylo shledáno pochybení. V případě jednoho vyhledávače probíhá další šetření, neboť není zřejmé, zda je uživateli umožněno zaslat redukovanou kopii (s použitím šablony pro zakrytí údajů, které nejsou potřebné) průkazu totožnosti, tedy takovou kopii, kde jsou viditelné pouze nezbytně nutné údaje pro ověření věku uživatele.

## Kopírování občanských průkazů

Mezi další častá témata stížností se řadila ta, kdy při zapůjčování věci (invalidní vozík, loďka...), docházelo ke zpracování všech osobních údajů z občanského průkazu (bez použití šablony pro zakrytí některých údajů, které pro identifikaci fyzické osoby nejsou potřebné), aniž správce disponoval právním důvodem, přičemž správce neplnil či nedostatečně plnil informační povinnosti dle čl. 13 GDPR.

## Obchodní sdělení a neplnění informační povinnosti

Neplnění či nedůsledné plnění informační povinnosti podle čl. 14 obecného nařízení v případě zasílání obchodních sdělení (nabídek na odkup nemovitého majetku). Správce čerpal osobní údaje z katastru nemovitostí (dohled nad využíváním dat z katastru nemovitostí náleží katastrálnímu úřadu).

## Zpřístupňování osobních údajů SVJ a bytovými družstvy neoprávněným příjemcům

Ve chvíli, kdy vedení SVJ / bytového družstva informuje o dění v domě své členy, vyvěsí dokument (obsahující osobní údaje) ve společných prostorách bytového domu – zpravidla na nástěnku umístěnou u poštovních schránek, výtahu nebo na dveře konkrétního bytu. Tím osobní údaje zpřístupní nejen členům SVJ / bytového družstva, ale neoprávněně také úklidové službě, popelářům, poštovním doručovatelům a dalším návštěvníkům bytového domu.



## Ztěžování výkonu práv subjektu údajů podle obecného nařízení

Někteří správci omezují komunikační kanály pro přijímání žádostí zpracováním dotčených osob. Podle čl. 38 odst. 4 obecného nařízení se subjekty údajů mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle tohoto nařízení. Správce však není oprávněn omezit komunikační kanály pro přijímání žádostí subjektu údajů v souvislosti s výkonem práv podle tohoto nařízení. Kontaktovat správce v záležitostech ochrany osobních údajů prostřednictvím pověřence je pro subjekt údajů žádoucí jako možnost, není to však jeho povinnost. Z pohledu subjektu údajů je výkon jeho práv prokazatelný zasláním žádosti prostřednictvím datové zprávy nebo dopisem do sídla společnosti (s doručenkou), na rozdíl od doručení žádosti na e-mailovou adresu pověřence.

## ● OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

V roce 2022 Úřad obdržel 313 ohlášení porušení zabezpečení osobních údajů (*data breach*), tedy téměř shodně jako v předchozích letech. Jako nejčastější příčinu porušení ohlašovatelé uváděli kybernetický útok, nejčastěji ransomware, event. jiný typ externího útoku.

Z obdržených ohlášení správců v oblasti poskytovatelů zdravotních služeb (typicky nemocnice) vyplývá, že nejčastější příčinou porušení zabezpečení byla lidská chyba, nikoli systémové pochybení správce při zpracování osobních údajů. V těchto případech se jednalo např. o přeposlání zdravotní dokumentace jiné nemocnici, než do které měla být odeslána, ponechání žádanek na vyšetření pacientů na stole u otevřených oken za bouřky, kdy se v důsledku průvanu písemnosti dostaly do přílehlého okolí budovy v areálu nemocnice.

Předmětem ohlášení byly i případy, kdy došlo k neoprávněnému nahlížení do zdravotní dokumentace ze strany lékařů, kteří z titulu svého pracovního zařazení neměli důvod do této dokumentace nahlížet a následně předali tak-

to získané informace třetí straně. V souvislosti s ohlášením porušení zabezpečení byl zaznamenán případ, kdy při zavádění nového informačního systému v rámci nemocnice byla volně přístupná příslušná dokumentace, která mimo jiné obsahovala i přístupová hesla do systému.

Na základě podnětu, v němž byl dokumentován nález většího množství zdravotnické dokumentace pacientů, ale i zaměstnanců nemocnice v centru města, se Úřad aktuálně zabývá možným porušením povinností správce, neboť i přestože se podle podnětu na místo nálezu dostavil pověřenec pro ochranu osobních údajů nemocnice, předmětný incident ze strany této nemocnice nebyl Úřadu ohlášen.

Pozitivně lze hodnotit, že v případě ohlášení porušení zabezpečení postupují ohlašovatelé v oblasti poskytovatelů zdravotních služeb zpravidla v souladu s povinnostmi správce podle čl. 33 obecného nařízení. Nemocnice v ohlášení k organizační stránce odkazují na interní akty řízení, kde je popsáno, jak se postupuje při nakládání s osobními údaji, včetně školení a poučení zaměstnanců. K technické stránce např. uvádí, jakými technickými prostředky jsou osobní údaje zabezpečeny, firewall, VPN, jestli jsou přístupy logovány, jaké je rozdělení přístupových oprávnění do informačního systému podle pracovního zařazení, po jakou dobu jsou logy uchovány, zda jsou prováděny penetrační testy, jak často dochází ke kontrole a prověrce zabezpečení informačního systému, zda dochází pravidelně k vyhodnocování rizik a následnému přijímání opatření, jak jsou silná přístupová hesla, jak často jsou měněna, zda dochází k monitorování informační sítě, jak a kde jsou data ukládána, zda jsou rozděleně zálohována, zda využívají hostingových služeb, cloud atd.

Podstatně horší je situace u škol, a to jak u základních, středních a vysokých, tak i u speciálních, stejně jako u spolků, bytových družstev, orgánů veřejné správy a obecních, městských i krajských úřadů.

Tito správci údajů často ani nevyužijí k ohlášení [formulář](#) k tomu určený na webové stránce Úřadu a plní ohlašovací povinnost pouze formálně. V ohlášení často chybí informace o osobě, která činí ohlášení jménem správce, nebývá

vždy uvedeno, zda se jedná o pověřence pro ochranu osobních údajů nebo kontaktní osobu, nadto nejsou ani uvedeny kontaktní údaje na tuto osobu.

Pokud jde o popis příčiny porušení, zde často správce údajů není schopen popsat příčiny porušení, např. uvede pouze: „ransomwarový útok“, „došlo k zneprístupnění dat“, „nelze pracovat s informačním systémem školy“, mnohdy je zaměřováno „porušení dostupnosti dat“ za „ztrátu dat“ popř. „zničení dat“. Opakovaně není v ohlášeních uveden popis zjištěných účinků ani přibližný počet dotčených subjektů údajů ani přibližný počet dotčených záznamů osobních údajů. Vhodný [postup je uveden na webových stránkách Úřadu](#).

Obdobně jako v předchozích letech ohlašovatelé chybují při informování dotčených subjektů o vzniklém porušení ochrany údajů. Dost často správce uvede, že nebudou informováni, aniž by tento postup náležitě zdůvodnil, popř. zavrhně možnost „představovalo by to nepřiměřené úsilí informovat každou fyzickou osobu individuálně“, avšak nesplní povinnost účinného veřejného oznámení. Ze strany Úřadu je následně vyžadováno zdůvodnění, popř. aby správce učinil účinné veřejné oznámení.

Orgány činné v trestním řízení chybně ohlašují porušení zabezpečení osobních údajů podle § 41 zákona o zpracování osobních údajů i v případech, kdy jsou v postavení správního orgánu tedy správně by měly postupovat podle článku 33 GDPR.

## ● ZÁVĚRY Z KONZULTAČNÍ ČINNOSTI

Úřad poskytuje podporu při řešení otázek spojených se zpracováním osobních údajů s cílem usnadnit plnění povinností vyplývajících pro správce/zpracovatele z obecného nařízení, a předcházet tak porušování pravidel při zpracování osobních údajů. Dalším cílem poskytování konzultací je zvyšovat povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním osobních údajů a podporovat povědomí správců a zpracovatelů o jejich povinnostech podle obecného nařízení. Níže jsou uvedeny stěžejní výstupy z konzultační činnosti za rok 2022.

## Zasílání obchodních sdělení ve zdravotnictví

Úřad řešil relevanci zasílání obchodních sdělení ve spojitosti s poskytováním zdravotních služeb, a to ve smyslu zákona č. 372/2011 Sb., o zdravotních službách. Vhodným příkladem je situace, kdy pacientovi, který byl přijat k hospitalizaci poskytovatelem zdravotních služeb v bezvědomí, jsou po ukončení jeho hospitalizace zasílána reklamní sdělení s nabídkou poskytování další zdravotní péče. Pokud je naplněna podmínka předvídatelnosti pro subjekt údajů a je řádně ve věci informován, pak poskytnutí informace (nikoliv však reklamního sdělení) o poskytování zdravotních služeb vyloučeno není. Jedná se například o připomenutí termínu poskytování zdravotních služeb, o informace o možnosti objednání na preventivní prohlídku nebo o informace o uvolnění termínu pro poskytování zdravotní služby (zubní zákroky, rehabilitace atd.).

Předpokládané zpracování osobních údajů správcem sloučením účelů plnění povinnosti uložené právním předpisem, tedy vedením zdravotnické dokumentace, a zasíláním obchodních sdělení, je možné považovat za protiprávní, a to zejména při zpracování zvláštní kategorie osobních údajů podle čl. 9 GDPR (zpracovávání zvláštních kategorií osobních údajů).

## Doložení nepřítomnosti žáka lékařským potvrzením

Ve své praxi se Úřad setkal se skutečností, kdy základní škola požadovala po zákonném zástupci žáka doložení každé nepřítomnosti žáka z důvodu nemoci lékařským potvrzením. Ze stanoviska Ministerstva zdravotnictví plyne: „Základní a střední škola může požadovat, pokud to považuje za nezbytné, doložení nepřítomnosti žáka z důvodu nemoci ošetřujícím lékařem žáka, resp. praktickým lékařem pro děti a dorost, a to pouze jako součást omluvenky vystavené zákonným zástupcem nezletilého žáka nebo omluvenky vystavené zletilým žákem, a to pouze v případě, že nepřítomnost žáka ve škole přesáhne tři dny školního vyučování.“ Z uvedeného je zřejmé, že prokazovat školskému zařízení každou jednotlivou návštěvu potvrzením poskytovatele zdravotních služeb žáka či studenta,



není nezbytně nutné. Mimo situace, kdy nejde o jiné závažné skutečnosti, např.: dlouhodobou nemoc, vysoce frekventované absence nebo jinou specifickou mimořádnou skutečnost, kdy se může jednat například o odklad složení státních zkoušek z důvodu nemoci. Na tyto skutečnosti by mělo být pamatováno ve školním řádu školského zařízení a je potřebné, aby o něm byli poučeni studenti i jejich zákonní zástupci.

### **Český jazyk a výkon funkce pověřence pro ochranu osobních údajů**

S rostoucím významem odpovědnosti za ochranu osobních údajů u jednotlivých správců a zpracovatelů osobních údajů se Úřad zabýval tím, zda je pro výkon funkce pověřence pro ochranu osobních údajů nezbytná znalost českého jazyka. V souladu s přílohou Pokynů pro pověřence pro ochranu osobních údajů (WP 243 rev.01)<sup>3</sup> platí, že „Pověřenec, v případě nutnosti s pomocí týmu, musí být schopen účinně komunikovat se subjekty údajů a spolupracovat s dotčenými dozorovými úřady. To znamená, že tato komunikace musí probíhat v jazyce nebo jazycích používaných dozorovými úřady a dotčenými subjekty údajů.“

Pro výkon funkce pověřence je tedy z pohledu obecného nařízení stěžejní, zda daná osoba dosahuje profesních kvalit obecně vymezených v rámci čl. 37 odst. 5 obecného nařízení, a je tak schopna plnit úkoly stanovené čl. 39 GDPR.

### **Souhlas se zpracováním zvláštní kategorie osobních údajů v online platformě**

Podle odst. 32 preambule GDPR je stanoveno, že souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů se zpracováním osobních údajů, které se jej týkají, a to v podobě písemného prohlášení učiněného elektronicky, nebo formou ústního prohlášení. Modelově by se mohlo jednat například o zaškrtnutí políčka při návštěvě internetové stránky, které v této souvislosti jasně signalizuje souhlas subjektu údajů

s navrhovaným zpracováním jeho osobních údajů volbou technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání. Mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za takové vyjádření souhlasu subjektu údajů.

Na základě ustanovení bodu 94 pokynů EDPB 05/2020 k souhlasu podle obecného nařízení je mj. uvedeno, že například v digitálním nebo online kontextu může být subjekt údajů schopen vydat potřebné prohlášení (udělení výslovného souhlasu) vyplněním elektronického formuláře, zasláním e-mailu, nahráváním naskenovaného dokumentu opatřeného podpisem subjektu údajů nebo pomocí elektronického podpisu.

Následně je v rámci bodu 97 příkladu 17 citovaného dokumentu uvedeno, že správce údajů může získat výslovný souhlas od návštěvníka svých internetových stránek rovněž nabídnutím obrazovky výslovného souhlasu, jenž obsahuje zaškrťovací políčka Ano a Ne, za předpokladu, že text dává jasně najevo souhlas, tedy například „Tímto souhlasím se zpracováním svých údajů“, nikoli „Chápu, že mé údaje budou zpracovávány“. Je jasné, že by měly být splněny podmínky pro informovaný souhlas, jakož i ostatní podmínky pro získání platného souhlasu podle obecného nařízení. To ovšem nedefinuje přesné postupy a mechanismy udělení výslovného souhlasu a jeho aplikace. Citované nařízení stanovuje pouze základní principy, při jejichž dodržení je možné výslovný souhlas aplikovat [čl. 4 bod 11, čl. 7, čl. 9 odst. 2 písm. a) GDPR].

### **Doručení volebních lístků s uvedením data narození voliče na obálce**

Podle článku 4 odst. 2 Poštovních podmínek vydaných k zákonu č. 29/2000 Sb., o poštovních službách, poštovní adresa v následujícím pořadí obsahuje označení adresáta – u fyzické osoby její jméno a příjmení, k nimž může být připojen další identifikátor, např. datum narození, je-li použito v souladu s právními předpisy. Tímto předpisem je obecné nařízení o ochraně osobních údajů, které v článku 5 odst. 1 písm. c) stanoví zásadu minimalizace údajů.

Využití data narození adresáta jako dalšího identifikátoru k eliminaci možné záměny s jinou osobou je namísto v případě úřední zásilky se

<sup>3</sup> WP byla zkratkou Pracovní skupiny pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů (pracovní skupina zřízená podle článku 29 Směrnice 95/46/EC) do 25. května 2018.

specifickým obsahem určeným výlučně adresátovi. Tak tomu v případě dodání sady volebních lístků, které jsou minimálně v příslušném volebním okrsku shodné, není.

V obchodních podmínkách, sjednaných mezi Ministerstvem vnitra a Českou poštou s. p. je uvedeno:

*„Objednatel pověřuje podnik zpracováním osobních údajů obsažených v seznamu voličů dle bodu 8, v rozsahu jméno, příjmení, adresa, datum narození, případně údaj o překážce ve výkonu volebního práva, za účelem dodání hlasovacích lístků bez adresy příjemce uvedené na zásilce, a to po dobu dle bodu 31.“*

Praxe obecních úřadů při doručování volebních lístků je různá. Volební lístky jsou některými obcemi doručovány se jménem a příjmením voliče na obálce. Ani zcela anonymní doručení bez uvedení jakýchkoli údajů na obálce nelze posuzovat jako porušení § 25 odst. 5 zákona č. 491/2001 Sb., o volbách do zastupitelstev obcí, jestliže počet sad hlasovacích lístků vložených v obálkách do poštovní schránky odpovídá počtu oprávněných voličů v příslušném bytě. Pokud by rodinný příslušník jinému rodinnému příslušníkovi hlasovací lístky omylem nebo i úmyslně nepředal, k čemuž může dojít i při označení datem narození, neznamená to, že ve smyslu citovaného ustanovení nedošlo k dodání hlasovacích lístků do příslušné poštovní schránky, ani to, že by voliči byla realizace volebního práva znemožněna, neboť má v každém případě možnost vyzvednout si volební lístky i přímo ve volební místnosti u volební komise.

Plošné uvádění dat narození voličů na obálkách jako výstupu ze seznamu voličů se proto jeví jako nedůvodné a mohlo by být posouzeno jako porušení zásady minimalizace údajů [čl. 5 odst. 1 písm. c) GDPR]. V úvahu je třeba brát i to, že obálky, v nichž byly hlasovací lístky dodány, zpravidla voliči po ukončení volby odhazují do k tomu určených košů, kde mohlo, při nedostatečném zabezpečení, dojít i k neoprávněnému přístupu k údajům na obálce v kombinaci s informací o tom, jak volič hlasoval ve volbách, v nichž použije pouze jeden lístek, který pak v sadě lístků chybí.

## ● ZÁVĚRY Z ANALYTICKÉ ČINNOSTI

Ochrana osobních údajů je oblastí práva, která není statická, ale vyvíjí se dynamicky v závislosti na vývoji technologií, které zpracovávají osobní údaje. Principy ochrany osobních údajů stanovené obecným nařízením Evropské unie o ochraně osobních údajů je třeba aplikovat na všechny oblasti a činnosti, kde dochází ke zpracování osobních údajů, a to již při jejich navrhování (princip *Privacy by Design*). Subjekt, který osobní údaje zpracovává, se stává správcem osobních údajů, který nese odpovědnost za jejich ochranu v souladu s právním rámcem ochrany dat. To, zda správce náležitě zajistil soulad s pravidly ochrany údajů, může být ověřeno prostřednictvím přezkumu nezávislým dozorovým úřadem nebo soudem. Rovněž pokud je přijímána nová právní úprava, která při své realizaci předpokládá využití nových technologií zpracovávajících osobní údaje, je třeba tento aspekt zohlednit jak při tvorbě legislativy, tak při její aplikaci.

### Problematika právní úpravy DNA z pohledu ochrany osobních údajů

Pokud jde o soulad právní úpravy uchovávání vzorků DNA v databázi Policie ČR s právním rámcem ochrany osobních údajů, z pohledu Úřadu jde o významné téma ochrany osobních údajů v ČR, v němž dosud nebylo dosaženo nastavení souladu (proporcionality) mezi oprávněnými požadavky na bezpečnost společnosti a právem na ochranu osobních údajů tak, jak je vyjádřeno v evropském, případně mezinárodním právu. Úřad se k této otázce již dříve vyjádřil tak, že samotné vedení databáze DNA zasahuje do práva na ochranu osobních údajů, což vyžaduje nastavení řady opatření předpokládaných právní úpravou ochrany osobních údajů.<sup>4</sup> Přitom zákon o Policii ČR neobsahuje výslovné zmocnění k vedení databáze DNA, byť rámcově problematiku řeší, nicméně schází v něm úprava přesnějších podmínek pro vedení databáze (například přesné vymezení lhůt pro uchovávání záznamů či podrobnější podmínky likvidace osobních údajů). Celkově lze shrnout,

4 Viz vyjádření Úřadu v ústavní stížnosti Pl. ÚS 7/18.





že úprava osobních údajů v zákoně o Policii ČR je neúplná, přičemž některé přesnější podmínky jsou stanoveny pouze v neveřejném interním nařízení policie. Proto Úřad nepovažuje současnou právní úpravu v zákoně o Policii ČR za dostatečný právní základ pro uchovávání vzorků DNA.<sup>5</sup>

Pokud jde o samotný nálezný Pl. ÚS 7/18, Úřad jej pečlivě analyzoval z hlediska ochrany osobních údajů. Lze shrnout, že i když Ústavní soud nevyhověl návrhovateli (Městský soud Praha) požadující zrušení § 65 odst. 1 a odst. 5 zákona o Policii ČR, přesto citovaný nálezný představuje důležitý krok směrem k nastavení potřebného souladu mezi chráněnými výše uvedenými hodnotami. K odmítnutí návrhu totiž Ústavní soud vedl, jak to v odůvodnění vysvětlil, procesní důvody, případně nevhodnost ustanovení navržených ke zrušení pro zásah do právní úpravy zákona o Policii ČR. V případě návrhu na zrušení § 65 odst. 5 Ústavní soud návrh zamítnul pro nedostatek aktivní legitimace (k posouzení ústavnosti podmínek pro likvidaci osobních údajů získaných odběrem může totiž dojít až následně po odběru a zpracování vzorku DNA, tedy nikoliv zároveň s odběrem samotným, který upravuje odstavec 1),<sup>6</sup> zatímco v případě § 65 odst. 1 Ústavní soud návrh odmítnul, když vysvětlil, že se nejednalo o nejpříhodnější případ (tedy tzv. podvozek) k zákroku Ústavního soudu, protože v samotném fyzickém odebrání biologických vzorků nelze spatřovat porušení základního práva na nedotknutelnost osoby podle čl. 7 odst. 1 ani zásah do soukromí podle čl. 10 odst. 2 a odst. 3 Listiny základních práv a svobod, stejně jako není protiústavní neúplnost, resp. nedostatečnost či přílišná obecnost právní úpravy.<sup>7</sup>

Lze dodat, že Ústavní soud považoval v odůvodnění za relevantní důvod pro nezrušení napadených ustanovení i plnění závazků plynoucích z mezinárodního a evropského práva v oblasti prevence a vyšetřování trestné činnosti, které předpokládá využití databází národních souborů DNA. V tomto ohledu Ústavní soud

upozornil na rozhodnutí Rady EU 2008/615/SVV ze dne 23. 6. 2008, o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti, které začlenilo do práva Evropské unie tzv. Průmskou smlouvu, která spolu s prováděcím rozhodnutím Rady EU 2008/616/SVV vychází z principu síťového propojení národních souborů analýzy DNA, přímého přeshraničního přístupu do nich a společných záruk zabezpečení práva na ochranu soukromí a osobních údajů. Ústavní soud konkrétně uvedl, že výpadek výslovného oprávnění policie k odběru biologických vzorků, např. v důsledku omezení nebo zrušení zákonného kompetenčního zmocnění, by vedl k oslabení garancí plnění závazku členského státu EU.<sup>8</sup> V případě existence těchto mezinárodních závazků lze považovat za přirozené, že do stávajícího systému právní úpravy v ČR v oblasti policejní spolupráce by mělo být zasahováno uvážene, a měl by tak učinit zákonodárce.

V uvedeném kontextu je na druhé straně třeba upozornit na to, že citované rozhodnutí Rady EU 2008/615/SVV předpokládá, že s ohledem na obsáhlou výměnu informací a údajů vyplývajících z užší policejní a justiční spolupráce musí být zaručena odpovídající úroveň ochrany osobních údajů, kterou se rozumí úroveň ochrany navržená pro zpracování osobních údajů v Úmluvě Rady Evropy č. 108 o ochraně osob s ohledem na automatizované zpracování osobních údajů ze dne 28. ledna 1981 (dále Úmluva), Dodatkovém protokolu k Úmluvě ze dne 8. listopadu 2001 a zásadách Doporučení Výboru ministrů Rady Evropy č. R (87) 15 ze dne 17. září 1987 o používání osobních údajů v policejní oblasti. Nadto článek 25 citovaného rozhodnutí 2008/615/SVV stanoví, že požadovanou úroveň ochrany údajů, které jsou podle něj předávány nebo byly předány, musí zajistit každý členský stát ve svém vnitrostátním právu.<sup>9</sup> Promitnutí výše uvedených předpisů do vnitrostátní právní úpravy představuje minimální standard ochrany osobních údajů v dané oblasti.

8 Viz nálezný Pl. ÚS 7/18 body bod 66.

9 Rozhodnutí Rady 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti. Body 19 a 20 preambule a článek 25 textu.

5 Viz nálezný Pl. ÚS 7/18 body 31–35.

6 Viz nálezný Pl. ÚS 7/18 body 43–46.

7 Viz nálezný Pl. ÚS 7/18 body 71–78.

Je třeba proto uvést, že nález Pl. ÚS 7/18 nijak nezasáhl do prostoru, který je určen pro budoucí stanovení kritérií potřebných pro soulad právní úpravy v oblasti shromažďování a uchování vzorků DNA s ochranou osobních údajů, když pouze konstatoval nedostatečnou přesnost současné právní úpravy a potřebu zpřesnění široce nastavených kritérií. V tomto ohledu Ústavní soud připomněl, že je vázán petitum návrhu, nikoliv odůvodněním, což mu bránilo posoudit návrhy, které navrhovatel v odůvodnění uvedl.<sup>10</sup> Z odůvodnění nálezu Ústavního soudu Pl. ÚS 7/18 tedy podle Úřadu vyplývá, že přesnější nastavení právní úpravy v souladu s právním rámcem ochrany osobních údajů je dosud budoucím úkolem zákonodárce.

## ● NÁRODNÍ LEGISLATIVA

Agresí Ruské federace vůči Ukrajině ve čtvrtek 24. února 2022 fakticky skončilo legislativní období věnované převážně problematice COVID-19. Byla sice ještě schválena problematická novela pandemického zákona č. 39/2022 Sb., ale 5. května 2022 vypršel stav pandemické pohotovosti a většina pandemického zákona pozbyla platnosti 30. listopadu 2022. S ohledem na to očekával Úřad větší legislativní aktivity Ministerstva zdravotnictví, zejména v nedostatečné právní úpravě tzv. hygienických registrů, které však dosud nebyly naplněny.

K vládnímu návrhu zákona, kterým se mění zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), a další související zákony, neměl Úřad připomínky, neboť se týkal ryze veterinární problematiky.<sup>11</sup> Byl však k němu načten pozměňovací návrh SD 904, který se týkal očkování fyzických osob. Bylo v něm navrženo odstranění duplicit zápisu při zachování vedení záznamů o očkování na cen-

<sup>10</sup> Viz nález Pl. ÚS 7/18 bod 92.

<sup>11</sup> Jednalo se o adaptaci českého právního řádu na nařízení Evropského parlamentu a Rady (EU) 2019/6 o veterinárních léčivých přípravcích a o zrušení směrnice 2001/82/ES a nařízení Evropského parlamentu a Rady (EU) 2019/4 o výrobě, uvádění na trh a používání medikovaných krmiv, o změně nařízení Evropského parlamentu a Rady č. 183/2005 a o zrušení směrnice 90/167/EHS. Šlo o sněmovní tisk č. 73.

trální úrovni v obou systémech (v systému eRecept podle zákona o léčivech a v hygienických registrech podle zákona o ochraně veřejného zdraví), ovšem za současného podstatného rozšíření oprávnění Ústavu zdravotnických informací a statistiky (ÚZIS) přistupovat k údajům týkajícím se očkování. Podle pozměňovacího návrhu měl mít ÚZIS automatizovaný přístup k individualizovaným údajům o očkování každé jednotlivé fyzické osoby, a to aniž byla navržena omezení pro ÚZIS při nakládání s osobními údaji. Už podle stávající úpravy § 81 odst. 3 písm. k) zákona o léčivech přitom má ÚZIS přístup k anonymizované databázi údajů o očkování vedených systémem eRecept. Ve vztahu ke stávající úpravě přitom Úřad opakovaně upozorňoval na to, že z hlediska ochrany osobních údajů pro modul OČKO v Informačním systému infekčních nemocí (ISIN) absentuje zákonný podklad, protože § 79 odst. 2 zákona o ochraně veřejného zdraví je příliš vágní a nenaplnuje podstatné náležitosti regulace registru (tj. primárně stanovení účelu a doby uchování údajů). Bez vymezení jasného právního základu ISIN nelze z pohledu ochrany osobních údajů souhlasit s jeho rozšiřováním. Před takto rozsáhlým novým zpracováním osobních údajů musí být také posouzen vliv na ochranu osobních údajů podle čl. 35 GDPR. Přijaté znění předmětné novelizace zákona o léčivech (zákon č. 314/2022 Sb.) nakonec zmíněné podstatné rozšíření přístupu ÚZIS k údajům o očkování na individualizované úrovni neobsahuje, mj. i v důsledku výše odůvodněného kritického postoje Úřadu. Nutno ovšem konstatovat, že původní výhrady Úřadu, zejména týkající se obecné neexistence právní úpravy pro „hygienické registry“, nadále přetrvávají.

Zvláštní pozornost vyvolal návrh zákona, kterým se mění některé zákony v oblasti obrany. Úřad se ve svých připomínkách soustředil na otázky eGovernmentu, tj. v kontextu tohoto návrhu zákona se zabýval zpracováním osobních údajů ve veřejnoprávních registrech a informování o něm.

V roce 2022 rostoucí inflace vedla k potřebě řady novel právních předpisů, zejména z dílny Ministerstva práce a sociálních věcí (cca 30). Úřad je sledoval, aby do těchto časových



opatření nebyly vmísены právní normy oslabující soukromí.

Úřad vlády představil rozsáhlý návrh novely legislativních pravidel vlády. Úřad pro ochranu osobních údajů k tomu uplatnil řadu koncepčních námětů, přičemž Úřad vlády vyhověl jeho návrhu na specifikaci zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů, které nově obsahuje obdobné náležitosti jako posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR.

Zásadní dopady do plnění úkolů Úřadu přinesla novela zákona č. 106/1999 Sb. provedená zákonem č. 241/2022 Sb., přičemž její vyhodnocení bude možné po zkušenostech z aplikační praxe.

Ministerstvo financí a Ministerstvo práce a sociálních věcí řádně plnily povinnosti z článku 36 odst. 4 GDPR a projednávaly s Úřadem návrhy právních předpisů v jeho působnosti. Koncepční výzvy lze spatřovat ve spolupráci s Ministerstvem spravedlnosti v oblasti prokazování trestní zachovalosti, v níž chybí obecná právní úprava, která by vykazování bezúhonnosti dala řád. Účelem odsouzení za trestný čin je uložení trestu. Ačkoliv trestní zákoník reguluje zákaz činnosti, desítky právních předpisů stanoví vedle toho paušální zákaz činnosti ze zákona, přestože nebylo přezkoumáno v rámci hodnocení dopadů regulace (angl. *Regulatory Impact Assessment*, RIA), zda je to potřeba a v jakém rozsahu. Kromě soudem uloženého zákazu činnosti se tedy pachatel až do zahlazení odsouzení nesmí zabývat množstvím dalších činností, což může být kriminogenní faktor, respektive faktor ztěžující resocializaci pachatele. Aniž Úřad pomíjí potřebu individuální prevence, respektive ochrany společnosti, připomíná, že neexistuje ani možnost přezkumu tvrdosti zákona soudem. Žádný rámcový zákon tedy nestanoví, jaké druhy trestných činů jsou překážkou jaké činnosti. Kriticky je rovněž nutno nahlížet na nevyvratitelnou právní domněnku aktuálnosti výpisu ne staršího než 3 měsíce čili jinými slovy: nedávný výpis je automaticky považován za správný bez ohledu na realitu, a naopak starší výpis je automaticky považován za nesprávný v rozporu s praxí, kde i roky staré výpisy jsou obvykle aktuální.

## UNIJNÍ LEGISLATIVA

Zvláštní význam mělo, že 1. ledna 2022 začalo II. trio předsednictví Rady EU (Francie – Česká republika – Švédsko) a 1. července 2022 předsednictví České republiky, které prosadilo schválení řady návrhů Evropské komise.

Největší význam má nařízení o digitálních službách (angl. *Digital Services Act*, DSA)<sup>12</sup>, které představuje novou regulaci elektronického obchodu a ve kterém Rada EU oproti původnímu komisnímu návrhu prosadila řadu změn. Většina DSA nabývá účinnosti 17. února 2024; zbytek již nabyl účinnosti 16. listopadu 2022.

Doprovodné je nařízení o digitálních trzích (angl. *Digital Markets Act*, DMA).<sup>13</sup> Jeho smyslem je nastavení pravidel pro přístup k digitální infrastruktuře prostřednictvím nových povinností pro tzv. gatekeepers, tj. vyhledávače, sociální média nebo poskytovatele cloudových služeb s cílem zabránit zneužití jejich dominantního postavení. Většina ustanovení DMA nabývá účinnosti 2. května 2023.

Mimo stojí nařízení o správě dat (angl. *Data Governance Act*, DGA).<sup>14</sup> Jeho cílem je usnadnit sdílení dat veřejného sektoru, a tím podpořit inovace. DGA nabývá účinnosti 24. září 2023. Doplněním DGA je návrh aktu o datech (angl. *Data Act*, DA),<sup>15</sup> který má za cíl definovat právní rámec pro přístup k datům a jejich využívání, zejména internetu věcí (IoT).

Stále ve stadiu návrhu zůstává nařízení o umělé inteligenci (angl. *Artificial Intelligence*

12 Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách).

13 Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích).

14 Nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat).

15 Návrh nařízení Evropského parlamentu a Rady ze dne 23. února 2022 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (Akt o datech), CELEX 52022PC0068.

Act, AIA),<sup>16</sup> u něhož české předsednictví Rady EU prosadilo obecný přístup. Návrh počítá s úplným zákazem používání nepřijatelných technologií, jako jsou například manipulace s chováním nebo sociální hodnocení. Vysoce riskantní systémy budou povoleny pouze tehdy, pokud projdou posouzením. Stávající text však nepřevzal návrhy ochránců dat o zákazu biometrické identifikace ve veřejných prostorech. Ve stejný den byl schválen obecný přístup k doplnění nařízení eIDAS<sup>17</sup> o „evropskou digitální peněženku“, tj. o soukromoprávní prokazování totožnosti.

Úřad podporuje aktivity, které jsou cíleny na boj proti pohlavnímu zneužívání dětí prostřednictvím prostředků elektronické komunikace. Nicméně ochránci dat vyjadřují vážné obavy u návrhu nařízení, CSA,<sup>18</sup> a to především s ohledem na hrozící bezprecedentní dopad zamýšlených opatření na soukromí. Konkrétně jde o povinné monitorování v zásadě veškeré komunikace na internetu.

## ● PŘEHLED OBLASTÍ UPRAVENÝCH POKYNY EDPB

Evropský sbor pro ochranu osobních údajů (EDPB) vydal ve sledovaném roce řadu dokumentů užitečných nejen pro odbornou veřejnost (správci, zpracovatelé, pověřenci pro ochranu osobních údajů), ale i veřejnost laickou (subjekty údajů). Jde o následující materiály (první tři byly již zveřejněny v oficiálním českém překladu, k ostatním probíhá veřejná konzultace nebo její vypořádání a jsou k dispozici pouze v angličtině):

<sup>16</sup> Návrh nařízení Evropského parlamentu a Rady ze dne 21. dubna 2021, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) a mění určité legislativní akty Unie, CELEX 52021PC0206.

<sup>17</sup> Návrh nařízení Evropského parlamentu a Rady ze dne 3. června 2021, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, CELEX 52021PC0281.

<sup>18</sup> Návrh nařízení Evropského parlamentu a Rady ze dne 11. května 2022, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu, CELEX 52022PC0209.

- [Pokyny 04/2021 týkající se kodexů chování jakožto nástrojů pro předávání,](#)
- [Doporučení 1/2022 k žádosti o schválení a k prvkům a zásadám, které musí být součástí závazných podnikových pravidel pro správce \(Článek 47 GDPR\),](#)
- [Pokyny 01/2022 k právům subjektu údajů – právo na přístup,](#)
- [Pokyny 02/2022 k uplatňování článku 60 GDPR,](#)
- [Pokyny 03/2022 k temným vzorcům v rozhraních platform sociálních médií: Jak je rozpoznat a vyhnout se jim,](#)
- [Pokyny 04/2022 k výpočtu správních pokut podle GDPR,](#)
- [Pokyny 05/2022 k použití technologie rozpoznávání obličejů v oblasti vynucování práva,](#)
- [Pokyny 06/2022 k praktickému uplatňování smírných řešení,](#)
- [Pokyny 07/2022 k certifikaci jakožto nástrojů pro předávání,](#)
- [Pokyny 8/2022 k identifikaci vedoucího dozorového úřadu pro správce nebo zpracovatele,](#)
- [Pokyny 9/2022 k ohlašování porušení zabezpečení osobních údajů podle GDPR.](#)

Z výše uvedených je věnována bližší zmínka následujícím dokumentům.

### **Pokyny 01/2022 k právům subjektu údajů – právo na přístup**

Právo na přístup je zakotveno v čl. 8 Listiny základních práv EU. Obecné nařízení o ochraně osobních údajů toto právo dále vysvětluje a upřesňuje. Tyto pokyny jsou určeny jako pomůcka správcům, kterým poskytují návod, jak žádosti o přístup k údajům posuzovat a vyřizovat, a v jakých lhůtách a jakou formou informovat žadatele o přístupu k osobním údajům. Upozorňují například, že pseudonymizovaná data zůstávají na rozdíl od dat anonymizovaných stále osobními údaji. Poznávají, že žádosti se mohou týkat nejenom osobních údajů v digitálních systémech, ale také v klasických analogových registrech. Pokyny rovněž popisují výjimky z práva na přístup. Dokument, u kterého je zástupkyně Úřadu členkou řešitelského týmu, prošel veřejnou konzultací a jeho konečná verze se dokončuje.



## Pokyny 04/2021 týkající se kodexů chování jakožto nástrojů pro předávání

Po vydání Pokynů 1/2019, které vymezují požadavky kladené na kodexy chování prokazující shodu s obecným nařízením, se Sbor soustředil i na druhou kategorii kodexů chování, totiž těch kodexů, jejichž účelem je vytvoření vhodných záruk pro ochranu osobních údajů ve třetí zemi, jak to předpokládá čl. 40 odst. 3 GDPR. Sbor v těchto pokynech co nejkonkrétněji vymezuje prvky, které takový kodex chování musí obsahovat, aby tyto vhodné záruky dokázal poskytnout, a mohl tak být použit jako nástroj pro předávání osobních údajů do třetí země. Především je konkretizováno, co musí být obsahem oněch „závazných a vymahatelných závazků“, které jako nezbytnou podmínku pro vytvoření vhodných záruk pro předávání osobních údajů do třetí země prostřednictvím kodexu chování vyžaduje čl. 46 odst. 2 písm. e) GDPR. Dále je předestřeno, jakým způsobem účastník takového kodexu čili zpravodla dovozce údajů ve třetí zemi může zajistit závazný charakter těchto závazných a vymahatelných garancí, přičemž nejschůdnější cestou se jeví smluvní závazek, který uzavírá dovozce údajů s jejich vývozcem. Viz také kapitulu této výroční zprávy k předávání údajů do třetích zemí.

## Pokyny 02/2022 k uplatňování článku 60 GDPR

Tyto pokyny vydal EDPB s cílem prohloubit a zefektivnit spolupráci jednotlivých dozorových úřadů a posílit jednotné uplatňování právních ustanovení týkajících se mechanismu jediného kontaktního místa podle obecného nařízení. Pokyny se týkají spolupráce mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady a jsou rozděleny do oddílů, které se zabývají postupy podle jednotlivých odstavců článku 60 GDPR. Jedná se např. o:

- popis situace, kdy vedoucí dozorový úřad požádá dotčené dozorové úřady o poskytnutí vzájemné pomoci podle článku 61 GDPR a provádí společné postupy podle článku 62 obecného nařízení,
- předložení návrhu rozhodnutí a popis různých scénářů, které následují po předložení tohoto návrhu a napomáhají k jed-

notnému postupu, pokud jsou vzneseny relevantní a odůvodněné námitky, nebo v případě, že vedoucí dozorový úřad považuje námitky za irelevantní a nedůvodné nebo relevantní a odůvodněnou námitku nesdílí a požádá o rozhodnutí EDPB,

- popis povinností správce nebo zpracovatele k zajištění toho, aby zpracování bylo ve všech jeho provozovnách v souladu s konečným rozhodnutím,
- podmínky pro uplatnění článku 66 obecného nařízení (postup pro naléhavé případy).

Součástí pokynů je i stručná příručka, která má poskytnout odborníkům v dozorových úřadech rychlý přehled o postupu v jednotlivých fázích spolupráce mezi dozorovými úřady a tento složitý postup názorně popsat.

## ● VÝVOJ V OBLASTI PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ, KODEXŮ CHOVÁNÍ A CERTIFIKACÍ

### Předávání údajů do třetích zemí

GDPR klade maximální důraz na jednotný výklad a jednotný postup všech dozorových úřadů, a to platí i v oblasti přenosů údajů do třetích zemí. V důsledku toho se těžiště práce v oblasti předávání výrazně přeneslo z jednotlivých dozorových úřadů na EDPB, resp. na jeho pracovní podskupiny International Transfers Subgroup (ITS) a Borders, Travel & Law Enforcement (BTLE), v nichž má Úřad své zástupce.

Podskupina ITS vypracovala a EDPB schválil dlouho očekávané Pokyny 5/2021 ke vztahu mezi čl. 3 a kap. 5 GDPR. Tyto pokyny přinášejí vymezení pojmu předání osobních údajů podle kap. 5. Práce na této definici trvala dosud cca 5 let a není stále ukončená.

Původní logické východisko práce vycházelo z předpokladu, že k předání dochází tehdy, když osobní údaje opouštějí prostor aplikace GDPR. Jinými slovy případy předání údajů entitám ve třetích zemích, které podléhají GDPR podle čl. 3, by nebyly předáním, protože by nebyl důvod uplatňovat na takové entity hned dvojí požadavky, tj. požadavek splňovat celé GDPR, a zároveň požadavek vytvořit vhodné záruky podle čl. 46 GDPR.

Zástupci některých dozorových úřadů ovšem namítali, že je velmi obtížné vymoci po entitách ve třetích zemích dodržování GDPR, a proto je třeba vyžadovat implementaci nástrojů čl. 46 GDPR, které jsou založeny na soukromoprávních závazcích takových entit, přičemž vymáhání soukromoprávních závazků, např. standardních smluvních doložek, je jednodušší než vymáhání dodržování GDPR ve třetí zemi. Tento přístup se nakonec prosadil, takže výslednou definici předání v uvedených pokynech lze jednoduše shrnout takto: předáním je, když správce nebo zpracovatel, který podléhá GDPR, bez ohledu na to, zda je v EU nebo ve třetí zemi, zpřístupní nebo přeneše údaje jinému správci nebo zpracovateli ve třetí zemi, bez ohledu na to, zda tento dovozce podléhá GDPR, nebo ne. To znamená, že přenos údajů správci nebo zpracovateli ve třetích zemích, kteří podléhají GDPR podle čl. 3 odst. 2, je předáním.

V roce 2022 proběhla veřejná konzultace a ITS podskupina vypořádávala její výsledky. Některé připomínky z veřejné konzultace upozornily na nerovnováhu, která vznikla tím, že zatímco přenos údajů správci nebo zpracovateli ve třetích zemích, kteří podléhají GDPR podle čl. 3 odst. 2, je podle nových pokynů předáním, tak přenos údajů v rámci provozoven podle čl. 3 odst. 1 předáním není. Tento problém ITS dlouhodobě diskutuje, přičemž i v případě přenosu údajů provozovnám ve třetích zemích podle čl. 3 odst. 1 je pocífována nezbytnost přijetí určitých opatření a záruk bez ohledu na to, zda daný přenos bude kvalifikován jako předání podle kapitoly 5 GDPR, nebo ne. Definitivní znění pokynů bude přijato až v roce 2023.

Vývoj zaznamenaly i jednotlivé nástroje pro předávání podle čl. 46 a 47 GDPR, jako jsou:

### Standardní smluvní doložky

Zdaleka nejpopulárnějším a nejpoužívanějším nástrojem pro předávání jsou standardní smluvní doložky. Evropská komise vydala 4. června 2021 rozhodnutí 2021/914, kterým stanovila nový text standardních smluvních doložek určený pro všechna předávání, kdy vývozcem je správce nebo zpracovatel podléhající GDPR a dovozcem je správce nebo zpracovatel nepodléhající GDPR. Nový text standardních

smluvních doložek sestává z několika modulů a pokrývá všechny čtyři možné scénáře, tzn. předání správce–správci, správce–zpracovateli, zpracovatel–správci a zpracovatel–zpracovateli, a zároveň počítá s připojováním dílčích zpracovatelů.

Přechodné ustanovení rozhodnutí Komise stanoví, že staré smluvní doložky z dob Směrnice 95/46/ES přestávají definitivně poskytovat vhodné záruky podle čl. 46 odst. 2 písm. c) k 27. prosinci 2022. Nejpozději do 27. prosince 2022 museli tedy všichni vývozci osobních údajů smluvní doložky staršího znění ukončit a nahradit je novými.

Nové standardní smluvní doložky již reflektují rozsudek Evropského soudního dvora ve věci C-311/18 Schrems II, kterým byl zrušeno rozhodnutí Komise 2016/1250 o odpovídající úrovni ochrany poskytované Štítem soukromí. Nicméně i nadále platí, že uzavření smluvních doložek nezabývá samo o sobě smluvní strany povinnosti provést předem analýzu přiměřenosti s cílem řešit případné dopady právních předpisů třetí země na dodržování doložek ze strany dovozce. Zejména se jedná o problematiku, jak vyřídit závazné žádosti orgánů veřejné moci třetí země týkající se zpřístupnění předávaných osobních údajů.

### Závazná podniková pravidla (BCR)

Na rozdíl od standardních smluvních doložek, které musejí být specifikovány pro každé předávání, ošetřují schválená [závazná podniková pravidla](#) (dále také jen „BCR“) v zásadě veškeré předávání osobních údajů v rámci skupiny podniků.

Závazná podniková pravidla získala svou základní sadu dokumentů pro jejich implementaci v podmínkách GDPR ještě v letech 2016–2018 před vznikem EDPB. Jedná se o schvalovací proceduru (WP263), formulář žádosti o schválení BCR pro správce (WP264) a pro zpracovatele (WP265), a především tzv. referentials, které rozpracovávají prvky a zásady, které musejí být součástí BCR pro správce (WP256) i pro zpracovatele (WP257). Lze konstatovat, že v roce 2021 se práce na stanoviscích EDPB na základě podaných žádostí o schválení BCR ze strany konkrétních nadnárodních skupin plně rozběhla a stává se postupně „rutinní“ záležitostí. Do konce roku 2022 EDPB vydal celkem 42 kladných sta-



novisek ke konkrétním BCR a desítky dalších žádostí čekají na schválení.

Na základě získaných zkušeností se schvalováním BCR podskupina ITS v roce 2022 finalizovala novou verzi výše uvedených dokumentů, kterou EDPB přijal jako Doporučení 1/2022 k žádosti o schválení a k prvkům a zásadám, které musejí být součástí BCR pro správce. Tento dokument upřesňuje a prohlubuje požadavky kladené na BCR pro správce. Příslušný dokument pro zpracovatele by měl být vypracován a přijat v průběhu roku 2023.

### **Kodexy chování a certifikace jako bezpečné nástroje předávání**

Základním východiskem pro práci s kodexy chování a certifikacemi je uvědomění si, že EDPB ve svých pokynech striktně oddělil dva typy kodexů chování a certifikací podle jejich účelu.

První typ kodexů chování a certifikací má účel prokázat shodu s GDPR a je určen pro správce a zpracovatele, kteří podléhají GDPR, prvoplánově pro ty, kteří sídlí v EU. K tomu EDPB již vydal nejen výkladové pokyny, ale i první stanoviska ke konkrétním nadnárodním kodexům chování a konkrétním certifikačním kritériím.

Druhý typ kodexů chování a certifikací má za účel vytvořit vhodné záruky pro ochranu osobních údajů ve třetí zemi a je určen primárně pro dovozce údajů ve třetích zemích. Obecný model je takový, že tyto dovozci svou účastí na takovém kodexu chování nebo svou certifikací vytvoří rámcové vhodné záruky pro předávané údaje, které pak budou završeny smlouvou s vývozcem údajů, která zajistí závazné a vymahatelné závazky dovozce tyto vhodné záruky uplatňovat, jak to předpokládají čl. 46 odst. 2 písm. e) a f) GDPR.

Podskupina ITS vypracovala a EDPB přijal Pokyny 4/2021 ke kodexům jako nástroji pro předávání, které už mají definitivní znění po veřejné konzultaci, a dále Pokyny 7/2022 k certifikacím jako nástroji pro předávání, ke kterým byla veřejná konzultace rovněž již uzavřena a jejíž výsledek je podskupinou ITS v současné době vypořádáván.

### **Předávání údajů do USA**

Rozsudek Soudního dvora EU (SDEU) Schrems II učinil velmi problematickým především předávání osobních údajů do USA poskytovatelům elektronických služeb, na něž se vztahuje zákon FISA 702<sup>19</sup>, potažmo EO 12 333,<sup>20</sup> které rozsudek Schrems II identifikoval jako překážku v zásadě rovnocenné ochrany osobních údajů, protože ukládají poskytovatelům elektronických služeb povinnost vyhovět plošnému přístupu amerických státních orgánů k předaným datům, který jde nad rámec toho, co je obvyklé v demokratické společnosti.

Prezident USA na začátku října 2022 vydal prezidentský dekrét, ve kterém stanovil nový postup federálních agentur a úřadů při sběru osobních údajů.

Zmíněný dekrét se snaží vyjít vstříc požadavkům rozsudku Schrems II, čili omezit pravomoci zpravodajských služeb USA, a obsahuje závazek provádět zpravodajské činnosti pouze za účelem dosažení stanovených cílů národní bezpečnosti a zohledňovat soukromí a občanské svobody všech osob bez ohledu na jejich státní příslušnost nebo zemi pobytu. Má být také zřízen nezávislý soud, který bude projednávat případy ochrany osobních údajů.

EU zahájila formální kroky potřebné ke schválení rámce EU a USA pro ochranu osobních údajů, počínaje přípravou návrhu rozhodnutí Komise o odpovídající ochraně údajů. Návrh nového právního rámce předložený Evropskou komisí bude předmětem posuzování ze strany EDPB, pravděpodobně pracovních podskupin ITS a BTLE, v rámci jejichž jednání bude prostor i pro Úřad, aby se aktivně zapojil do debat o konečné podobě nového právního rámce.

### **Předávání údajů v rámci využívání různých služeb**

V případě používání různých služeb a aplikací, např. od společností Microsoft či Google, které mohou využívat jednotlivé subjekty (např. školy v rámci výukového programu, může se jed-

<sup>19</sup> Jedná se o § 702 zákona o zabezpečování informací o činnostech cizí moci (Foreign Intelligence Surveillance Act).

<sup>20</sup> Jedná se o Výkonný dekrét prezidenta US (Executive Order 12 333).

nat o aplikace na videohry, na chat, nástroje na editaci dokumentů apod.), může zároveň docházet k předávání určitých kategorií osobních údajů, které jsou prostřednictvím poskytované služby zpracovávány, do třetích zemí, v případě Googlu a Microsoftu jako amerických společností primárně do Spojených států. Mnozí správci dnes často vůbec netuší, že jejich softwarová řešení pro sdílení dat nebo typicky videokonferenční systémy, používají nástroje Microsoft nebo Google, které mohou předávat osobní údaje o chování subjektů údajů do Spojených států.

Správce musí mít vždy na paměti, že předávání osobních údajů do třetích zemí může být spojeno s riziky, např. v důsledku rozporných vnitrostátních právních předpisů nebo přístupu vládních orgánů ve třetí zemi k osobním údajům, jakož i s obtížemi při vymáhání a získávání nápravy vůči entitám mimo EHP. Správce je odpovědný za své činnosti zpracování bez ohledu na to, kde probíhají, a musí vždy postupovat v souladu se základními principy zpracování a plnit povinnosti, které mu GDPR ukládá: čl. 24 (odpovědnost správce), čl. 25 (záměrná a standardní ochrana osobních údajů), čl. 28 (zpracovatelská smlouva), čl. 30 (záznamy o činnosti zpracování), čl. 32 (zabezpečení zpracování), čl. 33 (oznamování případů porušení zabezpečení osobních údajů), čl. 35 (posouzení vlivu na ochranu osobních údajů), čl. 48 (předávání nebo zpřístupňování nepovolené právem Unie).

V návaznosti na svou povinnost zavést technická a organizační opatření zohledňující mimo jiné rizika v souvislosti se zpracováním podle čl. 32 GDPR, případně provedením posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR, může správce dojít k závěru, že jsou zapotřebí rozsáhlá bezpečnostní opatření nebo že reálně neexistují žádná opatření technického ani organizačního rázu, která by dokázala minimalizovat předem definovaná rizika na přijatelnou úroveň, a předávání do třetí země tak z objektivních důvodů není možné. V takovém případě by správce neměl takovou službu využívat.

Nelze tedy pouze spoléhat na konstatování ze strany poskytovatele služeb, že plní požadavky GDPR. Soudní dvůr Evropské unie (dále „SDEU“)

ve svém rozsudku Schrems II rozvíjí detailně základní požadavky pro předávání údajů do třetích zemí. Především zdůrazňuje odpovědnost správců a zpracovatelů zajistit, aby zpracování probíhalo v souladu s úrovní ochrany stanovené právními předpisy EU o ochraně údajů, a pozastavit přenos nebo ukončit smlouvu v případě, kdy dovozce údajů není schopen dostát svým závazkům. Zdůrazňuje povinnost správců a zpracovatelů činit proaktivní opatření a povinnost průběžně provádět opatření na podporu a ochranu údajů při jejich zpracování – odst. 139 rozsudku SDEU.

Další povinností správce, která je často opomíjena, je povinnost informovat subjekt údajů o tom, že jeho osobní údaje jsou předávány mimo EU, resp. EHP do třetí země a správce musí poskytnout vysvětlení, co to pro něj znamená. Čl. 13 odst. 1 písm. f) GDPR výslovně ukládá správci povinnost sdělit subjektu údajů úmysl předat osobní údaje do třetí země nebo mezinárodní organizaci a dále povinnost informaci doplnit o to, jaké záruky správce přijal, aby subjektu údajů byla garantována bezpečná úroveň ochrany jeho osobních údajů ve třetí zemi.

### **Osvědčení o ochraně osobních údajů (certifikační mechanismy)**

V oblasti certifikací trvá nevyjasněná situace, která vznikla na konci roku 2021. Na základě připomínek EDPB k návrhu Úřadu „Požadavky na akreditaci subjektů pro vydávání osvědčení“ a připomínek vzešlých z meziresortního připomínkového řízení k návrhu vyhlášky o požadavcích na akreditaci subjektů pro vydávání osvědčení, k provedení zákona č. 110/2019 Sb., bylo zjištěno, že v souvislosti s rozdílnými požadavky stanovenými ze strany EDPB a legislativními pravidly vlády na obsah a strukturu dokumentů, a požadavkům na akreditaci subjektů pro vydávání osvědčení, nelze vytvořit dokument přijatelný pro obě strany (EDPB a Legislativní radu vlády).

Aby Úřad dostal své povinnosti zveřejnit akreditační požadavky ve snadno přístupné formě a předat je EDPB (čl. 43 odst. 6 GDPR), jsou zvažovány jiné možnosti řešení vyplývající z dikce § 54 odst. 1, písm. d) zákona č. 110/2019 Sb., o zpracování osobních údajů, který uvádí, že





Úřad „může stanovit vyhláškou kritéria nebo požadavky podle čl. 41 odst. 3, čl. 42 odst. 5 nebo čl. 43 odst. 1 písm. b) nařízení Evropského parlamentu a Rady (EU) 2016/679“.

## Kodexy chování

Požadavky na akreditaci subjektů pro monitorování kodexů chování byly Sboru předloženy v roce 2021, po projednání a vydání jeho stanoviska byly připomínky uvedené ve stanovisku zapracovány a výsledné znění ještě v roce 2021 znovu předloženo Sboru. Upravenou verzí stanoviska se EDPB do konce roku 2022 nezabýval. Požadavky na akreditaci subjektů pro monitorování kodexů chování Úřad zveřejňuje obdobně jako v případě Požadavků na akreditaci subjektů pro vydávání osvědčení. Je vysoce pravděpodobné, že bude nutné řešit obdobný problém neslučitelnosti jako v případě Požadavků na akreditaci subjektů pro vydávání osvědčení (viz výše).

V roce 2022 Úřad neschválil žádný kodex chování. Schválení jakéhokoliv kodexu není možné vzhledem k neexistenci schválených požadavků na akreditaci subjektů pro monitorování kodexů chování (není možno ustanovit monitorující subjekty a bez jejich ustanovení postrádá schvalování kodexů chování smysl). Předmětný rozpor by bylo vhodné řešit novelizací příslušného ustanovení zákona č. 110/2019 Sb., o zpracování osobních údajů.

## ZÁVAZNÁ ROZHODNUTÍ PODLE ČL. 65 GDPR

Základními prvky přeshraniční spolupráce jsou principy spolupráce a jednotnosti. Pokud se ovšem nedaří najít konsensus mezi dozorovými úřady, nastupuje role EDPB, a pro tyto účely jsou mu svěřeny některé pravomoci. Například podle čl. 65 odst. 1 písm. a) GDPR Sbor přijme závazné rozhodnutí v případě, že členské dozorové úřady mají odlišný pohled na návrh rozhodnutí vedoucího dozorového úřadu v konkrétní přeshraniční věci (čl. 60 odst. 3 GDPR).

V uplynulém roce přijal EDPB následující závazná rozhodnutí podle čl. 65 GDPR:

- [Závazné rozhodnutí 01/2022 – Accor SA \(FR\)](#).

- [Závazné rozhodnutí 02/2022 – Meta Platforms Ireland Limited \(Instagram\) \(IE\)](#),
- [Závazné rozhodnutí 03/2022 – Meta Platforms Ireland Limited \(Facebook\) \(IE\)](#),
- [Závazné rozhodnutí 04/2022 – Meta Platforms Ireland Limited \(Instagram\) \(IE\)](#),
- [Závazné rozhodnutí 05/2022 – Meta Platforms Ireland Limited \(WhatsApp\) \(IE\)](#).

## Zpracování jako nezbytnost pro splnění smlouvy

Přestože každé závazné rozhodnutí EDPB plní svým způsobem jednotící funkci v rozhodovací praxi členských dozorových úřadů, tři rozhodnutí z minulého roku si zaslouží zvláštní pozornost vzhledem k významu řešené otázky. Přestože se formálně jedná o vícero řízení, konkrétně závazná rozhodnutí 02/2022, 03/2022, 04/2022 a 05/2022 ve věcech Facebook, Instagram a WhatsApp (správce Meta Platforms Ireland Limited), jádro problému zůstává v zásadě obdobné – lze považovat zpracování osobních údajů uživatelů služeb pro účely marketingu na základě chování jedince (behaviorální marketing, resp. reklama), zlepšování kvality služeb apod. za zpracování nezbytné pro splnění smlouvy podle čl. 6 odst. 1 písm. b) GDPR? Podle EDPB v obecné rovině nikoliv.

Správce osobních údajů zakomponoval informaci o možnosti zpracování osobních údajů pro shora uvedené účely do smluvních podmínek, které každý uživatel musí přijmout, pokud chce služby správce využívat. Podle jeho přesvědčení se tak jednalo o zpracování nezbytné pro splnění smlouvy, přičemž je svobodným rozhodnutím každého správce, na kterém z právních titulů nabízených článkem 6 GDPR své zpracování založí.

EDPB svou argumentaci založil na ustanovení čl. 8 odst. 1 Listiny základních práv a svobod Evropské unie a čl. 16 odst. 1 Smlouvy o fungování EU. A dále GDPR rozvíjející tato ustanovení primárního práva jako právní předpis EU reagující na rychlý technologický rozvoj a neustálé navyšování množství shromažďovaných a sdílených dat, jehož cílem je zajistit vysokou

úroveň ochrany osobních údajů tak, aby bylo právo na ochranu osobních údajů přiměřeně vyváženo i ve vztahu k ostatním základním právům – v tomto případě primárně k právu na podnikání. V této souvislosti zvláště zdůraznil, že právo na ochranu osobních údajů je základním lidským právem a součástí důstojnosti člověka, nikoliv obchodovatelnou komoditou, a takto je k němu třeba přistupovat. Ostatně i SDEU v rozsudku *Google Spain SL* potvrdil, že právo na soukromí a ochranu osobních údajů zpravidla převažuje nad ekonomickými zájmy správce osobních údajů.

Podle EDPB skutečně neexistuje hierarchie mezi právními tituly pro zpracování osobních údajů, nicméně správce vždy musí zvolit takový právní titul, s jehož pomocí bude schopen dodržet veškeré navazující povinnosti tak, aby zpracování neodporovalo zásadám korektnosti, zákonnosti, transparentnosti a vůbec smyslu přijetí GDPR. Povinnosti správce se totiž uplatní i v situaci, kdy by správce s ohledem na své ekonomické zájmy preferoval odlišný postup.

Základem každého zpracování, které je nezbytné pro účely splnění smlouvy, je schopnost správce prokázat, že a) smlouva existuje a b) smlouva je platná. A přestože GDPR napřímo nepřiznává dozorovým úřadům pravomoc přímo rozhodovat o smluvních otázkách, každý dozorový úřad musí disponovat alespoň omezenou kompetencí posoudit platnost smlouvy v rozsahu nezbytném pro účely dostání svým úkolům v oblasti ochrany osobních údajů. To znamená, že nemůže považovat smlouvu za platnou např. v případě, že zjevně nebyla dostatečným způsobem projevena vůle smluvní strany ji uzavřít.

Dále se EDPB zabýval podmínkami podle samotné dikce ustanovení čl. 6 odst. 1 písm. b) GDPR, podle něhož je zpracování zákonné „pouze pokud (...) je nezbytné pro splnění smlouvy...“ Prvek nezbytnosti je pak podle EDPB objektivní kategorií, posuzováno optikou povahy poskytované služby, přičemž nesmí existovat alternativní méně invazivní možnost zpracování. Jak bylo v závazném rozhodnutí zvláště zdůrazněno, předmětný článek pokrývá toliko situace, kdy je zpracování skutečně nezbytné, a to pro samotné splnění smlouvy. Nikoliv

již však situace, kdy by takové zpracování bylo pouze užitečné či třeba dokonce i nezbytné, avšak pouze z pohledu dalších ekonomických zájmů správce. Současně musí být správce připraven tuto nezbytnost řádně odůvodnit, a to jak s ohledem na základní povahu jím nabízené služby, tak i s přihlédnutím k tomu, jak tuto službu a vztahy ze smlouvy vzniklé prezentuje svým uživatelům. Zásadní roli při interpretaci ustanovení podle EDPB hraje i otázka transparentnosti zpracování, neboť zpracování osobních údajů může být nezbytné pouze ve vztahu k tomu účelu, který může průměrný subjekt údajů rozumně očekávat. V této souvislosti pak EDPB ještě citoval stanovisko generálního advokáta SDEU Rantose, podle něhož je třeba ve vztahu k předmětnému právnímu titulu zaujmout zvláště přísný restriktivní přístup vzhledem k možnosti jeho využívání k obcházení požadavků na udělení platného souhlasu.

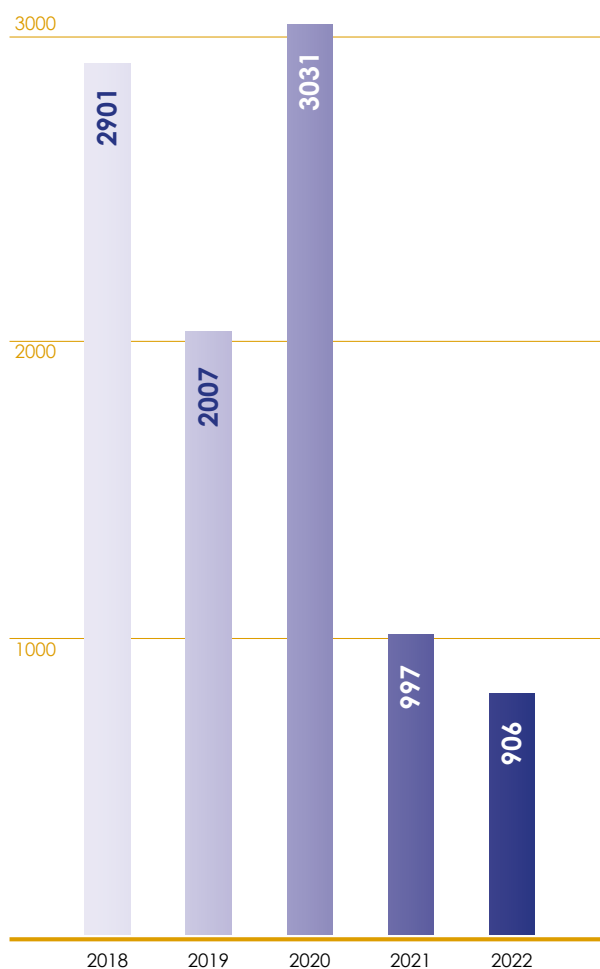
EDPB v rámci své argumentace v neposlední řadě odkázal i na ustanovení čl. 21 odst. 2 a 3 GDPR. To podle jeho názoru představuje absolutní právo subjektu údajů podat kdykoliv a bez uvedení jakéhokoliv důvodu námitku proti zpracování jeho osobních údajů pro účely přímého marketingu (včetně případného profilování), v důsledku čehož nelze tyto údaje jakkoli dále zpracovávat pro uvedené účely. To i s ohledem na veškerou další argumentaci EDPB zjevně svědčí ve prospěch závěru, že behaviorální reklama nemůže být nezbytná pro splnění smlouvy, a to lze považovat za obecné pravidlo.



## NEVYŽÁDANÁ OBCHODNÍ SDĚLENÍ

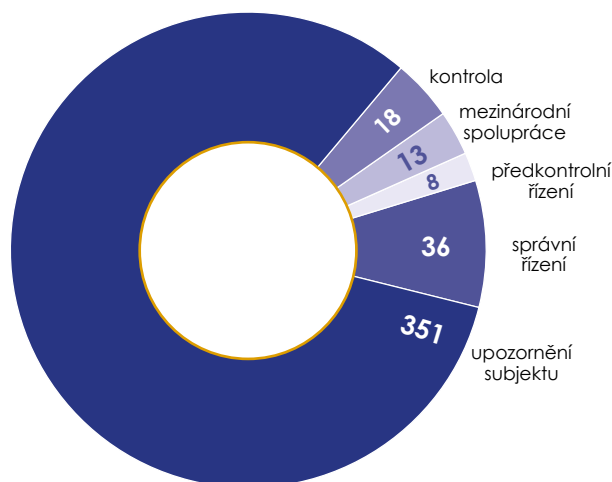
Úřad za rok 2022 evidoval celkem 906 podaných stížností na šíření nevyžádaných obchodních sdělení. Pokud tento počet porovnáme s rokem 2021, jedná se o velice podobné číslo. Oproti předchozím letům, kdy počet podaných stížností dosahoval několika tisíc, dochází nyní v této oblasti k určité stagnaci. Z dozorové činnosti je však patrné, že snížení počtu stížností neznamená nižší počet provedených řízení, ať už kontrolních, správních či jen formou upozornění dané společnosti.

## PODANÉ STÍŽNOSTI



## Shrnutí dozorové činnosti v oblasti šíření obchodních sdělení

### DOZOROVÁ ČINNOST V OBLASTI ŠÍŘENÍ OBCHODNÍCH SDĚLENÍ ZA ROK 2022



Z výše uvedeného grafu dozorových činností lze vyčíst, že stále je většina společností na zasílání nevyžádaných obchodních sdělení pouze upozorňována a žádána o provedení nápravy. Nejsou neobvyklé případy, kdy společnost, která byla na možné porušení upozorněna, právní titul k zasílání obchodních sdělení na daný elektronický kontakt skutečně doložila. Jednalo se o případy, kdy adresátem byl zákazník dané společnosti a tato společnost mu zaslala obchodní sdělení v souladu s § 7 odst. 3 zákona č. 480/2004 Sb., tedy na základě oprávněného zájmu, jelikož jeho elektronický kontakt získala v souvislosti s prodejem výrobku nebo služby. V této souvislosti je tedy třeba uvést, že ne každá stížnost nutně znamená porušení povinností při zasílání obchodních sdělení. Mnohdy si totiž sami stěžovatelé již nevybavují, že u dané společnosti nakoupili, uvedli svůj elektronický kontakt, a tato společnost jim pak může obchodní sdělení oprávněně zaslat. Někteří stěžovatelé se totiž mylně domnívají, že zaslat obchodní sdělení lze pouze po předchozím souhlasu. Určitá osvětová činnost je tak nutná, nejen ve vztahu ke společnostem, které obchodní sdělení zasílají, ale také k adresátům těchto sdělení. Tato činnost je pak plněna zejména prostřednictvím

webových stránek Úřadu, kde jsou uvedeny informace, jak ve vztahu k jednotlivým podmínkám pro zasílání obchodních sdělení, tak také pro podávání stížností. Kromě výše uvedených výzev jsou však vedena i kontrolní řízení. Těch bylo v roce 2022 celkem 18, a dále bylo Úřadem vedeno 30 správních řízení. Celková výše sankce činila 828 000 Kč. V šesti případech byla uložena též pořádková pokuta za neposkytování součinnosti v rámci kontrolního řízení a celková výše těchto pokut činila 120 000 Kč. Zahraničním úřadům (většinou na Slovensko) bylo postoupeno celkem 13 případů. Kontroly a správní řízení byly vedeny převážně se společnostmi, které provozují internetové obchody, kde nabízejí své výrobky a služby, ale také s finančními institucemi nebo společnostmi zabývajícími se průzkumy trhu či vydáváním periodik apod. V rámci správních řízení se často jednalo o opakovaná porušení (např. po předchozí kontrole nebo upozornění subjektu) či zasílání obchodních sdělení po předchozích prokazatelných odmítnutích jejich adresáty.

Nejčastějšími dotazy v roce 2022, které posléze vyústily i v doplnění informací na webových stránkách Úřadu, byly dotazy směřující k dodržování podmínek při zasílání obchodních sdělení formou SMS zpráv, zejména pokud jde o povinnost označení, dále také uvedení toho, jehož jménem se komunikace uskutečňuje, a zejména uvedení možnosti, jak zasílání takových obchodních sdělení odmítnout.

### **Závěry z dozorové činnosti v oblasti nevyžádaných obchodních sdělení**

Z kontrolní činnosti je třeba zmínit kontrolu společnosti, která v potvrzovacím e-mailu o provedeném nákupu uváděla nabídku třetích stran (se kterými měla uzavřeny předmětné smlouvy o marketingové spolupráci). Jednalo se o nabídky různých slev a voucherů u daných partnerů. Tato společnost argumentovala tím, že se o obchodní sdělení nejedná, jelikož jde pouze o odměnu či bonus, kterou zákazník může, ale nemusí využít bez splnění dalších podmínek. Z definice obchodního sdělení je však nepochybné, že i takovéto nabídky, byť jsou poskytovány jako odměny či bonusy těm, kteří u dané společnosti provedou nákup, se za obchodní

sdělení považují, jelikož propagují výrobky či služby třetí strany (dalšího podnikatelského subjektu) a jsou zasílány elektronickými prostředky (e-mailem). V tomto případě pak nelze pro zasílání takových obchodních sdělení využít právního titulu oprávněného zájmu, jelikož podle § 7 odst. 3 zákona č. 480/2004 Sb. by se muselo jednat o nabídku vlastních obdobných výrobků nebo služeb, nikoli tedy nabídku dalšího podnikatelského subjektu. Daná společnost by tak mohla předmětná obchodní sdělení zasílat pouze na základě souhlasu, tedy adresáti (zákazníci) by jí udělili souhlas k zaslání obchodního sdělení ve prospěch třetí strany. K tomu je nutno uvést, že podmínky pro získání platného souhlasu podle GDPR jsou použitelné i v situacích spadajících do oblasti působnosti směrnice 2002/58/ES, resp. zákona č. 480/2004 Sb. Z povahy souhlasu se zasíláním obchodních sdělení je patrné, že osoba udělující souhlas musí vědět, k čemu předmětný souhlas dává (pro jaký účel, k jakému zasílání obchodních sdělení, jakému subjektu nebo ve prospěch jakého subjektu jí budou obchodní sdělení zasílána). Společnost však neprokázala, že by takovým souhlasem adresátů disponovala. Tato kontrola byla významná zejména v tom ohledu, že daná společnost obchodní sdělení ve prospěch třetích subjektů zasílá již od roku 2015, přičemž tímto způsobem bylo za dané období osloveno více jak 40 milionů zákazníků.

Ve správním řízení stojí za zmínku řízení, které bylo zahájeno po provedené kontrole, ve které bylo konstatováno zasílání obchodních sdělení bez souhlasu adresátů ve prospěch obchodní společnosti, která však v rámci celého kontrolního řízení uváděla, že s danými rozesílkami (byť byly zasílány v její prospěch) nemá nic společného. Pro zasílání předmětných obchodních sdělení byly totiž použity freemailové účty s doménou post.cz či seznam.cz. Skutečnost, že za šíření obchodních sdělení je odpovědná kromě faktického odesílatele i společnost, v jejíž prospěch jsou obchodní sdělení zasílána, byla již několikrát Úřadem konstatována a též potvrzena judikaturou. V rámci tohoto správního řízení se však Úřadu podařilo vypátrat i faktického odesílatele předmětných obchodních sdělení, a to pomocí součinnosti společnosti Seznam.cz a.s., která k odesílajícím



e-mailovým adresám uvedla, že daná obchodní sdělení nebyla odesílána ze serveru freemailu Seznam.cz, ale třetí stranou, a to dle dostupných informací ze serveru pod amazon.com. Dále tak správní orgán s žádostí o součinnost oslovil též společnost AMAZON WEB Services Inc., která na základě zdrojových kódů z odesílaných obchodních sdělení (message-ID) identifikovala účet, který byl pro předmětné rozesílky použit. Tento účet, byť byl veden na smyšlené údaje, obsahoval i fakturační informace, které již byly vázány ke konkrétní fyzické osobě. Bylo zjištěno, že tato osoba figuruje v různých společnostech, které se zabývají činnostmi v oblasti informačních technologií a které se svým názvem velice podobají názvu společnosti, v jejíž prospěch byla předmětná obchodní sdělení šířena, a že hosting předmětných domén je na IP adrese, která je vedena pod zákaznickým účtem na tuto osobu (resp. s totožným jménem). Správní řízení tak na základě výše uvedených zjištění bylo zahájeno i s touto fyzickou osobou. Ze zjištěných skutečností bylo patrné, že spojitost mezi touto fyzickou osobou, která danou rozesílku fakticky provedla (tedy faktickým odesílatelem), a společností, v jejíž prospěch byla provedena, nebyla náhodná. Úřad tak v rámci správního řízení konstatoval spáchání přestupku v oblasti šíření obchodních sdělení jak u fyzické osoby (jakožto faktického odesílatele), tak i u společnosti, v jejíž prospěch byla předmětná obchodní sdělení zasílána. ●

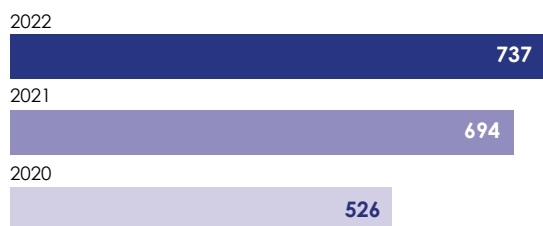
## • Rozhodování Úřadu v oblasti svobodného přístupu k informacím

### • PŮSOBNOST ÚŘADU

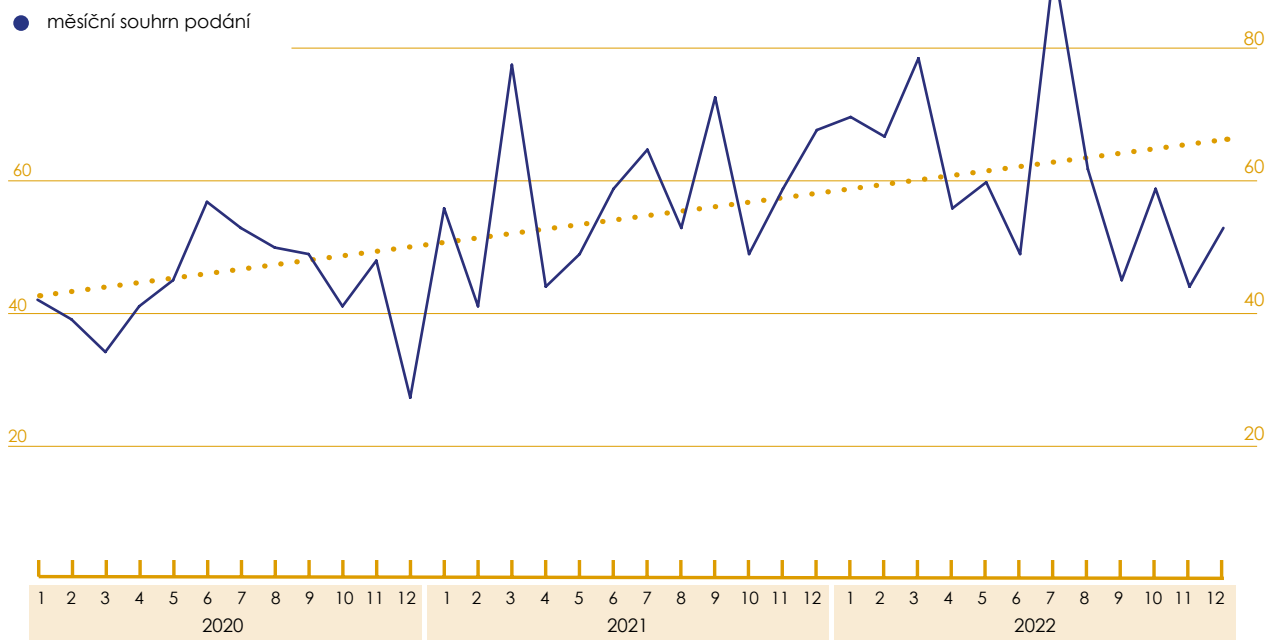
Úřad vykonává působnost vyplývající ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve třech oblastech.

1) Úřad je nadřízeným orgánem těch povinných subjektů, jejichž nadřízený orgán nelze určit podle § 178 správního řádu. V takových případech Úřad rozhoduje jak o odvolání proti rozhodnutí povinného subjektu o odmítnutí žádosti o informace, tak o stížnosti na postup povinného subjektu při vyřizování žádosti o informace. Taxativní výčet těchto povinných subjektů stanoven není, jejich okruh se postupně vyvíjí především s ohledem na soudní judikaturu.

### SROVNÁNÍ VELIKOSTI NÁPADU V LETECH 2020–2022



### VÝVOJ MĚSÍČNÍHO NÁPADU AGENDY PODLE ZÁKONA Č. 106/1999 SB. V LETECH 2020–2022





- 2) Úřad je v oblasti svobodného přístupu k informacím přezkumným orgánem. Přezkoumat je možné pravomocné rozhodnutí jakéhokoliv nadřízeného orgánu vydané v odvolacím řízení, jestliže lze důvodně pochybovat o tom, že je takové rozhodnutí v souladu s právními předpisy. Rozhodnutí o stížnosti na postup povinného subjektu při vyřizování žádosti o informace přezkumu nepodléhají. Přezkumné řízení je vedeno z moci úřední, avšak účastník řízení může dát podnět k jeho provedení.
- 3) Úřad je příslušný k přijímání opatření proti nečinnosti nadřízeného orgánu, a to jak v řízeních o odvolání či rozkladu, tak v řízeních o stížnosti na postup povinného subjektu při vyřizování žádosti o informace.

Úřad tyto pravomoci vykonává od 1. 1. 2020. Smyslem nově založené působnosti Úřadu v agendě svobodného přístupu k informacím bylo především sjednocení a zrychlení rozhodování v této oblasti, odbřemenění správních soudů a větší tlak na povinné subjekty, aby jednotlivým žádostem o informace věnovaly patřičnou pozornost a svá případná rozhodnutí pečlivě odůvodňovaly. Zásadní dopady do plnění úkolů Úřadu přinesla novela zákona č. 106/1999 Sb. provedená zákonem č. 241/2022 Sb., přičemž její vyhodnocení bude možné po zkušenostech z aplikační praxe.

## Rozhodovací činnost v číslech

nadřízený orgán (§ 20 odst. 5 zákona č. 106/1999 Sb.)	
1) odvolání	
– informační příkaz	5
– rozhodnutí povinného subjektu potvrzeno	48
– rozhodnutí povinného subjektu zrušeno, věc vrácena k novému projednání	152
– rozhodnutí povinného subjektu částečně potvrzeno, v části rozhodnutí povinného subjektu zrušeno a věc vrácena k novému projednání	7
– ostatní způsoby vyřízení	3
2) stížnost na postup povinného subjektu	
– postup potvrzen	26
– příkaz povinnému subjektu vyřídit žádost	33
– v části postup potvrzen, v části příkaz povinnému subjektu vyřídit žádost	13
– výše úhrady požadované povinným subjektem snížena	33
– ostatní způsoby vyřízení	1
3) opravný prostředek postoupen jinému subjektu z důvodu nepříslušnosti Úřadu	41
přezkum (§ 16b odst. 1 a 2 zákona č. 106/1999 Sb.)	
– přezkumné řízení nezahájeno	87
– rozhodnutí nadřízeného orgánu zrušeno, věc vrácena	5
– přezkumné řízení zastaveno	1
ochrana před nečinností (§ 16b odst. 3 zákona č. 106/1999 Sb.)	
– nedůvodný podnět	77
– opatření proti nečinnosti	105

## POZNATKY Z ROZHODOVACÍ PRAXE ÚŘADU A Z JUDIKATURY

### Informace o probíhajícím trestním řízení – žádost o poskytnutí textu trestního oznámení

Úřad v přezkumném řízení posuzoval adekvátnost aplikace ustanovení § 11 odst. 4 písm. a) zákona č. 106/1999 Sb. povinným subjektem, který není orgánem činným v trestním řízení. Žadatel požadoval text trestního oznámení. Povinným subjektem byla v tomto případě obec, která figurovala toliko v roli oznamovatele.

Úřad dospěl k závěru, že z podstaty typově vymezené informace (trestního oznámení) je evidentní, že její poskytnutí není z obecného hlediska v probíhajícím trestním řízení žádoucí, jelikož se lze důvodně obávat, že by mohla být

zpochybněna role státu při zjišťování trestných činů, odhalování, stíhání a odsuzování pachatelů trestných činů nebo při upevňování zákonosti. Po povinném subjektu, který není orgánem činným v trestním řízení, nelze objektivně požadovat úvahu v takovém rozsahu, jakého je schopen orgán činný v trestním řízení. Současně je ale třeba pečlivě rozlišovat mezi samotným trestním oznámením a dokumenty, které mohou být jeho přílohou. Tyto přílohy prostým založením do spisu policejního orgánu ochranu, kterou požívá text trestního oznámení, bez dalšího nezískávají.

### **Přípustnost přezkumného řízení – aplikace zásady non bis in idem**

Úřad v přezkumném řízení dospěl k závěru, že s ohledem na existenci dvou protichůdných správních rozhodnutí, z nichž jedno obživlo po rozhodnutí Nejvyššího správního soudu, je nutné upřednostnit zásadu „non bis in idem“ v pojetí judikatury správních soudů před podmínkou stanovenou v § 94 odst. 2 zákona č. 500/2004 Sb., správní řádu správního řádu, která přezkumné řízení v tomto ohledu nepřipouští.

Pokud by Úřad formalisticky vycházel z § 94 odst. 2 správního řádu a přezkumné řízení ne zahájil, docházelo by tímto postupem v řízeních podle zákona č. 106/1999 Sb. ke vzniku procesně nepřipustné situace, která by ve svém krajním důsledku nedávala účastníkům řízení dostatečnou záruku a přehled o tom, jakým způsobem by bylo o jejich ústavně zaručeném právu na informace rozhodováno a jaká zákonná omezení na žádané (ev. poskytnuté) informace materiálně dopadají. Jistým způsobem by nezahájením přezkumu bylo nepřímo podporováno porušení citované zásady non bis in idem.

### **Informace o fakturách za právní služby poskytnuté obci**

Úřad v přezkumném řízení posuzoval odepření poskytnutí faktur za právní služby poskytované obci, jež byly hrazeny z veřejných prostředků, přičemž dospěl k závěru, že tyto informace jsou z hlediska naplnění účelu práva na informace zakotveného v čl. 17 odst. 5 Listiny základních práv a svobod typickými informacemi sloužícími k veřejné kontrole hospodaření obce s veřejnými prostředky.

Rozhodnutí obou správních orgánů vyhodnotil Úřad jako nezákonná, neboť důvod, pro který byla žadatelova žádost odmítnuta, nemá v současném znění zákona č. 106/1999 Sb. ani v dosavadní judikatuře oporu, navíc v daném případě se jedná o standardní poskytnutí faktur k odběru právních služeb, tedy o informace typicky vypovídající o hospodářské činnosti povinného subjektu, na které se nadto vztahuje ustanovení § 8b odst. 1 a 3 zákona č. 106/1999 Sb. Informační příkaz vydaný v této věci Úřadem byl následně potvrzen jeho nadřízeným orgánem.

### **Výluka z práva na informace z důvodu ochrany autorského práva**

Úřad v odvolacím řízení přezkoumával adekvátnost aplikace § 11 odst. 2 písm. c) zákona č. 106/1999 Sb. (autorskopravní ochrana) ve vztahu k záznamovým archům s výsledky neúspěšných zkoušek s vyznačením nesprávných odpovědí. Úřad dospěl k závěru, že při užití tohoto obligatorního důvodu pro odmítnutí žádosti je nutné, aby povinný subjekt (zde vysoká škola) posoudil, zda požadovaná informace je dílem, jež kumulativně splňuje definiční znaky vymezené v § 2 zákona č. 121/2000 Sb., o právu autorském. Povinný subjekt se musí dále vypořádat s tzv. „třístupňovým testem“ vyplývajícím z § 29 odst. 1 téhož zákona a se závěry Ústavního soudu formulovanými v nálezu ze dne 21. 3. 2017, sp. zn. IV. ÚS 3208/16.

### **Poskytnutí kopie výplatní pásky vedoucího zaměstnance**

Úřad v odvolacím řízení přezkoumával postup povinného subjektu v případě žádosti o kopii výplatní pásky vedoucího zaměstnance a dospěl k závěru, že zákon č. 106/1999 Sb. nevylučuje, aby povinný subjekt omezil poskytnutí osobních údajů či údajů o soukromí fyzické osoby uvedených ve výplatní pásce i jiným adekvátním způsobem než anonymizací výplatní pásky, a to za předpokladu, že informační právo žadatele a účel zákona č. 106/1999 Sb. budou naplněny.

Úřad zdůraznil, že při poskytování informací podle zákona č. 106/1999 Sb. je podstatný obsah informací, nikoliv hmotný nosič tohoto obsahu. Úřad proto neshledal v rozporu s § 12 zákona č. 106/1999 Sb., pokud povinný subjekt





poskytl žadateli informace z výplatní pásky vedoucího zaměstnance, jejichž vydání zákon nezapovídá, formou samostatného sdělení a současně v rozsahu vyloučených informací žádost odmítl. Vzhledem k účelu výplatní pásky, kterým je umožnit zaměstnanci kontrolu správnosti výpočtu příjmu v příslušném kalendářním měsíci a jeho zúčtování o zákonné a další odvody, a vzhledem k obsahu výplatní pásky jakožto písemného dokladu sestávajícího téměř výlučně z osobních údajů či údajů vypovídajících o soukromí zaměstnance, považuje Úřad takový způsob poskytnutí informace za přiměřený. Žadateli umožňuje účinné využití poskytnutých informací a současně je šetrnější k právu na ochranu osobních údajů a soukromí dotčené osoby.

### **Aplikovatelnost ustanovení § 168 odst. 2 stavebního zákona jako speciálního důvodu pro odmítnutí žádosti o informace podané podle zákona o svobodném přístupu k informacím**

Úřad v odvolacím řízení přezkoumával rozhodnutí povinného subjektu o odmítnutí žádosti o stanovisko správce povodí k záměru stavebníka, které se opíralo o § 168 odst. 2 stavebního zákona, neboť nebyl dán souhlas pořizovatele dokumentace stavby, případně souhlas vlastníka stavby, které se dokumentace týká. Úřad musel předně určit, zda je výlučka uvedená v § 168 odst. 2 stavebního zákona aplikovatelná i ze strany správce povodí, přičemž dospěl k závěru, že na žádané stanovisko správce povodí nelze § 168 odst. 2 stavebního zákona aplikovat, neboť tento speciální důvod pojednává o omezení poskytnutí informace toliko ze strany stavebního úřadu.

Úřad přitom vyšel z textace ustanovení § 168 odst. 2 stavebního zákona a jazykovým výkladem dospěl k závěru, že tato výlučka se vztahuje na informace poskytované výlučně stavebním úřadem. Citované ustanovení nelze extenzivně rozšiřovat na další povinné subjekty. Správce povodí není stavebním úřadem, nevede správní řízení a nevydává jiná opatření podle stavebního zákona ani neeviduje a neukládá tomu odpovídající písemnosti ve smyslu ustanovení § 167 odst. 1 stavebního zákona. Úřad současně nevyločil, že požadované stanovisko může obsahovat některé chráněné údaje,

avšak posouzení, v jakém rozsahu je třeba tyto údaje při poskytování stanoviska vyloučit, je primárně na dotázaném povinném subjektu.

### **Náklady za mimořádně rozsáhlé vyhledání požadovaných informací nepodléhají dani z přidané hodnoty**

Úřad ve stížnostním řízení posuzoval postup povinného subjektu, který žadatele vyzval k úhradě nákladů spojených s mimořádně rozsáhlým vyhledáním informací. Povinný subjekt tyto náklady vyčísil podle sazebníku, podle něhož je k takto stanoveným nákladům třeba připočítat daň z přidané hodnoty.

Úřad si v rámci posuzování stížnosti vyžádal stanovisko Ministerstva financí, načež dospěl k závěru, že takto stanovená výše úhrady je neoprávněná, neboť náklady požadované po žadateli podle § 17 zákona č. 106/1999 Sb. nepodléhají dani z přidané hodnoty, jelikož nenaplnějí definici úplaty vymezenou v § 4 odst. 1 písm. a) zákona č. 235/2004 Sb., o dani z přidané hodnoty.

### **Soudní exekutor není povinným subjektem podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím**

Úřad se zabýval podnětem k přijetí opatření proti nečinnosti, která byla podatelem spatřována v tom, že domnělý nadřízený orgán nerozhodl o stížnosti na postup povinného subjektu při vyřizování žádosti o informace. Za povinný subjekt podatel označil soudního exekutora. Úřad tomuto podnětu nevyhověl, přičemž připomněl závěr, k němuž dospěl Nejvyšší správní soud v rozsudku ze dne 20. 3. 2019, č. j. Komp 2/2018-49, podle něhož soudní exekutor není povinným subjektem podle zákona č. 106/1999 Sb.

### **Určení nadřízeného orgánu příspěvkové organizace kraje – rozsudek Nejvyššího správního soudu ze dne 16. 2. 2022, č. j. Komp 3/2021-26**

Nejvyšší správní soud se zabýval otázkou určení nadřízeného orgánu příspěvkové organizace zřízené vyšším územním samosprávným celkem a aplikací § 20 odst. 5 zákona č. 106/1999 Sb., podle něhož, pokud není možné nadřízený orgán určit podle pravidel stanovených v § 178 správního řádu, plní funkci nadřízeného orgánu v odvolacím řízení a řízení o stížnosti Úřad.

Nejvyšší správní soud v tomto případě odkázal na aplikovatelnost závěrů, vyplývajících z jeho předchozích rozsudků, zejména z rozsudku č. j. Komp 2/2020-44, v němž zdůraznil, že § 178 odst. 1 správního řádu je třeba interpretovat s ohledem na působnost správního řádu podle § 1 odst. 1 a 3, podle nichž správní řád upravuje postup správních orgánů při výkonu působnosti v oblasti veřejné správy a nevztahuje se mimo jiné na právní jednání prováděná správními orgány ve sféře vrchnostenské.

Nejvyšší správní soud proto v rozsudku č. j. Komp 3/2021-26 určil, že k rozhodnutí o odvolání proti rozhodnutí příspěvkové organizace zřízené krajem, kterým byla odmítnuta žádost o informace podle zákona č. 106/1999 Sb., je příslušný Úřad, neboť taková příspěvková organizace nevykonává veřejnou správu autoritativními formami, na jejichž procesní realizaci by dopadal správní řád, a tedy není možné určit její nadřízený orgán podle § 178 správního řádu.

Úřad v návaznosti na uvedený rozsudek v praxi aplikuje závěr, že je nadřízeným orgánem takových povinných subjektů, které jsou příspěvkovými organizacemi krajů a které nevykonávají vrchnostenskou veřejnou správu, neboť u těchto příspěvkových organizací nelze určit nadřízený orgán dle ustanovení § 178 správního řádu. U příspěvkových organizací krajů, u nichž nadřízený orgán podle ustanovení § 178 správního řádu určit lze, postupuje nadále podle dosavadní judikatury.

## ● **ORGANIZAČNÍ ZAJIŠTĚNÍ ROZHODOVÁNÍ ÚŘADU V OBLASTI SVOBODNÉHO PŘÍSTUPU K INFORMACÍM**

Odbor práva na informace se v roce 2022 podobně jako v roce předchozím potýkal s potížemi způsobenými jeho nedostatečným personálním zajištěním. V odboru práva na informace je systemizováno devět míst státních zaměstnanců, z čehož pouze čtyři místa byla pro tuto agendu nově vytvořena za účelem výkonu působnosti v oblasti svobodného přístupu k informacím. Zbylých pět míst bylo bez náhrady vyčleněno z jiných útvarů Úřadu. Na služební místa v odboru práva na informace jsou sou-

časně kladeny vysoké odborné nároky, což je společně se značným pracovním vytížením jednotlivých zaměstnanců vyplývajícím z neustále narůstajícího nápadu vyřizovaných věcí důvodem nesnadného obsazování uvolněných míst.

Specifickým jevem, který přetrvával i v roce 2022, je procesní nástupnictví Úřadu v dříve zahájených soudních řízeních vedených o žalobách napadajících rozhodnutí jiných nadřízených orgánů. Prostřednictvím tohoto procesního nástupnictví se Úřad stává odpovědným za rozhodnutí vydaná před mnoha lety jinými subjektysubjekty, přičemž je nucen tato rozhodnutí aktivně hájit, ačkoliv související správní řízení nevedl a požadovanými informacemi v zásadě nedisponuje. Tato řízení se přitom týkají právně složitých otázek, trvají mnoho let a často generují povinnost hradit soudní náklady, které Úřad svou činností nezpůsobil.

Ve své činnosti se odbor práva na informace dále setkal s některými opakujícími se nedostatky v praxi povinných subjektů, které znesnadňují samotné rozhodování a prodlužují jednotlivá správní řízení. Za takový nedostatek je třeba považovat v první řadě vadné vedení spisů, které mnohdy nejsou řádně žurnalizovány a neobsahují všechny důležité dokumenty (především samotné informace, které jsou předmětem žádosti, ale též úřední záznamy, doručky či formální záznamy o skutkových zjištěních). Povinné subjekty rovněž opakovaně chybují při doručování písemností, a to jak prostřednictvím datové schránky (nevyznačení příznaku pro doručení do vlastních rukou žadatele), tak prostřednictvím elektronické pošty (absence kvalifikovaného potvrzení o doručení písemnosti).

Přestože Úřad prakticky nemá vliv na připravované změny zákona o svobodném přístupu k informacím, snaží se své právní názory na legislativu a další důležité otázky spojené se svobodným přístupem k informacím prezentovat alespoň jinými cestami, například účastí zástupců odboru práva na informace na workshopech, kulatých stolech či odborných seminářích. ●



## • Informační systém ORG

Na základě zákona č. 111/2009 Sb., o základních registrech, a jeho změně zákonem č. 100/2010 Sb., provozuje Úřad pro ochranu osobních údajů Informační systém ORG (IS ORG) jako součást systému základních registrů, která zajišťuje procesy spojené s identifikací fyzických osob a se zabezpečením jejich osobních údajů. IS ORG generuje a přiděluje následující neveřejné identifikátory:

- Zdrojové identifikátory fyzických osob (dále jen ZIFO),
- Agendové identifikátory fyzických osob (dále jen AIFO).

Aby nebylo možno mimo zákonný rámec spojovat údaje o občanovi vedené v různých agendách, zavádí zákon o základních registrech pro občana vícenásobnou digitální identitu – tzn., že v různých agendách je občan veden pod odlišným identifikátorem (AIFO). Vytváření a transformace AIFO je právě úkolem IS ORG (systém je také označován jako „převodník identifikátorů“).

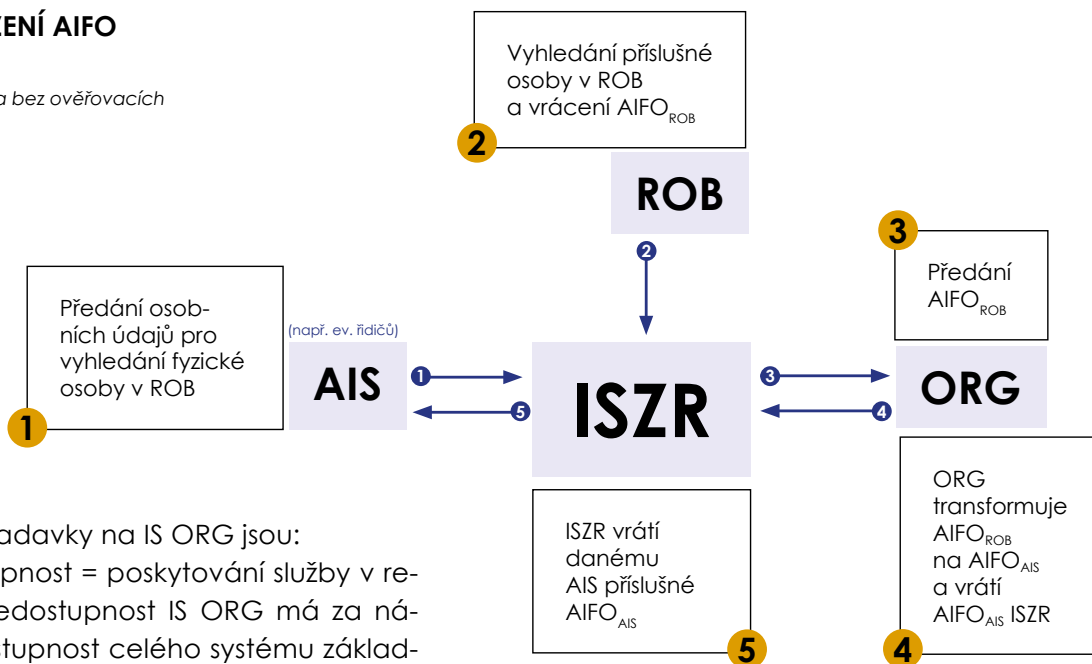
ZIFO je IS ORG vytvořen, jakmile je občan zapsán v informačních systémech evidence obyvatel nebo cizinců. Všechny AIFO občana jsou vytvářeny z jeho ZIFO a z AIFO nelze zpětně ZIFO odvodit. Všechny ZIFO a AIFO jsou uloženy v IS ORG. Jediným místem, které umí převést AIFO jedné agendy na AIFO agendy jiné, je IS ORG.

IS ORG komunikuje výhradně a pouze jen s Informačním systémem základních registrů (ISZR). Při každé komunikaci agendových informačních systémů s ISZR (a základními registry) dochází k ověřování oprávnění úředníka/uživatele na požadovanou operaci. Správcem a současně provozovatelem IS ORG je Úřad pro ochranu osobních údajů.

IS ORG má vysoký bezpečnostní potenciál, je uplatněním zákona na ochranu o zpracování osobních údajů v praxi. Je to základní komponenta systému základních registrů (ZR), řešící bezpečnost osobních dat ZR. IS ORG neuchovává a ani nezpracovává žádné osobní údaje. Je neveřejnou komponentou, která komunikuje pouze s ISZR.

## PRINCIP PŘIŘAZENÍ AIFO DANÉ AGENDĚ

*zjednodušené schéma bez ověřovacích a logovacích procesů*



Hlavními požadavky na IS ORG jsou:

- vysoká dostupnost = poskytování služby v režimu 24/7, nedostupnost IS ORG má za následek nedostupnost celého systému základních registrů,
- vysoká spolehlivost = informace budou unikátní a nenahraditelné,
- jednoznačnost = generátor identifikátorů,
- konzistence dat = identifikátory musí být konzistentní v řádu desítek let,
- dostatečná odezva = dotazy v řádu tisíců/sekundu.

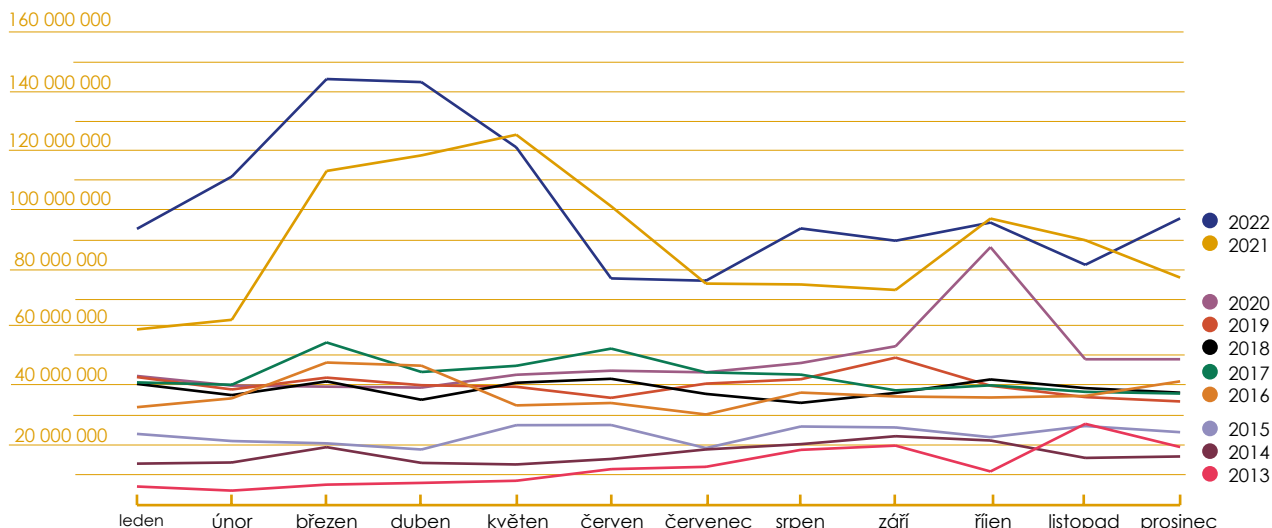
Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, byl ORG určen jako informační systém kritické infrastruktury a jako správce takového systému plní Úřad technická opatření stanovená ve vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitos-

tech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

V roce 2022 uběhlo 10 let od začátku fungování základních registrů a za tuto dobu fungování jejich význam i míra využívání velmi narostly. Jen počet provedených transakcí<sup>1</sup> v IS ORG vzrostl sedmínásobně. Za rok 2022 stoupl počet provedených transakcí o 14,73% oproti roku 2021. Zároveň opět stoupl i maximální měsíční počet transakcí, konkrétně o 14,92%. Spolu s tím roste i význam a provozní zatížení IS ORG. V roce 2022 bylo zaznamenáno vyšší využití základních registrů, a tím i IS ORG,

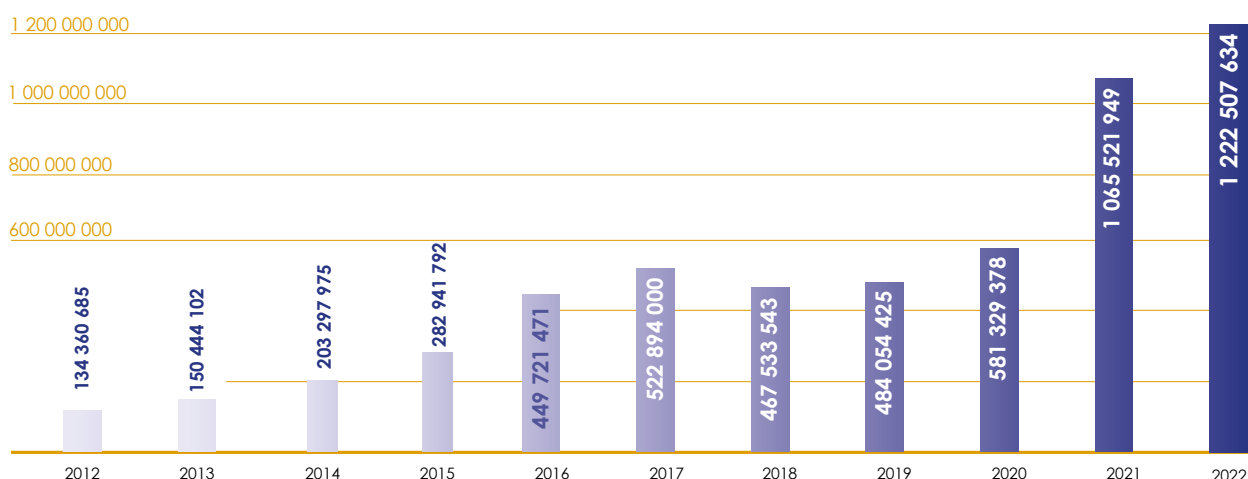
<sup>1</sup> Transakcí se rozumí operace provádění v IS ORG – založení ZIFO, generování AIFO, překlad AIFO pro jinou agendu a další.

## POČET TRANSAKČÍ V LETECH 2012–2022

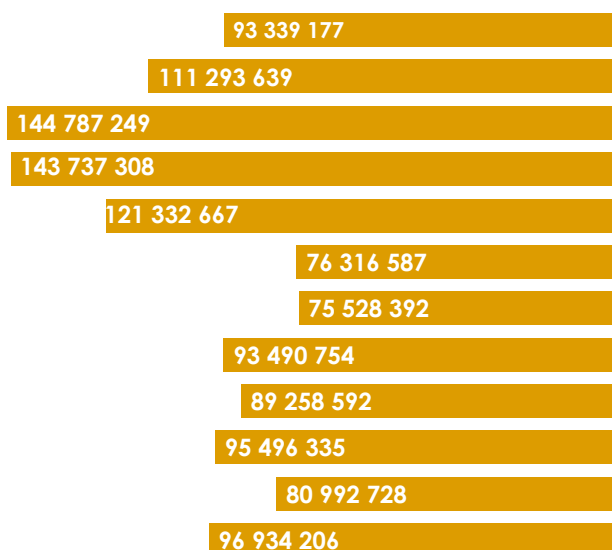




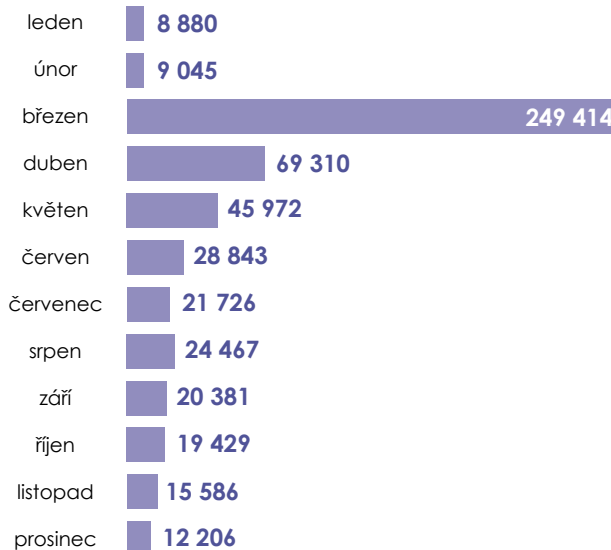
## CELKOVÝ POČET TRANSAKČÍ V LETECH 2012–2022



### MĚSÍČNÍ POČET TRANSAKČÍ V ROCE 2022



### POČET ZIFO V ROCE 2022



v měsících únor až květen v souvislosti s uprchlickou vlnou z Ukrajiny. Vyšší využití IS ORG (i základních registrů) lze pozorovat také v období voleb. V uplynulém roce to byly volby do místních zastupitelstev a části Senátu Parlamentu České republiky.

V roce 2022 proběhla další obnova HW, ježmuž skončila podpora od výrobce. IS ORG je v dobré kondici a v tuto chvíli mimo obnovy HW po konci podpory zvládá zvýšené nároky bez potíží s výkonem a výpadků.

V listopadu 2022 proběhl recertifikační audit IS ORG a systém byl úspěšně opětovně certifikován dle ČSN EN ISO/IEC 27001:2014 bez nálezů neshody. Kyberbezpečnost je pro provoz IS ORG absolutní prioritou. IS ORG v roce 2022 nezaznamenal větší bezpečnostní incident.

Pokračuje trend růstu využívání základních registrů, důvodem je mimo jiné také obecný rozvoj propojeného datového fondu. V roce 2023 čeká IS ORG tvorba nové strategie na roky 2024–2028, která se bude primárně orientovat na udržení dobré kondice systému, zejména s ohledem na obnovu HW s končící podporou, udržení kroku s moderními trendy v kyberbezpečnosti pro potřeby udržení certifikace ČSN EN ISO/IEC 27001:2014 a hlavně na nové úkoly spojené s dalším rozvojem základních registrů. V roce 2023 lze očekávat rovněž dynamický vývoj vzhledem k probíhajícím změnám ve správě základních registrů a vzniku Digitální a informační agentury, pod jejíž správou by měly být některé ze základních registrů převedeny. ●

## • O činnosti

### • **SPOLEČNÉ A KOORDINOVANÉ KONTROLY**

Úřad v roce 2022 navazoval těsnější spolupráci s úřady, které mohly s ohledem na zkušenosti v oblasti své působnosti přispět k efektivnějšímu provádění kontrol v oblasti ochrany osobních údajů.

V roce 2022 Úřad ve spolupráci s Českým úřadem zeměměřickým a katastrálním (ČÚZK) dokončil kontrolu společnosti, jejímž předmětem činnosti bylo mimo jiné poskytování osobních údajů o vlastních nemovitostech v České republice. Zapojení ČÚZK významně přispělo ke zmapování skutkového stavu věci, neboť tento úřad disponuje daty o vytěžování katastru nemovitostí. Na jejich základě bylo možné precizněji formulovat kontrolní závěry.

Spolupráce s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) v oblasti kontrol byla zahájena v září 2022. Společně byla provedena kontrola zpracování osobních údajů při využití cloudových služeb v rámci provozu Portálu veřejné správy, konkrétně jeho části Portál občana spravované Ministerstvem vnitra. V rámci této kontroly Úřad využil zkušeností NÚKIB v oblasti kybernetické bezpečnosti a kontrola spadala i do evropské koordinované kontrolní akce (k tomu dále níže).

Koncem roku 2022 pak byla také navázána spolupráce s Českým telekomunikačním úřadem o možnostech provedení společných či koordinovaných kontrol v oblastech společných úkolů.

Výhody provádění společných či koordinovaných kontrol zaměřených na ochranu osobních údajů jsou zjevné – v rámci takové spolupráce mohou být vhodně využity odborné zkušenosti zapojených partnerů, a to nejen v oblasti procesů, postupů, ale pro provádění kontrol obecně. Ochrana a zpracování osobních údajů je téma, které se týká všech odvětví, a to v konkrétních oblastech zpracování osobních údajů. Typickým příkladem je uvedená spolupráce s NÚKIB, jehož zkušenosti v rámci kybernetické bezpečnosti jsou mimořádně přínosné i pro činnosti prováděné Úřadem pro ochranu osobních údajů. Dokonce lze předpokládat, že s celkovým rozvojem digitalizace, všeobecné elektronizace



komunikace a rozšiřováním využití technologií umělé inteligence bude význam takové spolupráce významně umocněn. Působnost Úřadu v oblasti ochrany osobních údajů je velmi široká, a Úřad tak může dosáhnout svými dozorovými pravomocemi i na subjekty, které pro jiné úřady jsou mimo jejich působnost.

Jak bylo uvedeno výše, v roce 2022 probíhala napříč evropskými dozorovými úřady koordinovaná kontrolní akce (CEF 2022). Projekt byl iniciován Evropským sborem pro ochranu osobních údajů (EDPB) na základě Rámce pro koordinované prosazování předpisů podle obecného nařízení o ochraně osobních údajů. Ten EDPB přijal v rámci strategie na období let 2021–2023 s cílem zefektivnit postupy a vzájemnou spolupráci evropských dozorových úřadů.

Tematické zaměření koordinované akce vychází mimo jiné ze zjištění Eurostatu. Z něj vyplývá, že využívání cloudových služeb v EU se za posledních šest let zdvojnásobilo. K rozmachu digitalizace napříč soukromým i veřejným sektorem bezesporu přispěla i pandemická situace. Přejít na cloudové služby však klade vysoké nároky na ochranu osobních údajů, přičemž využívání nevhodných produktů či nespolehlivých služeb může vést k jejich ohrožení.

Společný postup evropských dozorových úřadů si tak kladl za cíl zmapovat situaci v jednotlivých členských státech a následně přijmout takové kroky, které zajistí dostatečnou ochranu osobních údajů zpracovávaných veřejným sektorem.

Na projektu se podílí celkem 22 dozorových úřadů, které by měly prověřit více než 75 veřejných institucí napříč Evropskou unií a Evropským hospodářským prostorem.

V první fázi společné akce byly formou dotazníkového šetření osloveny vybrané instituce, které pomohou zjistit aktuální stav využívání cloudových služeb ve světle obecného nařízení. Dotazníky například zkoumají, jak instituce zajišťují dostatečnou ochranu uložených dat či zda jsou adekvátně vymezeny a dodržovány povinnosti správce a zpracovatele.

Institucemi, které Úřad v rámci dotazníkového šetření oslovil, jsou Ministerstvo práce a sociálních věcí, Ministerstvo vnitra a Národní agentura pro komunikační a informační technologie.

Na základě získaných poznatků Úřad zahájil v září 2022 ve spolupráci s NÚKIB kontrolu Ministerstva vnitra, konkrétně Portálu občana jakožto transakční části Portálu veřejné správy.

Souhrnná zpráva o výsledku této koordinované záležitosti byla dokončena a předána EDPB na počátku roku 2023.

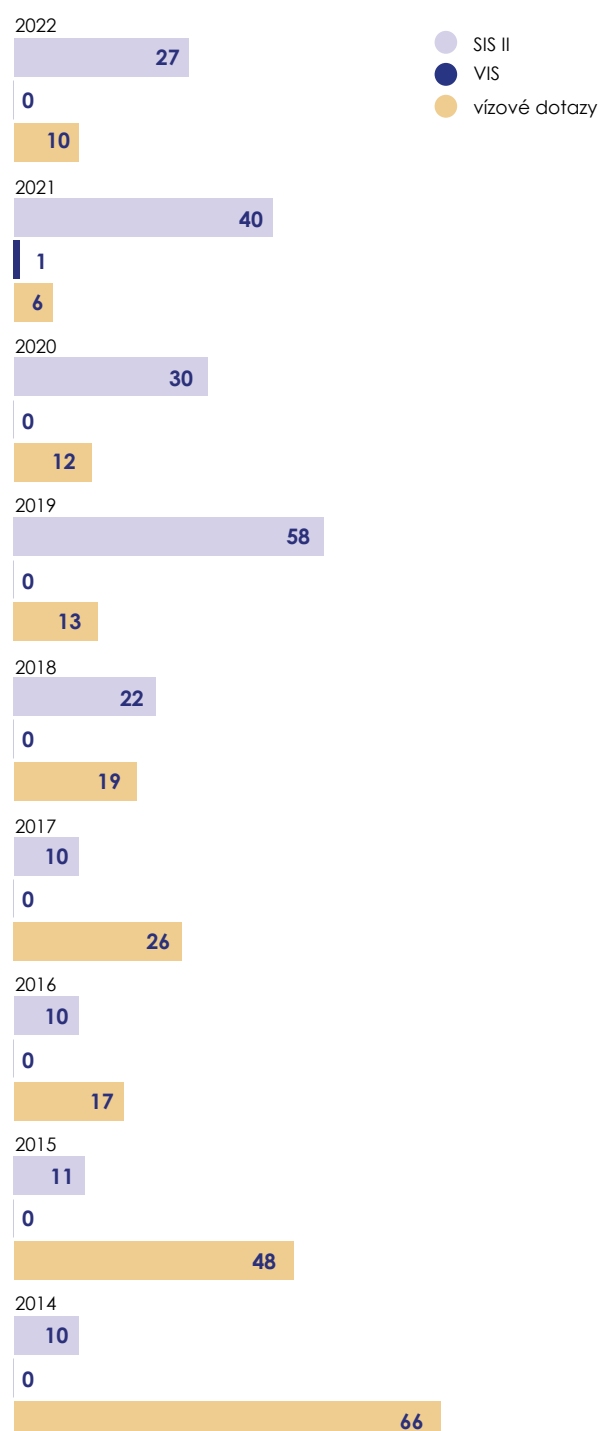
## ● SCHENGENSKÁ SPOLUPRÁCE

Stejně jako v předchozích letech i v roce 2022 Úřad plnil roli vnitrostátního dozorového orgánu, kterému přísluší dohled nad zpracováním osobních údajů v rozsáhlých evropských informačních systémech provozovaných v rámci schengenské spolupráce. V této roli Úřad dohlíží na dodržování příslušných právních předpisů a napomáhá k ochraně základních práv a svobod osob, jejichž údaje jsou v takových systémech zpracovávány. Konkrétně se jedná o Schengenský informační systém, Vízový informační systém, Celní informační systém a databázi otisků prstů Eurodac. Úřad je též příslušný k dohledu nad zpracováním osobních údajů národní jednotkou Europolu. U národní jednotky Europolu Úřad v roce 2022 realizoval v rámci kontroly místní šetření. Místní šetření byla realizována u Policie České republiky též v souvislosti se zahájenou kontrolou Schengenského informačního systému druhé generace (SIS II). Z hlediska zpracování osobních údajů ve Vízovém informačním systému (VIS), resp. zpracování osobních údajů při vízovém procesu, realizoval Úřad v roce 2022 místní šetření na velvyslanectví České republiky v zemi mimo EU včetně šetření ve vízovém centru externího poskytovatele služeb. V roce 2022 byla dále ukončena kontrola zpracování osobních údajů v databázi otisků prstů Eurodac. Kontrolovanou osobou bylo v tomto případě Ministerstvo vnitra, které v návaznosti na kontrolní zjištění postupně přijalo a dále přijímá opatření směřující k odstranění zjištěných nedostatků.

Při dozoru nad zpracováním osobních údajů v rámci schengenského prostoru spolupracuje Úřad s vnitrostátními orgány dozoru ostatních členských států a s Evropským inspektorem ochrany údajů (EDPS). Zástupci Úřadu se v prů-

běhu roku 2022 zúčastnili všech osmi jednání koordinačních skupin k výše uvedeným informačním systémům, resp. též dvou jednání výboru pro koordinovaný dozor, do jehož působnosti se agendy koordinačních skupin postupně přesouvají.

## POČET VYŘÍZENÝCH PODNĚTŮ OHLEDNĚ ZPRACOVÁNÍ ÚDAJŮ V SCHENGENSKÉM PROSTORU v letech 2014–2022



Úřad je ze své pozice dále příslušný též k vyřizování podnětů vztahujících se ke zpracování osobních údajů ve zmíněných informačních systémech. V roce 2022 Úřad obdržel a vyřídil celkem 27 podnětů týkajících se zpracování údajů v Schengenském informačním systému (stížnosti, žádosti o konzultaci či žádosti o přístup k osobním údajům, jejich opravu či výmaz). Z hlediska ostatních systémů nebyla žádná podání učiněna. Úřadu však bylo v roce 2022 doručeno 10 dotazů týkajících se vízové problematiky. Tyto dotazy byly, stejně jako v předchozích letech, Úřadu adresovány i přesto, že tato oblast není v jeho působnosti. Ve všech případech Úřad jednotlivým žadatelům objasnil své zákonné kompetence a poskytl relevantní informace a kontaktní údaje s cílem pomoci žadatelům s řešením jejich životní situace. Obsah některých podání týkajících se Schengenského informačního systému i obsah některých vízových dotazů bezprostředně souvisel s válečným konfliktem na Ukrajině. Žadatelé se na Úřad obraceli ve snaze získání víz, ověření možnosti vstupu do schengenského prostoru či přímo se žádostmi o výmaz ze Schengenského informačního systému, pokud jim byl vstup do schengenského prostoru odepřen. K tomu lze doplnit, že podněty a dotazy jsou Úřadu zasílány jak v českém jazyce, tak i např. v jazyce anglickém, ukrajinském či ruském, ve všech případech se však Úřad vždy snaží poskytnout žadatelům potřebné informace. Ty byly v roce 2022 poskytovány i osobám, které se se žádostí o radu na Úřad dostavily osobně.

## ● PORADENSTVÍ A KONZULTACE

Konzultanti Úřadu především v první polovině roku 2022 v souvislosti s novelou zákona č. 127/2005 Sb., o elektronických komunikacích, vyřizovali množství dotazů v oblasti cookies, jež se především týkaly cookie lišt. Dále Úřad obdržel, obdobně jako v přechodných letech, množství dotazů ke kamerovým systémům, dlužnickým registrům, manipulacím se zdravotnickou dokumentací. Významná část dotazů také směřovala mimo působnost Úřadu, primárně se jednalo o dotazy spadající do působnosti zákona





č. 89/2012 Sb., občanský zákoník, tedy oblasti, jež je v kompetenci soudu. Také se jednalo o dotazy směřující k výkladu zvláštních právních předpisů, k nimž je příslušný gestor dané právní úpravy (ministerstvo). V těchto případech byli tazatelé nasměrováni na kompetentní instituce.

V roce 2022 Úřad poskytoval osobní konzultace. Například s Ministerstvem organizátoři projektu Correny, jež je nástrojem na distribuci finanční podpory lokální ekonomiky. S Ministerstvem financí byla projednávána problematika regulatorního sandboxu ve finančnictví, jehož využívání předpokládá Národní plán obnovy. Sdružení pro internetový rozvoj byla poskytnuta konzultace ve věci cookie lišty. S oběma subjekty bylo rovněž v rámci uvedených témat komunikováno i písemnou formou. S Ministerstvem vnitra bylo projednáno využívání bezvýznamového směrového identifikátoru podle § 12a zákona č. 12/2020 Sb., o právu na digitální služby, který by měl nahradit rodné číslo. S pověřenkyní resortu obrany byla prodiskutována působnost zákona č. 110/2019 Sb., o zpracování osobních údajů, v tomto resortu.

Zástupci Úřadu se rovněž podíleli na aktualizaci metodiky Českého telekomunikačního úřadu „Jak se bránit nevyžádanému telemarketingu“ v kontextu citované novely zákona o elektronických komunikacích. Konzultanti Úřadu se dále zúčastnili konference ISSS 2022 v Hradci Králové zaměřené na reformu veřejné správy, rozvoj eGovernmentu a informatizaci společnosti a konference Ochrana osobních údajů v éře digitalizace v Praze.

Začátkem roku zástupci Úřadu na základě žádosti podle § 38 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, s Policií České republiky projednali zpracování osobních údajů v aplikaci Karanténa využívané v průběhu pandemie onemocnění COVID-19.

Stejně jako v předchozích letech ani v roce 2022 neobdržel Úřad žádost, která by splňovala požadavky na poskytnutí konzultace podle čl. 36 obecného nařízení. Několik správců se na Úřad obrátilo s žádostí o konzultaci k otázkám posuzování vlivu zpracování na ochranu osobních údajů, jež nevyústily v žádost podle čl. 36 obecného nařízení a byly zodpovězeny v rámci podpory povědomí správců a zpracovatelů o jejich

povinnostech podle čl. 57 odst. 1 písm. d) obecného nařízení.

Operativně byly poskytovány konzultace pověřencům pro ochranu osobních údajů jmenovaným správcem usazenými v České republice.

## ● **EVROPSKÁ A ZAHRANIČNÍ SPOLUPRÁCE** **Evropský sbor pro ochranu osobních údajů**

Evropský sbor pro ochranu osobních údajů (EDPB) představuje hlavní platformu pro mezinárodní činnost Úřadu v evropském rozměru. Členství v EDPB umožňuje Úřadu podílet se na tvorbě pracovních dokumentů (pokyny, doporučení, stanoviska, rozhodnutí), které především mají napomáhat kvalitnímu a pokud možno jednotnému uplatňování zásad obecného nařízení o ochraně osobních údajů.

Delegát Úřadu se účastnil všech patnácti plenárních zasedání EDPB, která se jedenáctkrát uskutečnila distanční formou a čtyřikrát s osobní účastí v Bruselu. Vedle pléna jakožto vrcholného orgánu Sboru vyvíjí činnost řada tematicky specializovaných odborných skupin a formací, přičemž svého zástupce má Úřad v osmi odborných skupinách (expert groups) a další zástupce má ve formacích zřízených ad hoc (taskforces) a zaměřených na výkon dozorové činnosti v úzce definované oblasti (např. využívání cloudových služeb ve veřejném sektoru). Celkem se zúčastnili více než 80% veškerých pracovních schůzí těchto skupin a formací. Nejen vzhledem k pandemické situaci, ale také s ohledem na úsporu finančních nákladů, silně převažovala distanční forma účasti.

Úřad se aktivně podílel ve dvou případech jako spolupracující hodnotitel předložených závazných podnikových pravidel pro správce, v pěti případech jako spolupracující zpravodaj ke stanovisku EDPB k závazným podnikovým pravidlům pro správce a jednou jako spolupracující hodnotitel předložených certifikačních kritérií. Jako spolupracující zpravodaj se Úřad podílí na vyhodnocení poznatků získaných při přípravě zprávy EDPB pro výbor LIBE Evropského parlamentu ohledně zdrojů disponibilních dozorovým úřadům a o jejich činnosti v oblasti prosazování práva. Cílem má být sladění struktury a obsahu statistických ukazatelů sledovaných

jednotlivými úřady. V postavení spolupracujícího zpravodaje pokračuje Úřad při vypořádání veřejné konzultace k Pokynům 01/2022 o právech subjektu údajů – právo na přístup.

Dozorová činnost v oblasti případů mezinárodního rozměru dlouhodobě přinášela poznatky a zkušenosti posilující názor, že by bylo účelné dále harmonizovat na úrovni EU některé procedurální aspekty, což by pomohlo překlenout některé rozdíly ve vnitrostátní procesní praxi jednotlivých dozorových úřadů, a zefektivnit tak jejich spolupráci v oblasti dozoru a vymáhání práva. Koncem dubna roku 2022 se ve Vídni sešli na vysoké úrovni zástupci úřadů, kde se mimo jiné dohodli na sestavení seznamu procedurálních aspektů, kterým by prospěla harmonizace Schengenu. Úřad do něho přispěl náměty, které vyhodnotil jako důležité a vhodné k harmonizaci, přičemž členové EDPB jeho podněty sdíleli. Seznam byl v říjnu tohoto roku zaslán Evropské komisi, která ho akceptovala jako vstupní položku do svého plánu práce pro rok 2023.

### **Mechanismus spolupráce**

Obecné nařízení upravuje různé mechanismy, v jejichž rámci Úřad může, resp. v některých případech je povinen, postupovat v souladu s ostatními evropskými dozorovými úřady a jinak s nimi spolupracovat. Nejčastější formu této spolupráce představuje žádost podle čl. 61 GDPR. Může se jednat o případy výměny informací ke konkrétním případům a stížnostem, případně o dotazy legislativního a výkladového charakteru. Těchto žádostí Úřad v uplynulém roce 2022 obdržel celkem 198. Sám odeslal 7 žádostí.

Dalším často užívaným postupem je tzv. mechanismus jediného kontaktního místa (one-stop-shop). Využívá se v případech přeshraničního zpracování osobních údajů, tj. takového zpracování, které probíhá buď v souvislosti s činnostmi provozovanými správce či zpracovatele ve více než jednom členském státě, anebo zpracováním dochází či pravděpodobně dojde k podstatnému dotčení práv a svobod subjektů údajů ve více než jednom členském státě. V takovém případě je nejprve v souladu s čl. 56 GDPR určen vedoucí dozorový úřad, který se stává jediným kontaktním místem. Ten poté fakticky vede vyšetřování, v jehož rámci provádí další procesní kroky vůči správci či zapracov

vateli, a postupuje spolu s dotčenými dozorovými úřady podle čl. 60 GDPR.

Úřad na základě obdržení podnětů inicioval celkem 3 procedury podle čl. 56 GDPR, kdy navrhl příslušnost některého ze zahraničních dozorových úřadů, aby se věcí zabýval z pozice vedoucího dozorového úřadu. Naopak do této role byl navržen celkem ve 34 případech, přičemž doposud přijal 13 z nich. Ve zbývajících případech nebylo o vedoucím dozorovém úřadu zatím rozhodnuto nebo role vedoucího dozorového úřadu nebyla přijata.

### **Oblast předávání osobních údajů do třetích zemí a mezinárodním organizacím**

Úřad se aktivně účastní řešení problematiky předávání osobních údajů do třetích zemí v EDPB, a to především v rámci expertní podskupiny pro mezinárodní předávání (International Transfers Subgroup, ITS). Tato podskupina pracuje průběžně prostřednictvím elektronické komunikace, přičemž cca jednou měsíčně řeší aktuální problémy v rámci videokonferenčních schůzí.

V rámci podskupiny EDPB pro mezinárodní předávání se Úřad zapojoval jako spoluhodnotitel do hodnocení jednotlivých návrhů závazných podnikových pravidel vypracovaných konkrétními skupinami podniků.

Úřad vykonával v režimu obecného nařízení roli spoluhodnotitele (co-reviewer) již v celé řadě případů, a získal tak v této oblasti řadu zkušeností, které využívá při hodnocení předkládaných BCR a zasílání konstruktivních připomínek hlavnímu hodnotiteli (vedoucímu dozorovému úřadu).

Pro vyjasnění konkrétních nejasností jednotlivých návrhů se cca jednou měsíčně konají specializované videoschůze podskupiny, kterých se zástupce Úřadu pravidelně účastní. Hodnocení, komentáře a doporučení podskupiny mají zajistit, aby do procedury podle čl. 64 odst. 1 písm. f) obecného nařízení byly přijímány pouze již dobře propracované návrhy.

Kromě role spoluhodnotitele vystupoval Úřad rovněž v roli spoluzpravodaje, formulujícího text Stanovisek Sboru, a to v těchto případech:

- [Stanovisko 4/2022 k návrhu rozhodnutí dánského úřadu o BCR-C skupiny Norican](#),



- [Stanovisko 5/2022 k návrhu rozhodnutí dánskému úřadu o BCR-C skupiny Lundbeck,](#)
- [Stanovisko 7/2022 k návrhu rozhodnutí maďarského úřadu o BCR-C skupiny MOL,](#)
- [Stanovisko 17/2022 k návrhu rozhodnutí španělského úřadu o BCR-C skupiny Antolín,](#)
- [Stanovisko 26/2022 k návrhu rozhodnutí bavorského úřadu pro privátní sektor o BCR-C skupiny Munich Re.](#)

## Oblast osvědčení o ochraně osobních údajů (certifikační mechanismy)

Na základě výzvy pracovní skupiny (CEH) Sboru přijal Úřad (spolu s dozorovým úřadem SRN) funkci (spolu)hodnotitele návrhu národních rakouských certifikačních kritérií, a to vzhledem k tomu, že národní certifikační kritéria podléhají projednání a vydání stanoviska Evropského Sboru pro ochranu údajů (podle článku 63 obecného nařízení o ochraně osobních údajů). Materiál Úřad obdržel dne 31. 8. 2022 a návrhy a připomínky Úřadu byly 4. 10. 2022 postoupeny přímo předkladateli kritérií k zapracování a předložení nové verze.

Zaslaná kritéria byla obecného charakteru (nešlo o kritéria na vybrané operace zpracování nebo operace zpracování v nějakém odvětví). Kritéria by tedy měla pokrýt všechna zpracování osobních údajů, resp. všechny operace zpracování. Z toho plynuly některé návrhy a připomínky Úřadu (např. v některých částech jsou kritéria příliš obecná, přepisují požadavky dané obecným nařízením a nepřináší tak nic nad rámec povinností uložených obecným nařízením; výsledkem je, že někdy chybí dostatečně konkrétní požadavky, aby bylo možno odpovědně provést certifikaci, resp. dávají certifikačnímu orgánu nadměrnou volnost při hodnocení).

## Oblast Kodexů chování

Počátkem roku 2022 pokračovalo jednání s Bankovní asociací, která již v roce 2019 zpracovala soft standard „Rámcový výklad některých ustanovení GDPR v bankovním sektoru“ a v roce 2021 aktualizovala původní verzi, ke které se Úřad vyjadřoval.

Úřad zahájil debatu s Asociací direct marketingu, e-commerce a zásilkového obchodu, z.s. (ADMEZ), která vyjádřila úmysl vytvořit kodex chování podle čl. 40 obecného nařízení pro ob-

last přímého elektronického marketingu a požádala Úřad o konzultaci. Schvalování kodexu chování ze strany Úřadu má dvě fáze. V první fázi se jedná o kontrolu náležitostí kodexu podle kritérií uvedených v dodatku 3 pokynů 1/2019 a až následně, ve druhé fázi, je posuzována věcná stránka. Jelikož Úřad zatím neschvaluje kodexy chování, zůstává debata nad podobou kodexu na úrovni konzultační.

## Světové shromáždění pro ochranu soukromí (GPA)

Je-li EDPB hlavní platformou pro spolupráci úřadů v evropském měřítku, pak v globální rovině takovou činnost podporuje Global Privacy Assembly (Světové shromáždění pro ochranu soukromí). Úřad je členem tohoto uskupení, které sdružuje přibližně 130 členských úřadů z celého světa. Další úřady a mezinárodní instituce mají status pozorovatele. V říjnu tohoto roku se zástupci Úřadu distančně zúčastnili výroční konference GPA, která se pod titulem „Věc rovnováhy: soukromí v době rychlého technologického pokroku“ konala v tureckém Istanbulu. Delegáti během závěrečné části konference schválili tři rezoluce:

1. Usnesení upravující cestovní mapu konference do budoucna a časovou osu,
2. Usnesení o mezinárodní spolupráci při budování kapacit k vylepšení nařízení o kybernetické bezpečnosti a chápání škod z kybernetických incidentů,
3. Usnesení o zásadách a očekáváních v souvislosti s přiměřeným využitím osobních informací v oblasti technologií pro rozpoznávání obličejů.

## Rada Evropy

Delegát Úřadu se ve Štrasburku zúčastnil listopadového plenárního zasedání T-PD, tedy Konzultačního výboru pro Úmluvu o ochraně osobních dat (Úmluva 108). Výbor mimo jiné schválil a publikoval Vodítka pro národní digitální identitu, která z perspektivy zásad ochrany osobních údajů podle Úmluvy 108 nabízejí řadu doporučení pro strany podílející se na tvorbě schémat národní digitální identity (zákonodárci, správci dat, výrobci, vývojáři a poskytovatelé služeb) a rovněž návrhy, jak příslušné dozorné úřady mohou být začleněny do celého

procesu od vývoje až po dohled nad uplatňováním zásad ochrany osobních údajů.

## Jarní konference

V květnu v chorvatském Cavtatu proběhla 30. konference úřadů pro ochranu dat za přítomnosti dvou delegátů Úřadu. Tato tzv. jarní konference přivedla dohromady delegáty ze čtyřiceti zemí. Byla přijata dvě usnesení. V prvním z nich delegáti vyzývají k urychlenému podpisu a ratifikaci Úmluvy 108+ Rady Evropy, tedy Úmluvy 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, modernizované dodatkovým protokolem v květnu 2018. Připomínají, že v oblasti ochrany osobních údajů je tato úmluva jediným právně závazným nástrojem na mezinárodní úrovni. Druhý přijatý dokument, Usnesení o vizi a poslání konference, se zaměřuje na další směřování konference a plnění dohodnutých priorit.

Na okraji konference proběhl workshop k závazným podnikovým pravidlům (BCR), kde za účasti pracovníka Úřadu, specializujícího se na mezinárodní předávání dat, účastníci diskutovali o novelizaci doporučení EDPB pro žadatele o schválení závazných podnikových pravidel. Novelizovaný dokument s názvem [Doporučení 1/2022 k žádosti o schválení a k prvkům a zásadám, které musí být součástí závazných podnikových pravidel pro správce](#) (Článek 47 GDPR), byl uveřejněn na webových stránkách EDPB v listopadu 2022 v rámci veřejné konzultace.

## ● POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

Úřad jako povinný subjekt poskytoval i v roce 2022 údaje o své činnosti v rozsahu, který ukládá orgánům veřejné moci zákon č. 106/1999 Sb., o svobodném přístupu k informacím. Základní informace podle zákona o svobodném přístupu k informacím zpřístupňuje Úřad několika způsoby: na svých webových stránkách na adrese [www.uoou.cz](http://www.uoou.cz) a na úřední desce umístěné v sídle na adrese Pplk. Sochora 27, 170 00 Praha 7.

Níže uvedené informace se vztahují k postavení Úřadu jako povinného subjektu a jsou zveřejňovány ve smyslu § 18 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.<sup>1</sup>

Úřad za rok 2022 eviduje 100 písemných žádostí podaných podle zákona o svobodném přístupu k informacím, což představuje obdobné číslo jako v roce 2021. Obecně je však nutno podotknout, že celkový počet žádostí o poskytnutí informace přímo nekorresponduje s počtem informací skutečně poskytnutých, neboť téměř každá žádost o poskytnutí informace byla více-položková, jednalo se tedy o společnou žádost o poskytnutí informace pro několik souvisejících, ale častěji nesouvisejících dotazů. Nejčastěji tak bylo požadováno v jedné žádosti poskytnutí značného množství různorodých informací, vzájemně nesouvisejících, případně většího množství rozhodnutí Úřadu, jež byly v žádosti o poskytnutí informace vymezeny buď typem řízení, nebo předmětem řízení za určité období.

Žadatelé tradičně pocházeli nejen z řad laické veřejnosti, ale i veřejnosti odborné, kdy lze v roce 2022 vysledovat nárůst žádostí o poskytnutí informace od osob vykonávajících právnické povolání. Předmětem žádostí o poskytnutí informace byla jak činnost Úřadu coby dozorového úřadu, jak již bylo uvedeno výše, ve formě jednotlivých rozhodnutí, případně dalších dokumentů z kontrolních a správních spisů, včetně informací o počtech řízení či výši sankce, případně činnosti svěřené Úřadu zákonem o svobodném přístupu k informacím, zejména § 16b a § 20 odst. 5, tak současně i další informace o fungování Úřadu.

Konkrétně z obsahového hlediska měli žadatelé obdobně jako v minulých letech největší zájem o informace o probíhajících správních řízeních, kde se převážná část žádostí o poskytnutí informace týkala výstupů ve formě rozhodnutí z přestupkových řízení zahájených pro porušení ustanovení obecného nařízení, případně vydaných na základě § 16b zákona o svobodném přístupu k informacím (přezkumná řízení, opatření proti nečinnosti) či kontrolních protokolů z Úřadem provedených kontrol. Ve vztahu

<sup>1</sup> Zde není zohledněno specifické postavení Úřadu podle zákona č. 111/2019 Sb., tedy ustanovení § 16b a § 20 zákona o svobodném přístupu k informacím.



k dozorové činnosti žadatele nejčastěji zajímaly obecné a statistické údaje o počtu provedených kontrol či správních řízení za různá časová období nebo informace o počtu dosud uložených pokut za porušení GDPR nebo o jejich výši. Část žádostí o poskytnutí informace se týkala personálního obsazení Úřadu, vnitřního uspořádání a interních předpisů Úřadu, případně dokumentů vypovídajících o hospodaření Úřadu. Poskytnuté informace byly standardně zpřístupňovány způsobem umožňujícím dálkový přístup podle [§ 5 odst. 3 zákona o svobodném přístupu k informacím na webových stránkách Úřadu](#).

Naprostou většinu požadovaných informací poskytl Úřad v roce 2022 bezplatně. Avšak i Úřad na svých webových stránkách v souladu se zákonem o svobodném přístupu k informacím zveřejňuje sazebník úhrad za poskytování informací – směrnici č. 8/2018 – respektující možnosti poskytované zákonem o svobodném přístupu k informacím. V roce 2022 došlo k vyměření úhrady za mimořádně rozsáhlé vyhledání informací ve čtyřech případech. Výše stanovených úhrad činila celkem 12 978 Kč. Jeden ze žadatelů obdržel dvě oznámení o výši požadované náhrady za mimořádně rozsáhlé vyhledání, na jejichž podkladě žádost o poskytnutí informace upravil tak, že Úřad na základě upravené žádosti o poskytnutí informace poskytl informaci bezplatně. Tato situace se opakovala u totožného žadatele v případě jiné žádosti, kdy Úřad po změně žádosti o poskytnutí informace poskytl informaci bezplatně, v tomto případě však žadateli bylo zasláno pouze jedno oznámení o výši požadované náhrady za mimořádně rozsáhlé vyhledání. Další ze žadatelů, kterému bylo zasláno oznámení o výši požadované náhrady za mimořádně rozsáhlé vyhledání, úhradu nákladů ve lhůtě stanovené zákonem o svobodném přístupu k informacím neprovedl, proto byla žádost o poskytnutí informace odložena.

O části žádostí o poskytnutí informace, kterým Úřad nevyhověl, a současně se nejednalo o situaci, kdy žádost o poskytnutí informace pouze odložil, neboť se nevztahovala k jeho působnosti (takových bylo v roce 2022 pět), případně, kdy žadatel na výzvu k do-

plnění žádosti o poskytnutí informace podle § 14 odst. 5 písm. a) zákona o svobodném přístupu k informacím nedoplnil požadované údaje (taková byla v roce 2022 jedna), byl povinen vydat správní rozhodnutí o odmítnutí žádosti o poskytnutí informace, případně její části. Podle organizačního řádu vydává rozhodnutí v prvním stupni ředitel odboru legislativy a metodiky. O rozkladu proti prvostupňovému rozhodnutí Úřadu rozhoduje předseda Úřadu.

V roce 2022 bylo vydáno 18 rozhodnutí o odmítnutí žádosti o poskytnutí informace, případně její části. Převažujícím důvodem, pro který byly žádosti o poskytnutí informace zcela či alespoň částečně odmítány, byla zákonná výluka dle § 2 odst. 4 zákona o svobodném přístupu k informacím, kdy se žadatelé domáhali právních rad či návodů, jak se domoci svých práv, výkladu právních předpisů, „dovysvětlení“ konkrétních rozhodnutí Úřadu anebo jejich analýzy. Takové požadavky bylo nutno v souladu s platnou právní úpravou vyhodnotit jako dotazy na názor, budoucí rozhodnutí, vytváření nových informací či jako informaci neexistující, které podle § 2 odst. 4 a § 3 odst. 3 zákona o svobodném přístupu k informacím informační povinnosti nepodléhají. Avšak ani v případech, kdy požadované informace spadají pod zákonné výluky z práva na informace, nepostupoval Úřad zcela mechanicky a žádosti o poskytnutí informace z těchto důvodů bez dalšího neodmítal, a to zejména v případech, kdy se jedná o obecné dotazy spadající do působnosti obecného nařízení nebo zákona č. 110/2019 Sb., o zpracování osobních údajů. V těchto případech příslušný útvar Úřadu postoupil příslušnou žádost o poskytnutí informace oddělení konzultací, které požadovanou informaci poskytlo.

Proti rozhodnutí povinného subjektu o odmítnutí žádosti o poskytnutí informace byly v roce 2022 podány pouze dva rozklady. V obou případech předseda Úřadu jako nadřízený orgán rozklad svým rozhodnutím zamítl a napadené rozhodnutí potvrdil.

V roce 2022 nebyly Úřadem poskytnuty žádné výhradní licence.

V roce 2022 obdržel Úřad pět stížností dle § 16a zákona o svobodném přístupu k informacím. Důvodem pro podání první a druhé stíž-

nosti bylo tvrzení žadatele, že mu byla úmyslně poskytnuta nepravdivá informace. Obě podání byla shledána nedůvodnými. Důvodem pro podání další stížnosti byla skutečnost, že informace byla poskytnuta pouze částečně, aniž by o zbytku žádosti o poskytnutí informace bylo vydáno rozhodnutí o odmítnutí části žádosti. Tato stížnost byla povinným subjektem vyřízena ve smyslu § 16a odst. 6 in fine zákona o svobodném přístupu k informacím, kdy povinný subjekt beze zbytku stížnosti vyhověl a vydal rozhodnutí o odmítnutí části žádosti o poskytnutí informace. Důvodem pro podání další stížnosti byla skutečnost, že informace byla poskytnuta pouze částečně, aniž by o zbytku žádosti o poskytnutí informace bylo vydáno rozhodnutí o odmítnutí části žádosti o poskytnutí informace. Povinný subjekt stížnosti částečně vyhověl a část žádosti o poskytnutí informace vyřídil podle § 16a odst. 6 in fine zákona o svobodném přístupu k informacím ve zbylé části stížnost postoupil nadřízenému orgánu, který přikázal povinnému subjektu poskytnout konkrétní a úplné informace. V posledním případě se jednalo o stížnost předčasně podanou a Úřad poskytl informaci v zákonné lhůtě.

V roce 2022 neevduje Úřad v případech, kdy byl povinným subjektem, podání žádné žaloby ve věci přezkoumání zákonnosti rozhodnutí povinného subjektu o odmítnutí žádosti o poskytnutí informace.

## KOMUNIKACE S MÉDIÍ

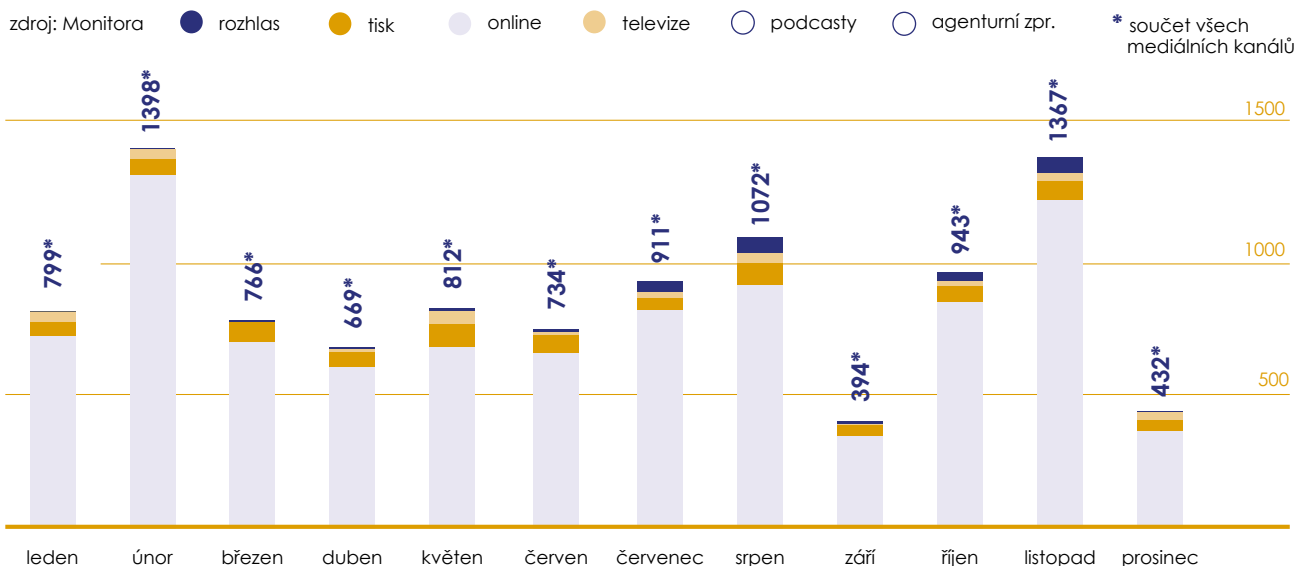
Mediální komunikace Úřadu se v průběhu celého roku 2022 ještě nesla v dozvucích uplynulé dvouleté epidemie onemocnění COVID-19.

V únoru Úřad oznámil, že prošetří, zda hnutí Chcíp! PES neporušilo obecné nařízení o ochraně osobních údajů při nakládání s osobními údaji, když na sociální síti publikovalo adresy trvalých pobytů poslanců, kteří hlasovali pro přijetí tzv. pandemického zákona. Toto téma pak bylo následně i častým a opakovaným předmětem novinářského zájmu. Podobně silný mediální ohlas přineslo šetření nakládání s osobními údaji občanů v rámci aplikace Karanténa, kde byla v prvostupňovém rozhodnutí Úřadu uložena pokuta téměř milion korun (975 000 Kč). Mediální zájem se soustředil především na výsledky kontroly Policie ČR a předávání strukturovaných dat o osobách, kterým byla nařízena karanténa, k využití Policii ČR.

V rámci komunikační podpory bylo aktivně komunikováno i téma novelizované právní úpravy o elektronických komunikacích, a to především s ohledem na problematiku nevyžádaných obchodních sdělení, změnu v udělení souhlasu z mechanismu opt-out na opt-in a relevantní nastavení sběru marketingových a technických dat o návštěvnících webových portálů, tzv. cookie lišt.

### MEDIÁLNÍ DOPAD (GRP) PRO TÉMA OCHRANY OSOBNÍCH ÚDAJŮ

období 1. 1. 2022–31. 12. 2022





Mezi tématy, která zaznamenala širší mezinárodní mediální zájem, šlo především o předávání osobních údajů občanů EU do třetích zemí v rámci EU – US Data Privacy Framework, podobně jako využívání cloudových a serverových datových operátorů mimo území EU (zejména společností *Microsoft*, *Google*, *TikTok* a *META Irsko*).

Z hlediska měřitelného mediálního zásahu s tématem ochrany osobních údajů hrálo pro komunikaci Úřadu v roce 2022 naprosto dominantní roli online prostředí. Printová a další elektronická média v komunikaci Úřadu sehrála sice nezastupitelnou úlohu, ale v násobně nižší míře mediálního dopadu (viz Graf Mediální dopad GRP).

V rámci komunikační podpory povědomí o ochraně osobních údajů se mimo jiné Úřad pro ochranu osobních údajů aktivně zapojil do soutěže v kybernetické bezpečnosti „*Cyber Security Competition*“, které se účastní 5 000 žáků a studentů z celé České republiky. Kromě toho proběhla i celá řada dalších aktivit, kterým poskytl svou záštitu předseda Úřadu. Z těch nejvýznamnějších lze jmenovat slavnostní vyhlášení *Pověřence roku*, konferenci *GDPR 2022*, *Information Security Summit – IS2* a konferenci *Ochrana osobních údajů v době digitalizace*.

K významným projektům zaměřeným na komunikační podporu činnosti Úřadu patří i aktualizace a úprava grafických dat. Základním parametrem pro zpracování byla taková úprava, která zachová základní myšlenkový charakter logotypu Úřadu pro ochranu osobních údajů, ale zároveň poskytne i odpovídající prostor pro jeho nasazení ve všech marketingových a komunikačních platformách včetně potenciálu případné animace. Po dokončení úpravy grafických dat logotypu tento Úřad zavádí a implementuje postupně, a to především s ohledem na omezené rozpočtové prostředky. Zároveň Úřad k logotypu požádal o registraci ochranné známky u Úřadu průmyslového vlastnictví České republiky.

## ● VYŘIZOVÁNÍ STÍŽNOSTÍ PODLE § 175 SPRÁVNÍHO ŘÁDU

Správní řád umožňuje těm, kteří nejsou spokojeni s výstupy správních orgánů, včetně Úřadu pro ochranu osobních údajů, podat stížnost podle § 175 zákona č. 500/2004 Sb., správního řádu. Konkrétně se mohou dotčené osoby obracet na správní orgány se stížnostmi proti nevhodnému chování úředních osob nebo proti postupu správního orgánu. Takovou možnost mají stěžovatelé v případě, neposkytuje-li jim správní řád jiné prostředky ochrany, tj. zejména odvolání nebo další řádné či mimořádné opravné prostředky.

Úřad v roce 2022 obdržel celkem 50 nových podání podle § 175 správního řádu, a to 43 stížností a 7 žádostí o přešetření vyřízení stížnosti. V polovině případů byli stěžovatelé nespokojeni s vyřízením svého 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 třetinou se na celkovém počtu podílely stížnosti směřující do relativně nové agendy svobodného přístupu k informacím. Za pozornost stojí, že podatelem plné čtvrtiny podání z celkového nápadu věcí podle § 175 správního řádu byl jeden konkrétní stěžovatel.

Ve stejném období Úřad vyřídil celkem 43 podání podle § 175 správního řádu, a to 36 stížností a 7 žádostí o přešetření vyřízení stížnosti. Z tohoto počtu bylo 9 stížností vyhodnoceno jako důvodných nebo částečně důvodných a 27 nedůvodných. Dále 1 žádost o přešetření vyřízení stížnosti byla vyhodnocena jako důvodná, 6 nedůvodných. Typickým opatřením v případě důvodné stížnosti je podle povahy věci v takových případech následné nové posouzení původního podnětu a uplatnění dozorových postupů. Zbývajícími 9 stížnostmi a 1 žádostí o přešetření z roku 2022 se bude Úřad zabývat v roce 2023. Ve 2 případech směřovaly podněty, které Úřad obdržel od stěžovatelů, proti údajnému nevhodnému chování úředních osob, ve zbytku proti jejich postupu. ●

## • Fungování Úřadu

### • PERSONÁLNÍ OBSAZENÍ ÚŘADU

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

K 1. 1. 2022 byl celkový počet systemizovaných služebních a pracovních míst v Úřadu 113, přičemž k 31. 12. 2022 se tento počet systemizovaných míst nezměnil, a byl tak rovněž 113.

I v roce 2022 plynule pokračoval chod jednotlivých procesů personální správy Úřadu, a to v návaznosti na vývoj legislativy v oblasti státní služby a pracovněprávních vztahů.

V rámci Úřadem zajišťované zvláštní části úřednické zkoušky pro obor služby „Ochrana osobních údajů“ absolvovalo tuto zkoušku celkem 17 žadatelů, přičemž 16 žadatelů složilo zkoušku úspěšně v prvním řádném termínu, jeden žadatel složil zkoušku úspěšně v opravném termínu na druhý pokus.

K 1. lednu 2022 bylo v Úřadu v evidenčním stavu 105 zaměstnanců, k 31. prosinci 2022 byl pak jejich počet 108.

Průměrný evidenční přepočtený počet zaměstnanců za rok 2022 činil 105,25.

Celkem 44 osob vykonávalo v Úřadu činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr. Z tohoto celkové počtu 20 externích spolupracovníků vykonávalo činnosti spojené s rozhodováním rozkladové komise a zbylý počet s Úřadem spolupracoval zejména v oblasti expertních prací ve vztahu k informačním a komunikačním technologiím nebo administrativní výpomoci.

Z grafu „Členění zaměstnanců Úřadu podle věku a pohlaví“ vyplývá, že v Úřadu pracují převážně zaměstnanci ve věku 31-40 let a 51-60 let. Seniorní zaměstnanci mají kromě odpovídajícího vzdělání i dlouhodobou praxi a velké zkušenosti. Řada z nich působí v Úřadu dlouhou dobu a svoje zkušenosti předávají novým zaměstnancům, kteří jsou přijímáni na uvolněná funkční místa. Předpoklad vysokoškolského vzdělání je stanoven u dvou třetin funkčních míst v Úřadu, na zbývající třetinu je předpokládáno dosažení úplného středního vzdělání.

Úřad umožňuje a zabezpečuje odborný rozvoj svých zaměstnanců. Zajišťuje jim prohlubování odborné kvalifikace a v případě potřeby





i její zvýšení. Studentům vysokých škol Úřad poskytuje možnost absolvovat odbornou praxi. Tímto způsobem podporuje jejich zájem o problematiku ochrany osobních údajů, a zároveň tak vyhledává nové potenciální zaměstnance.

## POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ ÚŘADU

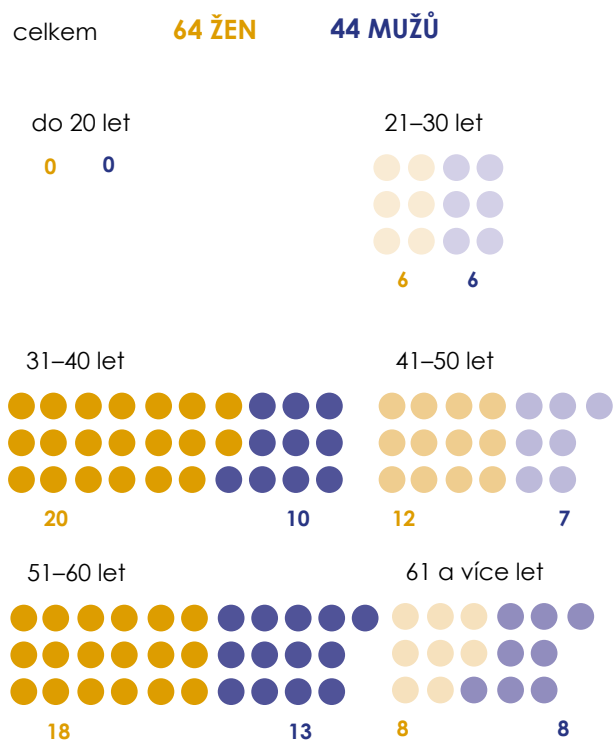
Úřad jako orgán veřejné moci má v souladu s čl. 37 obecného nařízení jmenovaného pověřence pro ochranu osobních údajů, jehož hlavní úkoly vyplývají z čl. 39 obecného nařízení.

V roce 2022 v činnosti pověřence převažovala konzultační činnost uvnitř Úřadu spojená především s problematikou uživatelských oprávnění a přístupu k dokumentům. Ve vztahu k veřejnosti se pak jednalo o zodpovídání dotazů k pojmům ochrany osobních údajů a vyřizování žádostí subjektů údajů souvisejících s realizací jejich práv vyplývajících z čl. 13–21 obecného nařízení.

Pověřenec Úřadu je také členem neformální sítě pověřenců Evropského sboru pro ochranu osobních údajů, v jejímž rámci se podílí na dokumentech souvisejících s právním posouzením zpracování.

### ČLENĚNÍ ZAMĚSTNANCŮ ÚŘADU PODLE VĚKU A POHLAVÍ

stav k 31. prosinci 2022



### ČLENĚNÍ ZAMĚSTNANCŮ ÚŘADU PODLE VZDĚLÁNÍ A POHLAVÍ

stav k 31. prosinci 2022

Celý soubor	Muži	Ženy	Celkem
Základní	0	0	0
Sřední odborné +VL	1	0	1
Sřední odborné	0	0	0
Úplné střední všeobecné	1	5	6
Úplné střední odborné + VL	1	2	3
Úplné střední odborné	3	14	17
Vyšší odborné vzdělání	0	0	0
Bakalářské	0	2	2
Vysokoškolské	38	41	79
<b>Celkem</b>	<b>44</b>	<b>64</b>	<b>108</b>

## ● HOSPODAŘENÍ ÚŘADU

Odbor provozně ekonomický zodpovídá za financování chodu Úřadu, a to jak o jeho způsob, tak i o jeho výši. Z tohoto pohledu jsou zásadní přehledy čerpání rozpočtu, potažmo investiční akce realizované v roce 2022.

Rozpočet Úřadu byl pro rok 2022 schválen ve výši 160 431 506 Kč.

Rozpočet Úřadu byl schválen zákonem č. 57/2022 Sb., o státním rozpočtu České republiky na rok 2022, ve znění zákona č. 344/2022 Sb.

### Příjmy

Příjmy pro rok 2022 byly schváleným rozpočtem stanoveny ve výši 1 000,00 tisíc Kč.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částkou 1 388,18 tisíc Kč.

#### Jednalo se především o:

- sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti,
- sankce uložené podle zákona č. 110/2019 Sb., o zpracování osobních údajů, zákona o kontrole č. 255/2012 Sb., a dalších zákonů,
- náhrady nákladů řízení,
- vrácené přeplatky za energie z minulého roku.

### Výdaje

#### Čerpání výdajů ve výši 167 401,39 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, cestovního, vzdělávání a údržby,
- výdaje související s neinvestičními nákupy.

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

Čerpání rozpočtu na platy zaměstnanců, ostatních výdajů za provedenou práci a souvisejících výdajů, vč. základního přídělu FKSP, a náhrad v době nemoci, ve výši **100 848,52 tisíc Kč**, je dán kvalifikační strukturou a plněním plánu počtu pracovníků.

Stav k 31. prosinci 2022 byl **108 zaměstnanců**.

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

V souladu se schválenou dokumentací programu 043V01 „Rozvoj a obnova materiálně technické základny Úřadu pro ochranu osobních údajů od r. 2017“ bylo celkem vyčerpáno **12 485,75 tisíc Kč**.

V souladu se schválenou dokumentací programu 343V02 „Rozvoj a obnova materiálně technické základny Úřadu pro ochranu osobních údajů od r. 2022“ bylo celkem vyčerpáno **466,70 tisíc Kč**.



## ČERPÁNÍ STÁTNÍHO ROZPOČTU KAPITOLY 343 – ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Souhrnné ukazatele		v tisících Kč
<b>Příjmy celkem</b>		1 388,18
<b>Výdaje celkem</b>		167 401,39
Specifické ukazatele – příjmy		
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem		1 388,18
v tom: příjmy z rozpočtu Evropské unie bez společné zemědělské politiky celkem		0
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem		1 388,18
Specifické ukazatele – výdaje		
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů		167 401,39
Průřezové ukazatele výdajů		
Platy zaměstnanců a ostatní platby za provedenou práci		74 026,80
Povinné pojistné placené zaměstnavatelem*)		24 637,47
Základní přiděl fondu kulturních a sociálních potřeb		1 446,67
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech		11 674,45
Platy zaměstnanců na služebních místech dle zákona o státní službě		53 092,84
Platy zaměstnanců v pracovním poměru odvozené od platů ústavních činitelů		7 126,62
Výdaje spolufinancované zcela, nebo částečně z rozpočtu Evropské unie bez společné zemědělské politiky celkem		0
v tom: ze státního rozpočtu		0
podíl rozpočtu Evropské unie		0
Výdaje vedené v informačním systému programového financování EDS/SMVS celkem		12 952,45

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

## PŘEHLED ČERPÁNÍ ROZPOČTU V ROCE 2022

Položka	Název ukazatele	Schválený rozpočet v tis. Kč	Konečný rozpočet v tis. Kč	Skutečnost v tis. Kč	Skutečnost /konečný rozpočet v %
2211, 2212, 2322, 2324, 4132	Ostatní nedaňové příjmy	1 000,00	1 000,00	1 388,18	138,8
<b>Příjmy celkem</b>		<b>1 000,00</b>	<b>1 000,00</b>	<b>1 388,18</b>	<b>138,8</b>
501	Platy	68 417,94	73 311,12	71 893,91	98,1
5011	Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	8 130,02	12 032,82	11 674,45	97,0
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	53 164,72	54 151,10	53 092,84	98,0
5014	Platy zaměstnanců v pracovním poměru odvoz. od platů úst. činitelů	7 123,20	7 127,20	7 126,62	100,0
502	Ostatní platby za provedenou práci	1 890,91	2 329,53	2 132,89	91,6
5021	Ostatní osobní výdaje	1 890,91	2 232,28	2 035,64	91,2
5024	Odstupné	0,00	97,25	97,25	100,0
503	Povinné pojistné placené zaměstnavatelem	23 764,39	25 309,13	24 637,47	97,3
5031	Povin. pojist. na sociál. zabezp.	17 436,59	18 564,42	18 029,70	97,1
5032	Povin. pojist. na veřej. zdr. pojišť.	6 327,80	6 744,71	6 607,77	98,0
513	Výdaje na nákup materiálu	1 731,00	1 236,38	902,91	73,0
514	Úroky a ost. fin. výdaje	20,00	20,00	12,63	63,1
515	Nákup vody, paliv a energie	1 806,00	1 856,16	1 621,42	87,4
516	Výdaje na nákup služeb	47 757,62	49 768,23	45 964,21	92,4
517	Výdaje na ost. nákupy	4 833,00	3 556,54	3 248,32	91,3
518	Výdaje na netransfer. převody uvnitř. org., na převzaté povinnosti a na jistoty	20,00	0,00	0,00	0,00
519	Výdaje souvis. s neinv. nákupy, příspěvky, náhrady a věcné dary	1 990,00	2 330,06	1 848,84	79,3
534	Převody vlastním fondům a ve vztahu k útv. bez plné práv. subjektivity	1 368,36	1 474,52	1 446,67	98,1
5342	Základní přiděl fondu kult. a soc. potřeb a soc. fondů obcí a krajů	1 368,36	1 474,52	1 446,67	98,1
536	Ostatní neinvest. transf. jiným rozpočtům a platby daní	15,94	20,94	2,09	10,0
542	Náhrady placené fyzickým osobám	612,35	740,46	737,58	99,6
5424	Náhrady platů v době nemoci	612,35	740,46	737,58	99,6
<b>Běžné výdaje celkem</b>		<b>154 227,51</b>	<b>161 953,07</b>	<b>154 448,94</b>	<b>95,4</b>
611	Pořízení dlouh. nehmot. majetku	2 104,00	2 104,00	466,70	22,2
612	Pořízení dlouh. hmot. majetku	4 100,00	16 905,43	12 485,75	73,9
<b>Kapitálové výdaje celkem</b>		<b>6 204,00</b>	<b>19 009,43</b>	<b>12 952,45</b>	<b>68,1</b>
<b>Výdaje celkem</b>		<b>160 431,51</b>	<b>180 962,50</b>	<b>167 401,39</b>	<b>92,5</b>

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. prosince 2022.



## ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2022 a informace o jejím předání proběhne v řádném termínu do 31. července 2023 podle 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 zákonem č. 563/1991 Sb., o účetnictví v platném znění, není Úřad povinen mít účetní závěrku ověřenu auditorem.

## ZPRÁVA AUDITORA

Služební místo vnitřního auditora bylo v roce 2022 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 2022:

- 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,
- mezinárodní rámec profesní praxe interního auditu.

Cíle vnitřního auditu v roce 2022:

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

Činnost auditora v roce 2022 vycházela především ze střednědobého plánu auditů, z výsledků předchozích auditů a z požadavků vedoucích zaměstnanců Úřadu, přičemž byla zaměřena i na kon-

zultační činnost v souvislosti s veřejnosprávní kontrolou ze strany Ministerstva financí, která v Úřadu v roce 2022 proběhla. Následně byla v prosinci 2022 zahájena Finančním úřadem pro Kraj Vysočina daňová kontrola, při které Úřad poskytoval součinnost a která do konce roku 2022 nebyla ukončena.

Provedená kontrola Ministerstvem financí, jejímž předmětem bylo hospodaření Úřadu s veřejnými prostředky v letech 2020–2021, se zabývala mnoha oblastmi od ekonomicko-provozních činností včetně realizace veřejných zakázek přes oblast účetnictví až po personální správu. V protokolu o výsledku veřejnosprávní kontroly Ministerstva financí konstatovalo určité nedostatky vnitřního kontrolního systému Úřadu, které však, jak Úřad dokládá v rámci kontroly, nevedly k nehospodárnému nakládání s finančními prostředky ani ke vzniku škody na majetku státu. Totéž se týká pochybení v oblasti zaúčtování části pohledávek z pokut udělených Úřadem, ohledně něhož bylo návazně zahájeno příslušným finančním úřadem prozatím také neukončené přestupkové řízení. Toto konkrétní pochybení vycházelo z předchozí aplikační praxe Úřadu založené v roce 2013. Úřad tento problém identifikoval a připravoval nápravná opatření již před zahájením veřejnosprávní kontroly; v mezidobí tak byla provedena příslušná oprava a dále přijata preventivní opatření zabuzující opakování obdobné chyby. Také s některými kroky zaměřenými na posílení efektivity vnitřního kontrolního systému Úřad započal ještě před zahájením předmětné veřejnosprávní kontroly. Další opatření směrem k optimalizaci vnitřního kontrolního systému, spočívající v revizi vybraných interních aktů řízení a jejich aktualizaci, a současně v novém nastavení interních procesů zaměřených na lepší dokladování účelnosti, hospodárnosti a efektivnosti postupů při nakládání s veřejnými prostředky, provedl Úřad po ukončení kontroly a v souladu s požadavky Ministerstva financí jej o odstranění nedostatků a přijatých opatřeních podrobně informoval.

Cílem přijatých opatření přitom bylo dosažení maximální transparentnosti při vykazování efektivity hospodaření v souladu s nejlepší praxí v dané oblasti vyplývající z doporučení kontrolujícího orgánu. Funkčnost těchto přijatých opatření bude přezkoumána vnitřními audity naplánovanými na rok 2023. ●

## • Úřad v číslech

## • POČET STÍŽNOSTÍ A PODNĚTŮ

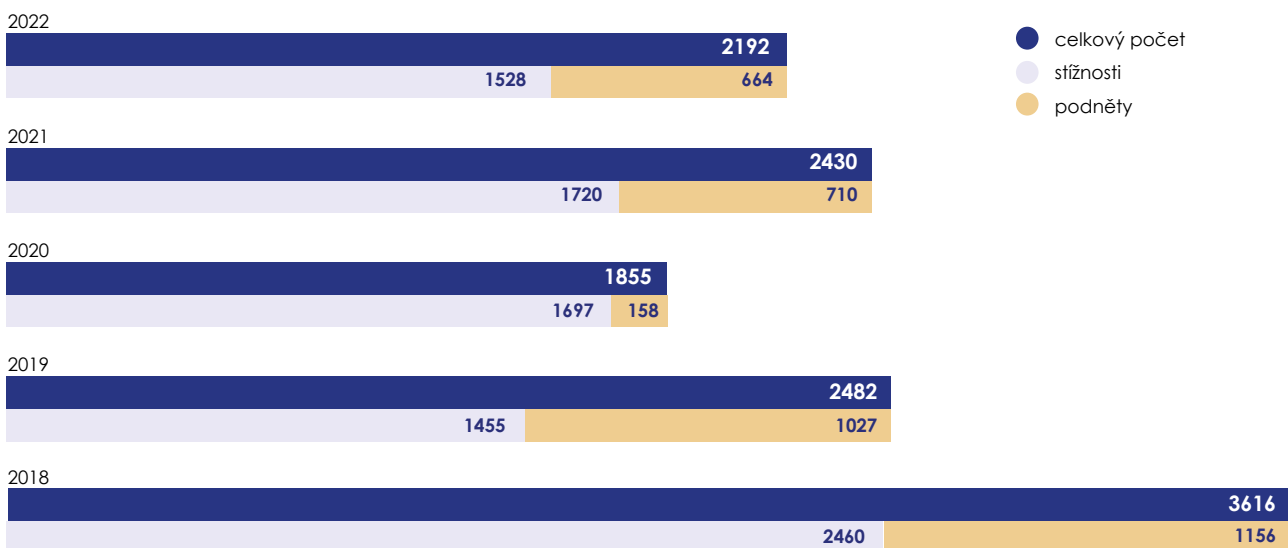
Při celkově menším počtu stížností a podnětů realizoval Úřad v porovnání s předchozími lety v roce 2022 nebývale vysoký počet upozornění správčům. Pokud jde o data breach, jejich počet byl v roce 2022 o něco vyšší než v předchozím roce, ale mnohem vyšší je počet doplnění data breach.

Celkový počet přijatých podnětů a stížností v roce 2022	2 192
z toho stížností <sup>[1]</sup>	1 528
z toho podnětů	664
Doplnění stížností/podnětů <sup>[2]</sup>	714
Vyřízeno odpovědí podatelů	1 264
Vyřízeno upozorněním správce na možné porušení obecného nařízení	785
Reakce správčů na upozornění	550
Předáno ke kontrole nebo jinému řízení	141
Poskytnutí součinnosti policii/žádost OČTR o součinnost	23
Počet ohlášení data breach	313
Doplnění data breach	151

<sup>[1]</sup> Namítané zpracování osobních údajů se týká podatele (podání učiněná subjektem údajů)

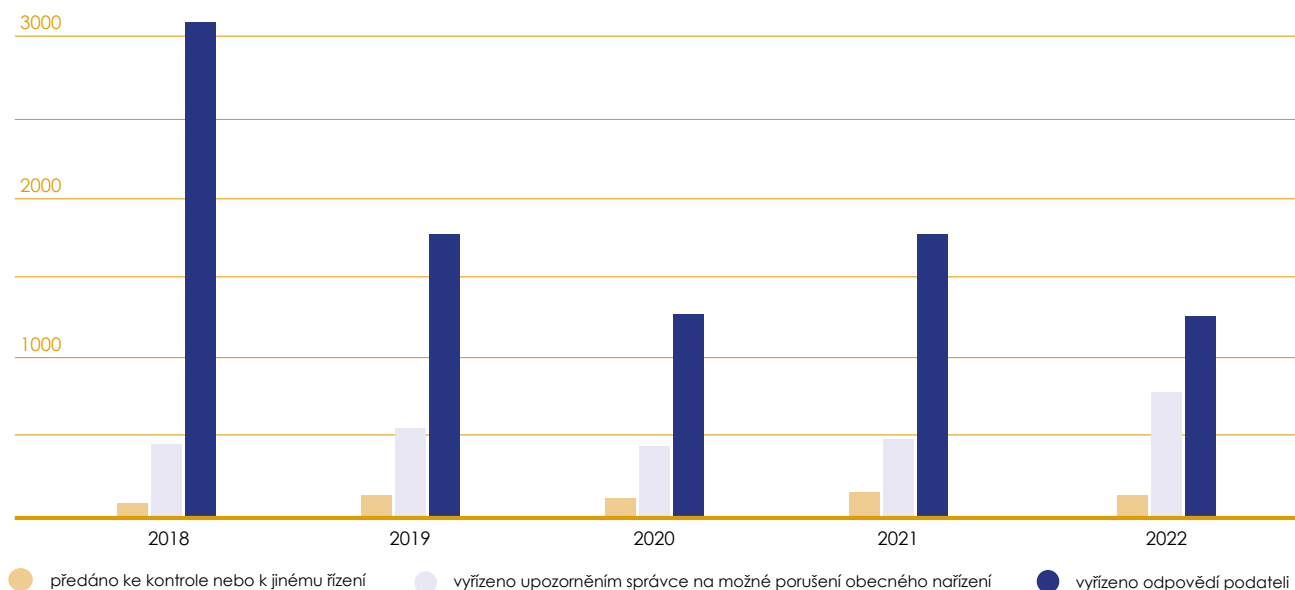
<sup>[2]</sup> Doplnění po žádosti Úřadu o upřesnění, nebo iniciovaná samotnými stěžovateli

## POČET PŘIJATÝCH PODÁNÍ V LETECH 2018–2022

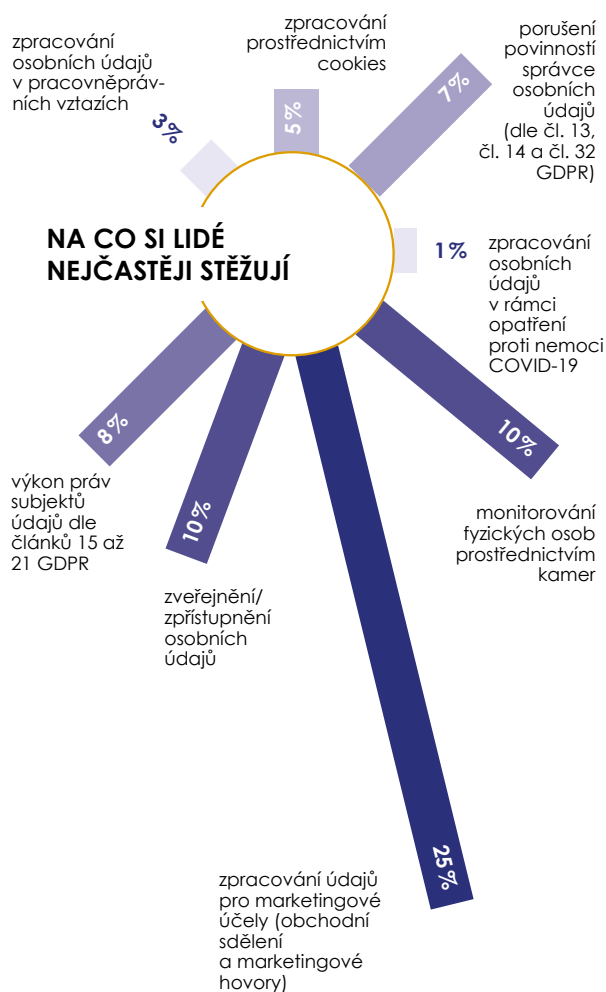




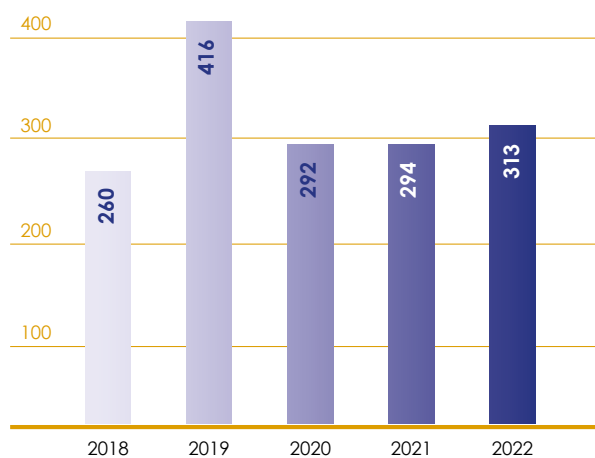
## ZPŮSOB VYŘÍZENÍ PŘIJATÝCH PODÁNÍ V LETECH 2018–2022



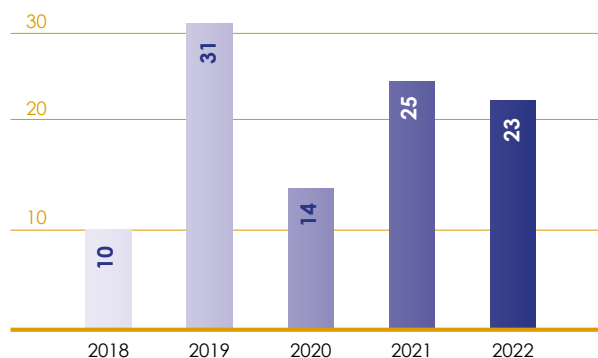
## Hlavní oblasti stížností



## PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ (DATA BREACH) V LETECH 2018–2022



## POSKYTNUTÍ SOUČINNOSTI OČTŘ/ŽÁDOST OČTŘ O SOUČINNOST V LETECH 2018–2022





## DOZOROVÁ ČINNOST ÚŘADU

(vyjma dozoru v oblasti obchodních sdělení)

Počet zahájených kontrol	25
Počet ukončených kontrol	20
z toho z předchozích let	17
Počet kontrolních protokolů napadených námitkami	14
Počet vyřízených námitek	13
- námitkám vyhověno	1
- námitkám částečně vyhověno	4
- námitky zamítnuty	5
- vráceno k došetření	3
Uložené tresty dle kontrolního řádu za neposkytnutí součinnosti	1
Zahájená správní řízení	29
Upuštěno od potrestání ve smyslu § 65 zákona č. 110/2019 Sb.	3
Vyřešeno jinak	32

## Dozorová činnost v oblasti obchodních sdělení

- V roce 2022 uložil Úřad pravomocně 30 pokut za porušení zákona č. 480/2004 Sb. ve věci zasílání obchodních sdělení. Z toho bylo 10 správních řízení vedeno za opakovaná porušení povinností při zasílání obchodních sdělení.
- Nejvyšší částka uložené pokuty 250 000 Kč byla uložena za zasílání obchodních sdělení bez právního titulu.
- Celková částka uložených pokut za rok 2022 v souvislosti se zasíláním obchodních sdělení činí 828 000 Kč.
- Za neposkytování součinnosti při kontrole dodržování povinností při zasílání obchodních sdělení bylo vedeno 6 správních řízení, přičemž celková výše pokut za toto porušení činila 120 000 Kč.
- Mezi nejčastější pochybení patřilo zasílání obchodních sdělení bez právního titulu, ale stejně tak jako v předchozím roce docházelo k porušení i v náležitostech obchodních sdělení, zejména neuvádnění možnosti další zasílání obchodních sdělení odmítnout.

## DOZOROVÁ ČINNOST V OBLASTI OBCHODNÍCH SDĚLENÍ

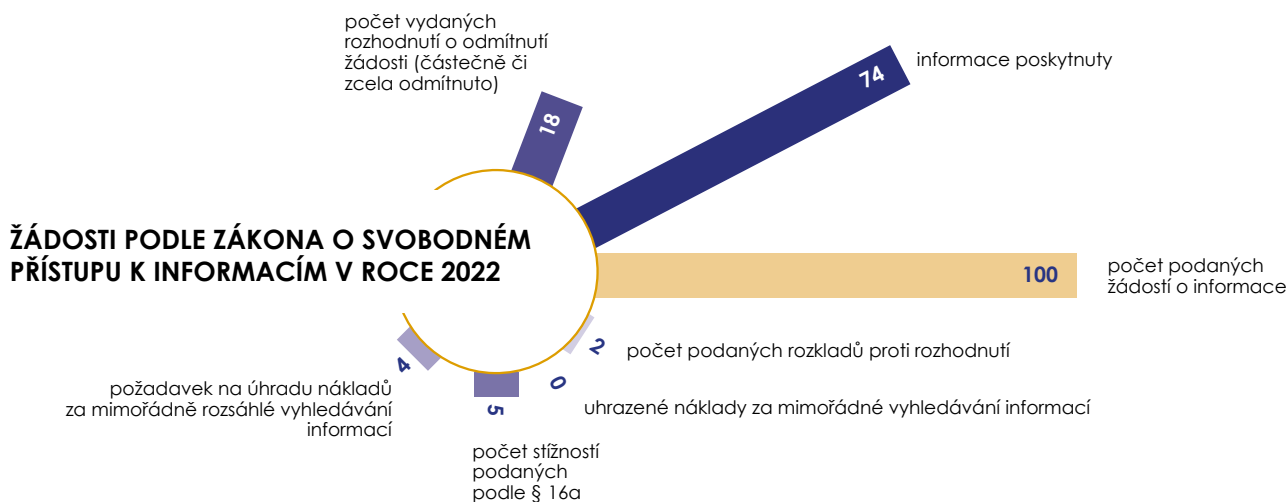
podnětů celkem	906
zahájených kontrol	12
ukončených kontrol	10*
napadeno námitkami	2
řízení o sankci	30
pokuty za neposkytnutí součinnosti v kontrole	6
pokuty za neposkytnutí součinnosti v kontrole	351

\* z toho 4 z předchozích let

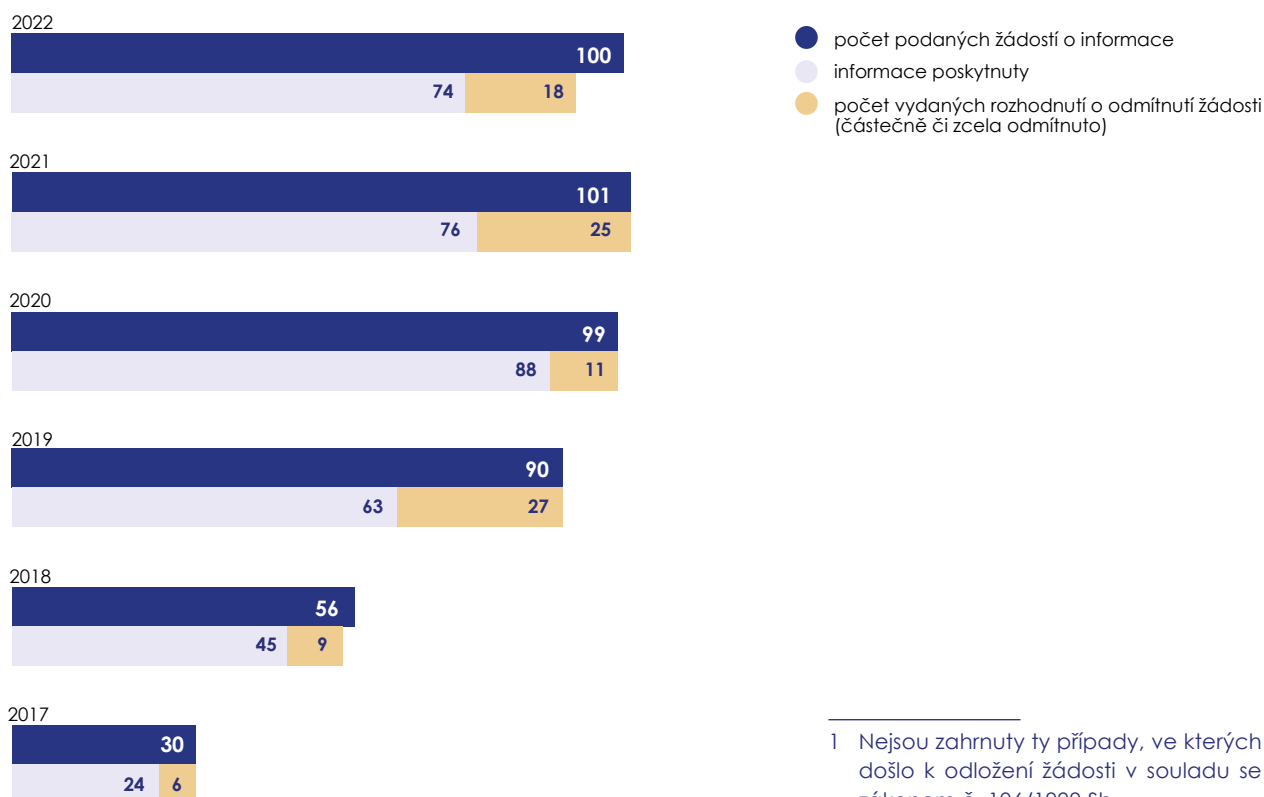




## ÚŘAD A POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/ 1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM



### ŽÁDOSTI PODLE ZÁKONA O SVOBODNÉM PŘÍSTUPU K INFORMACÍM V LETECH 2017–2022<sup>1</sup>



## ROZHODOVÁNÍ PŘEDSEDY ÚŘADU

### SPRÁVNÍ ŘÍZENÍ

Podané rozklady proti rozhodnutím Úřadu	7
Vyřízené rozklady	7*
- rozklad zamítnut	2
- rozhodnutí zrušeno, vráceno	1
- rozhodnutí zrušeno, řízení zastaveno	2
- rozhodnutí změněno	2
Změna	2

\*z toho 3 z předchozích let

### Přijata podání k nadřízenému správnímu orgánu (§ 175 správního řádu)

Přijatých podání podle § 175	50
z toho stížností podle § 175 odst. 1	43
z toho žádostí podle § 175 odst. 7	7
Vyřízených podání podle § 175	43
z toho stížností podle § 175 odst. 1	36
z toho žádostí podle § 175 odst. 7	7
Ze všech vyřízených podání posouzeno jako	
stížností důvodných	1
stížností částečně důvodných	8
žádostí důvodných	1
zbývajících podání nedůvodných	3
Nevyřízeno	10

## SOUDNÍ PŘEZKUM ROZHODNUTÍ (PŘEDSEDY) ÚŘADU

Městský soud v Praze:

Podané žaloby	1
Žaloba se zamítá	1
Rozhodnutí se ruší a věc se vrací	0
Řízení se zastavuje	0

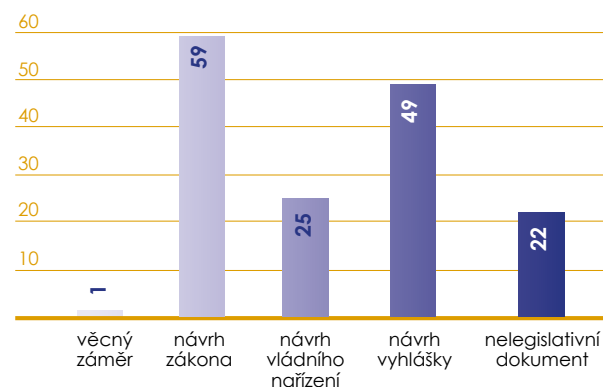
Nejvyšší správní soud:

Podané kasační stížnosti	0
Kasační stížnost se zamítá	1

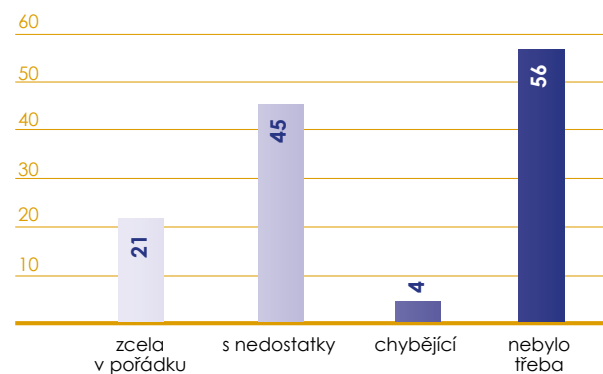
Celkem podaných žalob od roku 2001	172
z toho ukončených soudních řízení	166
neukončených soudních řízení	6

## LEGISLATIVA

### DRUHY PŘIPOMÍNKOVANÝCH NÁVRHŮ

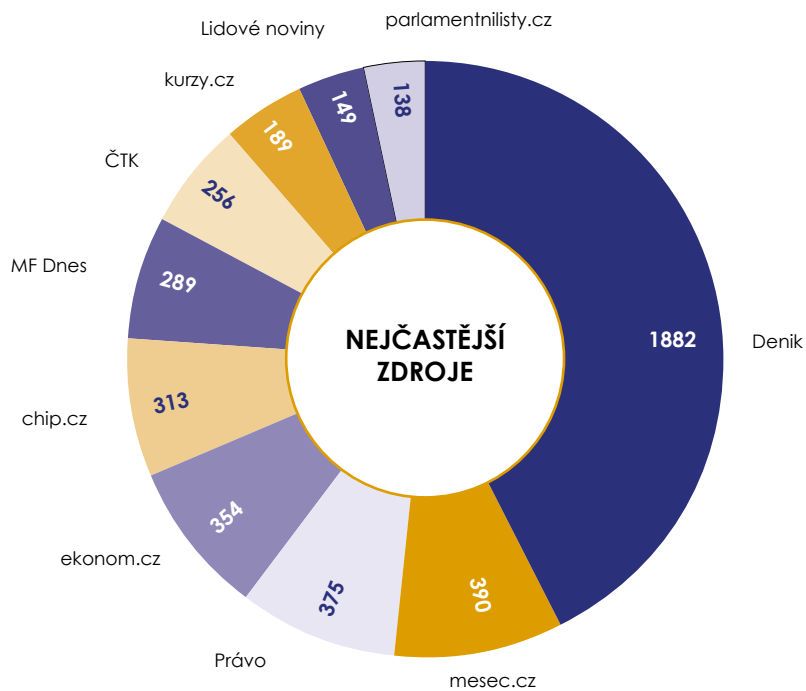


### POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ – DPIA



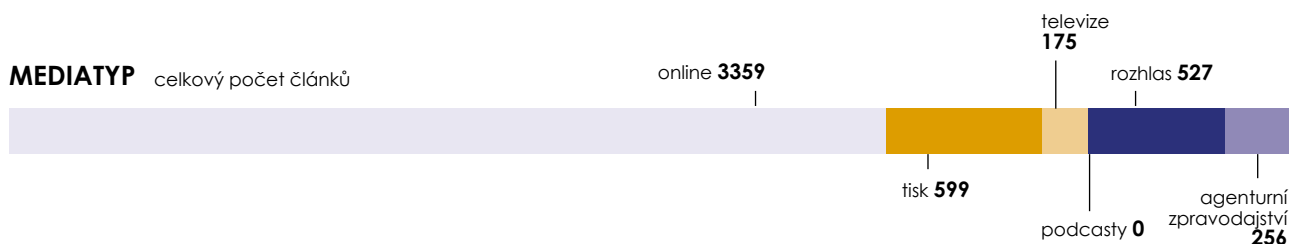


## KOMUNIKACE



### MEDIATYP

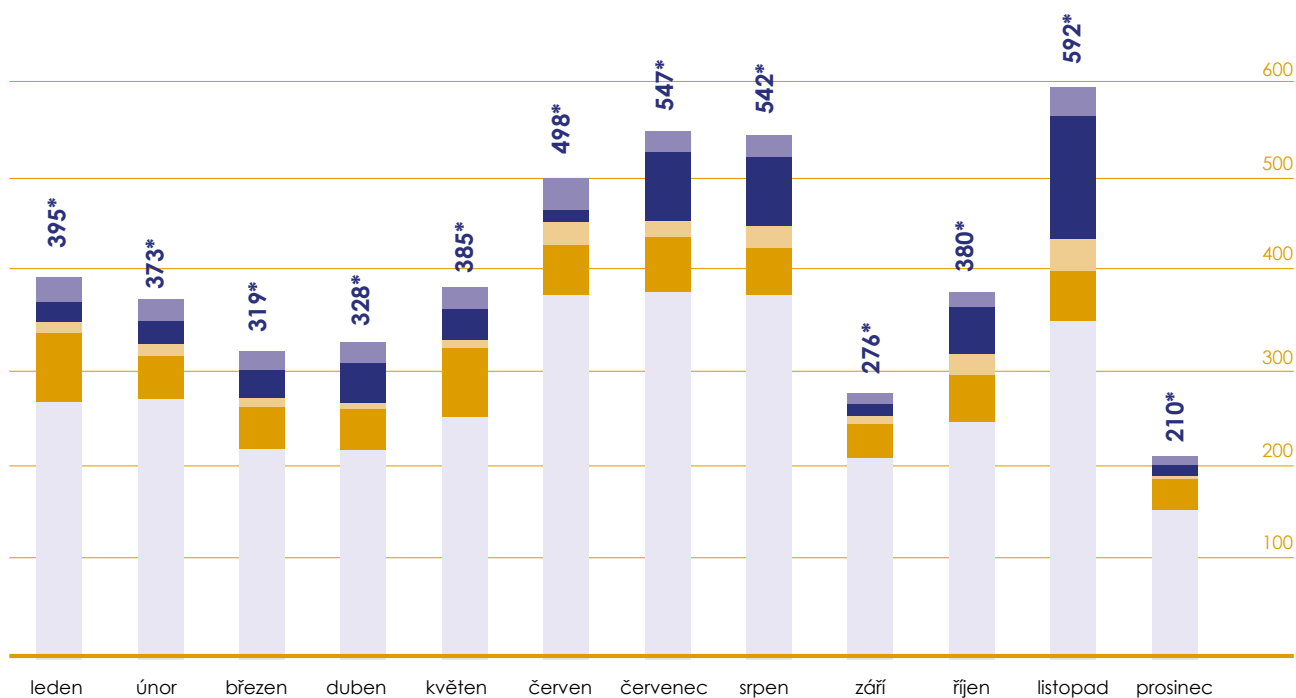
celkový počet článků



### POČET MEDIÁLNÍCH VÝSTUPŮ

● rozhlas 
 ● tisk 
 ● online 
 ● televize 
 ● agenturní zpr.

\* součet všech mediálních kanálů







## • Seznam použitých zkratk

AIFO	Agendový identifikátor fyzické osoby
AIS	Agendové informační systémy
BCR	Binding Corporate Rules (Závazná vnitropodniková pravidla)
BTLE	Borders, Travel & Law Enforcement (Pracovní podskupina EDPB pro hranice, cestování a vymáhání práva)
CEF	Coordinated Enforcement Action (Společná dozorová akce EDPB)
CEH ESG	EDPB Compliance, E-government and Health Expert Subgroup (Podskupina EDPB pro dodržování předpisů, elektronickou veřejnou správu a zdravotnictví)
CIS	Celní informační systém
ČÚZK	Český úřad zeměměřický a katastrální
EDPB	<ul style="list-style-type: none"><li>• European Data Protection Board (Evropský sbor pro ochranu osobních údajů)</li><li>• Sbor</li></ul>
EDPS	European Data Protection Supervisor (Úřad evropského inspektora pro ochranu osobních údajů)
EHP	Evropský hospodářský prostor
EU	Evropská unie
EURODAC	European Asylum Dactyloscopy Database (Evropská databáze pro srovnání otisků prstů žadatelů o azyl a některých kategorií ilegálních přistěhovalců)
GDPR	<ul style="list-style-type: none"><li>• Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)</li><li>• Obecné nařízení Evropské unie o ochraně osobních údajů</li><li>• Obecné nařízení</li><li>• Nařízení (EU) 2016/679</li></ul>
GPA	Global Privacy Assembly (Světové shromáždění pro ochranu osobních údajů)
ISIN	Informační systém infekčních nemocí
IS ORG	Informační systém ORG (Informační systém pro převod identifikátorů)

ITS	International Transfers Subgroup (Pracovní podskupina EDPB pro předávání do třetích zemí)
ISZR	Informační systém základních registrů
MZ ČR	Ministerstvo zdravotnictví České republiky
NSS	Nejvyšší správní soud
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OP	Občanský průkaz
ROB	Registr obyvatel České republiky
SDEU	Soudní dvůr Evropské unie
SIS	Schengenský informační systém
Směrnice o elektronickém obchodu	Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
Směrnice o soukromí a elektronických komunikacích	Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)
ÚOOÚ / Úřad	Úřad pro ochranu osobních údajů
ÚZIS	Ústav zdravotnických informací a statistiky České republiky
VIS	Vízový informační systém
ZIFO	Zdrojový identifikátor fyzické osoby
ZR	Základní registry
Zákon č. 99/1963 Sb.	Zákon č. 99/1963 Sb., občanský soudní řád
Zákon č. 106/1999 Sb.	Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
Zákon č. 101/2000 Sb.	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
Zákon č. 258/2000 Sb.	Zákon č. 258/2000 Sb., o ochraně veřejného zdraví
Zákon č. 301/2000 Sb.	Zákon č. 301/2000 Sb., o matrikách, jménu a příjmení
Zákon č. 120/2001 Sb.	Zákon č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů
Zákon č. 235/2004 Sb.	Zákon č. 235/2004 Sb., o dani z přidané hodnoty



Zákon č. 480/2004 Sb.	Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů
Zákon č. 500/2004 Sb.	Zákon č. 500/2004 Sb., správní řád
Zákon č. 127/2005 Sb.	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
Zákon č. 111/2009 Sb.	Zákon č. 111/2009 Sb., o základních registrech
Zákon č. 100/2010 Sb.	Zákon č. 100/2010 Sb., kterým se mění zákon č. 111/2009 Sb., o základních registrech
Zákon č. 372/2011 Sb.	Zákon č. 372/2011 Sb., o zdravotních službách
Zákon č. 255/2012 Sb.	Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)
Zákon č. 110/2019 Sb.	Zákon č. 110/2019 Sb., o zpracování osobních údajů
Zákon č. 283/2021 Sb.	Zákon č. 283/2021 Sb., stavební zákon
Vyhláška č. 98/2012 Sb.	Vyhláška č. 98/2012 Sb., vyhláška Ministerstva zdravotnictví o zdravotnické dokumentaci



**Úřad pro ochranu  
osobních údajů**

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2022

Úřad pro ochranu osobních údajů

Pplk. Sochora 27, 170 00 Praha 7

E-mail: [posta@uouu.cz](mailto:posta@uouu.cz)

Internetová adresa: [www.uouu.cz](http://www.uouu.cz)

Na základě povinnosti, kterou 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 na svých internetových stránkách.

Editor: Milan Řepka (T +420 234 665 286)

Redakce: Milan Řepka

Grafická úprava a sazba: MgA. Lucie Baťková

Stylistická a jazyková korektura: Mgr. Lenka Brabencová, Zdeněk Švehla (Korektury Švehla)

Tisk: Expressta







Úřad pro ochranu  
osobních údajů