Úřad pro ochranu
osobních údajů

VÝROČNÍ ZPRÁVA
2023

Úřad pro ochranu
osobních údajů

VÝROČNÍ ZPRÁVA

2023

Obsah

(interaktivní)

Slovo předsedy

Vážené dámy, vážení pánové,

rok 2023 přinesl v oblasti ochrany osobních údajů celou řadu výzev, které reflektovaly především velmi dynamický rozvoj digitálních služeb a digitálních nástrojů, a to v evropském i globálním rozměru. Zároveň se zásadně zlepšilo obecné povědomí o tom, že naše osobní údaje jsou skutečně důležitými a cennými informacemi, s nimiž se velmi vyplácí obchodovat. Úřad pro ochranu osobních údajů tak vzhledem k používání stále sofistikovanějších nástrojů monetizace osobních údajů věnoval intenzivní pozornost jejich ochraně před jejich potenciálním zneužitím.

Současný překotný vývoj informačních technologií jasně potvrzuje nutnost relativně detailní regulace zpracování osobních údajů, a to zejména u „velkých zpracovatelů". Prudce vzrůstá zájem o osobní data uživatelů internetu a nejrůznějších datových služeb včetně sociálních platforem a snaha o jejich monetizaci či jiné zneužití. Obecné nařízení o ochraně osobních údajů zůstává zásadním dokumentem, jehož pravidla zpracování osobních údajů se stala základem pro celou řadu nově přijímaných regulací, jako jsou například Digital Services Act (DSA), European Data Governance Act (DGA), Digital Markets Act (DMA) nebo nařízení o umělé inteligenci (Artificial Inteligence Act, AIA). Naším úkolem jako národního dozorového úřadu pro oblast ochrany osobních údajů je v rámci uvádění těchto předpisů v život i jejich následné aplikace důsledně dbát na aplikaci právě ve prospěch ochrany osobních údajů. Úřad dlouhodobě upozorňuje na objektivní stav nedostatečných personálních kapacit, které v zásadě vylučují řádný výkon nových jemu přidělovaných agend.

Opodstatněnost důsledné ochrany osobních údajů, zejména před jejich masovým zneužíváním, je zásadně umocněna trvající vojenskou agresí Ruské federace, která rozpoutala hybridní válku proti svobodnému světu. To mj. vede k zásadním požadavkům na ochranu osobních údajů v úzkém propojení se zajištěním kybernetické bezpečnosti. Společným jmenovatelem je právě ochrana soukromí jednotlivců, ať už při obchodování s jejich osobními údaji anebo při jejich systémovém ohrožení v digitálním prostoru, masové manipulaci veřejného mínění, šíření dezinformací, krádeži identity nebo organizovaných nátlakových akcích.

Ochrana osobních údajů nikdy nemůže být převážně reaktivní v podobě dozoru národního dozorového orgánu, tedy v našem případě Úřadu. Bez efektivního dozoru, včetně sankčního řízení, bychom však nedokázali zajistit generální prevenci zneužívání osobních údajů. Úřad se proto snaží důsledně chránit práva subjektů osobních údajů, a to i v oblastech, kde to doposud nebylo tolik vidět. Jako zásadní zlom vnímáme skutečnost, že Úřad v roce 2023 dokončil řízení v případu informačního systému Karanténa, kdy Policie ČR neoprávněně plošně shromažďovala údaje o osobách, kterým byla z důvodu onemocnění COVID-19 nařízena izolace. Z historického pohledu jde o první pokutu v oblasti zpracování osobních údajů podle tzv. trestněprávní směrnice. Úřad se potenciálnímu porušování trestněprávní směrnice bude intenzivně věnovat i nadále, protože veřejná moc má mnohem invazivnější prostředky získávání a zpracování osobních údajů, a proto by zejména v trestněprávní oblasti měla být podrobena intenzivní kontrole.

V soukromém sektoru i v roce 2023 vzhledem ke změně právní úpravy silně rezonovalo téma zpracování osobních údajů na internetu prostřednictvím cookies souborů. Úřad v této oblasti působí především metodicky (podstatně rozšířil „otázky a odpovědi " pro oblast cookies souborů), ale intenzivně se věnuje též dozorové činnosti, aby došlo k principiální změně prostředí internetu. Doposud Úřad udělil pokuty za téměř 5 milionů korun. Můžeme konstatovat, že již dochází ke změně praxe provozovatelů webových stránek v České republice. Skutečně pozorujeme viditelnou snahu uvádět vše do souladu s obecným nařízením a dalšími právními předpisy. Aby tyto změny byly trvalé, Úřad nepoleví ve své snaze postihovat nezákonné vytěžování osobních údajů prostřednictvím cookies souborů.

V rámci kontrol krajů zavedl v roce 2023 Úřad novou efektivní metodiku pro kontrolu veřejného sektoru, která je založena na šetření prostřednictvím standardizovaných dotazníků. Tento přístup je inspirován celoevropským přístupem a Úřad se chystá k jeho široké aplikaci.

Při naplňování naší působnosti v oblasti kontroly vízového procesu se Úřadu podařilo odhalit pochybení při zpracování osobních údajů nejen v České republice, ale také na našich zastupitelských úřadech mimo Evropskou unii. Výrazně jsme zintenzivnili naši reálnou kontrolní činnost, když při kontrolách byla realizována místní šetření na zastupitelských úřadech České republiky a v jejích vízových centrech ve třech zemích mimo EU. Výsledky kontrol přispěly ke zkvalitnění postupů ochrany osobních údajů v této vysoce citlivé oblasti, přičemž přínos těchto změn je mnohem širší a dopadá i do bezpečnostní oblasti.

S cílem efektivnějšího provádění dozoru nad zpracováním osobních údajů v režimu hlavy III zákona č. 110/2019 Sb., o zpracování osobních údajů, a v rámci informačních systémů SIS, VIS, CIS, Eurodac, Europol a dalších vzniklo v odboru dozoru nové specializované oddělení bezpečnostních agend, které se kromě uvedeného podílí i na činnosti společných dozorových orgánů a spolupracuje s ostatními dozorovými úřady, jakož i s Evropským inspektorem pro ochranu osobních údajů (EDPS – European Data Protection Supervisor).

Úřad se trvale snaží o preventivní působení i v agendě nevyžádaných obchodních sdělení. V roce 2023 jsme např. při kontrole dopravní společnosti zjistili, že cestujícím, kteří si zakoupili jízdenku na internetových stránkách, byla prostřednictvím e-mailu neoprávněné rozesílána obchodní sdělení ve prospěch třetích subjektů. Jednalo se o 40 milionů takových sdělení za dobu několika let. Proto i z důvodu celospolečenského dopadu takového jednání Úřad udělil pokutu přes 7 milionů korun.

V oblasti práva na informace jsem rád, že se podařilo personálně stabilizovat odbor práva na informace, neboť z více konkrétních důvodů jsou řízení právně a odborně stále náročnější. Přes trvalý nárůst objemu i složitosti kauz se doposud daří zákonné požadavky na obsah i proces naší činnosti průběžně zvládat. Vzhledem k pokračujícímu zásadnímu rozšiřovaní okruhu povinných subjektů nicméně dochází k postupnému zahlcovaní systému, na což doplácejí především žadatelé tím, že se v zákonem předvídaném krátkém čase nemohou dobrat realizace svého zákonného práva na informace. Zařazení této agendy do působnosti Úřadu se v určitých ohledech jeví jako pozitivní, protože v řízení o žádosti se může vhodně vyvažovat právo na informace s právem na soukromí osob, jichž se předmět žádosti týká. Například se jedná o výklad pojmu osobní údaj a výklad konceptů anonymizace

a pseudonymizace podle obecného nařízení. Přestože je Úřad de facto ústředním úřadem pro ochranu práva na informace, není relevantně účasten legislativního procesu novel informačního zákona. To vede k tomu, že novelizace informačního zákona často nevyčerpávají potenciál zlepšení realizace práva na informace nebo dokonce situaci značně ovlivněnou dynamickou judikaturou spíše komplikují.

V oblasti konzultací se podařilo zavést nové projekty. Mohu zmínit cyklus vzdělávacích seminářů pro odbornou veřejnost. V roce 2023 se uskutečnily čtyři semináře a pro obrovský zájem z řad odborné veřejnosti jsme kromě prezenční formy zajistili možnost zúčastnit se prostřednictvím online streamů. Díky možnosti online účasti návštěvnost seminářů stoupla skokově o stovky procent. Vzdělávací činnost chce Úřad rozvíjet i v dalších letech, protože vliv tohoto přístupu, kdy bereme správce osobních údajů spíše jako partnery než adresáty naší úřední činnosti, je někdy pro kultivaci prostředí zpracování osobních údajů významnější než dopad individuálních rozhodnutí v dozorové agendě Úřadu. Dále Úřad, obdobně jako v minulých letech, zaznamenal velký zájem odborné i laické veřejnosti o zpracování osobních údajů prostřednictvím kamerových systémů. Na tento zájem jsme reagovali zpracováním nové Metodiky k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů, kterou jsme poskytli k veřejné konzultaci. Na jejím základě byl návrh metodiky upraven, a mohl tak nahradit původní dokument, který Úřad publikoval před více než deseti lety, v roce 2012. Počítáme s tím, že tento dokument bude průběžně aktualizován, zejména v návaznosti na poznatky z dozorové činnosti a využívání sofistikovanějších programů, které využívají kamerové systémy. Rovněž bychom v návaznosti na legislativní vývoj a vývoj aplikační praxe na evropské úrovni rádi dopracovali metodiku o specifika kamerových systémů umožňujících zpracování biometrických osobních údajů.

Úřad v roce 2023 vydal řadu materiálů formou tištěných informačních letáků, které jsou zaměřeny např. na pravidla Schengenského informačního systému, zpracování osobních údajů, posouzení vlivu na zpracování osobních údajů (tzv. DPIA), zpracovávání souborů cookies nebo podmínek pro poskytování konzultací Úřadem. V oblasti obecné prezentace činnosti Úřadu jsme pokračovali v implementaci nového jednotného vizuálního stylu a podařilo se nám také realizovat kompletní redesign struktury, obsahu a vizuálního stylu u našeho nového internetového prostředí. Nemohu opomenout ani úspěšný přechod Úřadu na novou státní doménu gov.cz.

V evropské koordinaci jsme standardizovali přípravu na jednání našich expertů v Evropském sboru pro ochranu osobních údajů (EDPB), v jeho pracovních skupinách i v plénu. Fungování EDPB je závislé právě na aktivitě národních dozorových úřadů, která je i mimořádnou příležitostí k přebírání nových poznatků do vlastní dozorové činnosti Úřadu.

Rok 2023 byl zároveň pětiletým výročím účinnosti obecného nařízení o ochraně osobních údajů. Lze proto učinit i určitou širší bilanci tohoto období. Obecné nařízení, které nabylo účinnosti 25. května 2018, od svého rozpačitého přijetí a přes zčásti oprávněnou kritiku přílišné administrativní zátěže vedlo za dobu své aplikace k zásadnímu zlepšení standardů ochrany osobních údajů i soukromí obecně. Zlepšení standardů ochrany osobních údajů se podařilo i přesto, že překotný rozvoj informačních technologií naopak přinášel stále intenzivnější rizika pro bezpečí osobních údajů i intimitu našeho soukromí. Lze tedy předpokládat, že by v případě setrvání u předchozí právní úpravy došlo k opačnému jevu. Díky obecnému nařízení a z něj vycházející aplikační praxi, zejména u velkých kauz týkajících se celosvětově působících firem, se zásadně zlepšilo i obecné povědomí o faktu, že naše osobní údaje jsou velmi důležité a je nezbytné jim a jejich ochraně věnovat odpovídající míru pozornosti. Z ní pak pramení zájem jednotlivců nejen o to, co to vlastně jsou jejich osobní údaje, ale také o to, jak s nimi bude nakládáno, když je někomu poskytnou.

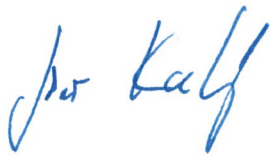
Obecné nařízení zavedlo také některé nové instituty. Jedním z nich je preventivní povinnost posouzení vlivu na ochranu osobních údajů u zpracování, které by mohlo představovat vysoké riziko pro práva a svobody fyzických osob (tzv. DPIA). Toto posouzení vlivu má, pokud je provedeno správně, rozhodující vliv na to, aby

osobní údaje byly řádně chráněny. A to jak u jednotlivého zpracování, tak z mého pohledu především v legislativní oblasti před přijetím nové právní normy (tzv. legislativní DPIA). Pokud toto posouzení neprovedeme nebo je provedeme čistě formálně, riskujeme další a další nepřiměřené nebo dokonce nezákonné zásahy do ochrany osobních údajů, a to z hlediska nadbytečnosti shromažďovaných údajů, rozsahu nebo doby, po kterou jsou zpracovávány, rizika jejich potenciálního zneužití apod. Není bez významu, že „ušetřená" práce s tvorbou řádného posouzení vlivu na počátku se zpravidla vymstí jak při kontrole jednotlivého zpracování, tak zejména při aplikaci právní normy, kdy lze vysledovat mnohá systémová selhání. Obecné nařízení přineslo významné zapojení dozorových orgánů do přípravy nových právních předpisů. Úřad právě o takové řádné posouzení usiluje v meziresortních připomínkových řízeních i v dalších fázích legislativního procesu.

I v roce 2023 zajišťoval Úřad provozování kritického informačního systému poskytujícího zdrojové a agendové identifikátory fyzických osob (IS ORG). Přestože význam i provozní zatížení IS ORG nadále vzrůstá, což níže dokládají grafy zpracovaných transakcí, systém obdobně jako v minulých letech spolehlivě fungoval a jeho provoz nebyl výrazněji zasažen např. ani spuštěním aplikace eDoklady.

Vážené dámy, vážení pánové, ve výroční zprávě Úřadu pro ochranu osobních údajů za rok 2023 najdete mnohem více podrobnějších informací o činnosti v ochraně osobních údajů, realizaci práva na informace i v plnění dalších zákonných úkolů Úřadu. Dovoluji si vyjádřit naději, že vám naše výroční zpráva přinese mnoho užitečných informací a pomůže podpořit vnímání skutečné nezastupitelnosti významu ochrany osobních údajů a soukromí jednotlivce.

S úctou



MGR. JIŘÍ KAUCKÝ
předseda Úřadu

> „Současný překotný vývoj informačních technologií jasně potvrzuje nutnost relativně detailní regulace zpracování osobních údajů, a to zejména u ‚velkých zpracovatelů'. Prudce vzrůstá zájem o osobní data uživatelů internetu a nejrůznějších datových služeb včetně sociálních platforem a snaha o jejich monetizaci či jiné zneužití."

Úřad 2023

1. Cookies

Porušení, která ÚOOÚ shledal v oblasti zpracování osobních údajů prostřednictvím souborů cookies

Více než

70 %

zpracování osobních údajů prostřednictvím cookies souborů před získáním souhlasu návštěvníka internetových stránek s jejich nahráním

50 %

nedostatky v plnění informační povinnosti

Téměř

30 %

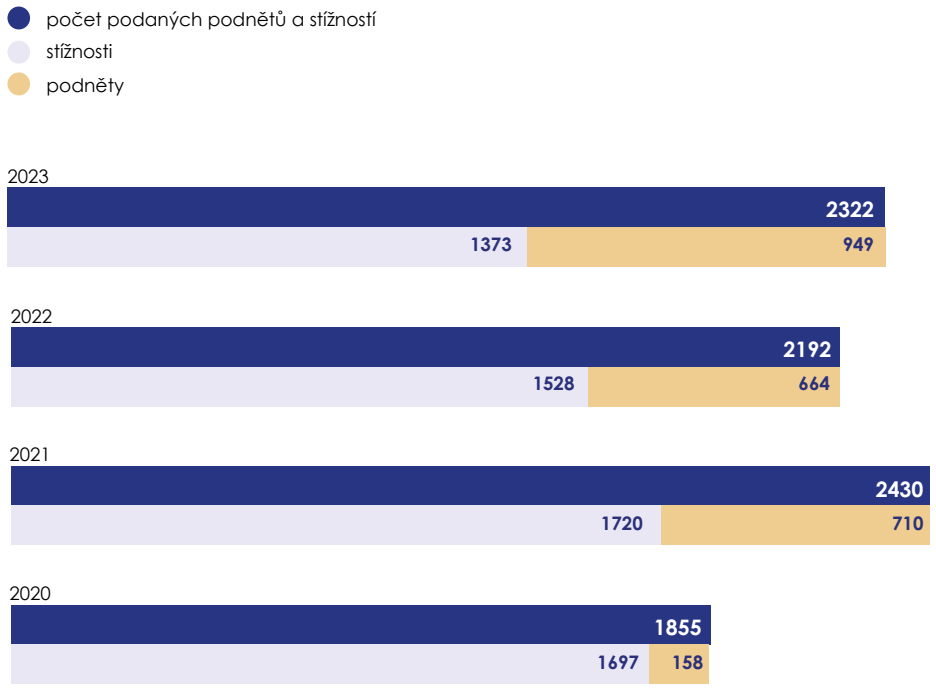
porušení v umístění možnosti souhlasu a odmítnutí s nahráním netechnických cookies souborů do různých vrstev cookie lišty

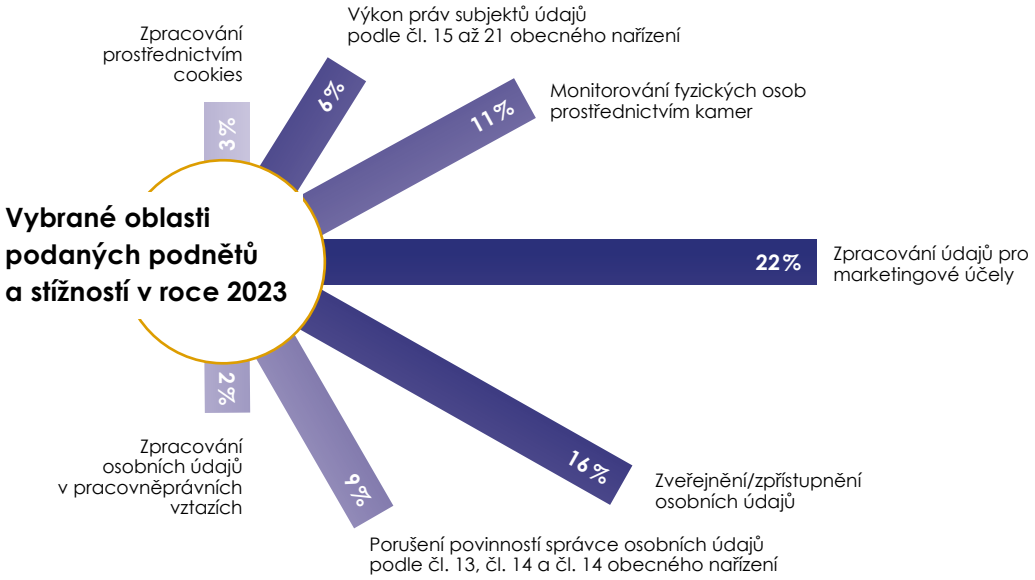
2. Podněty a stížnosti

Ochrana osobních údajů

Úřad provádí dozorovou činnost v oblasti ochrany osobních údajů upravenou především obecným nařízením a zákonem 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.

PODANÉ PODNĚTY A STÍŽNOSTI

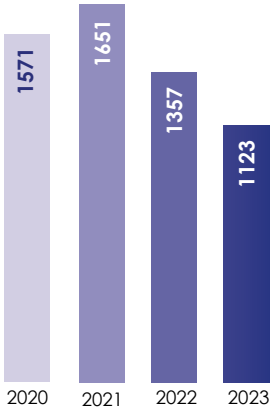




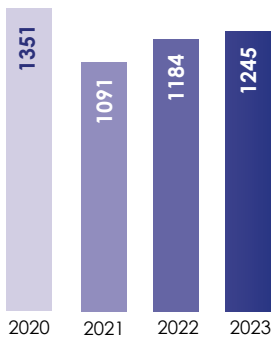
3. Konzultační činnost

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

POČET PÍSEMNÝCH DOTAZŮ VEŘEJNOSTI



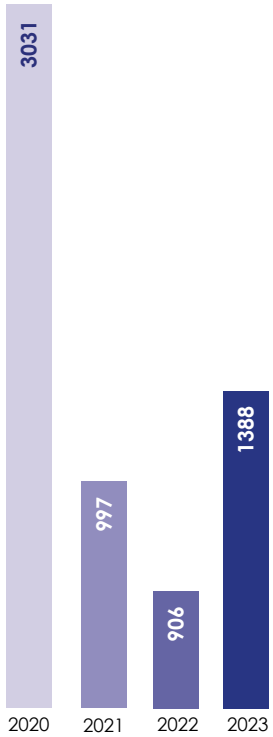
POČET TELEFONNÍCH DOTAZŮ NA KONZULTAČNÍ LINCE



4. Nevyžádaná obchodní sdělení

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

POČET PODANÝCH STÍŽNOSTÍ



5. Svobodný přístup k informacím

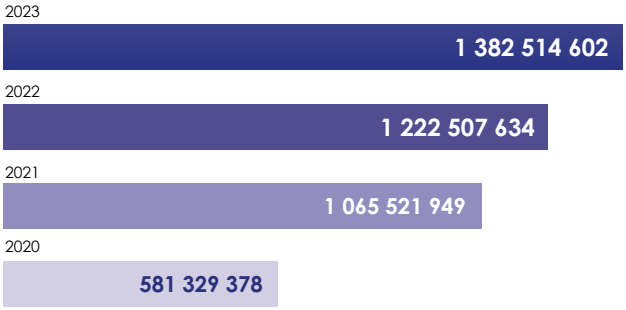
Počet soudních řízení s účastí Úřadu, týkajících se zákona č. 106/1999 Sb., oznámených Úřadu v jednotlivých letech

6. IS ORG

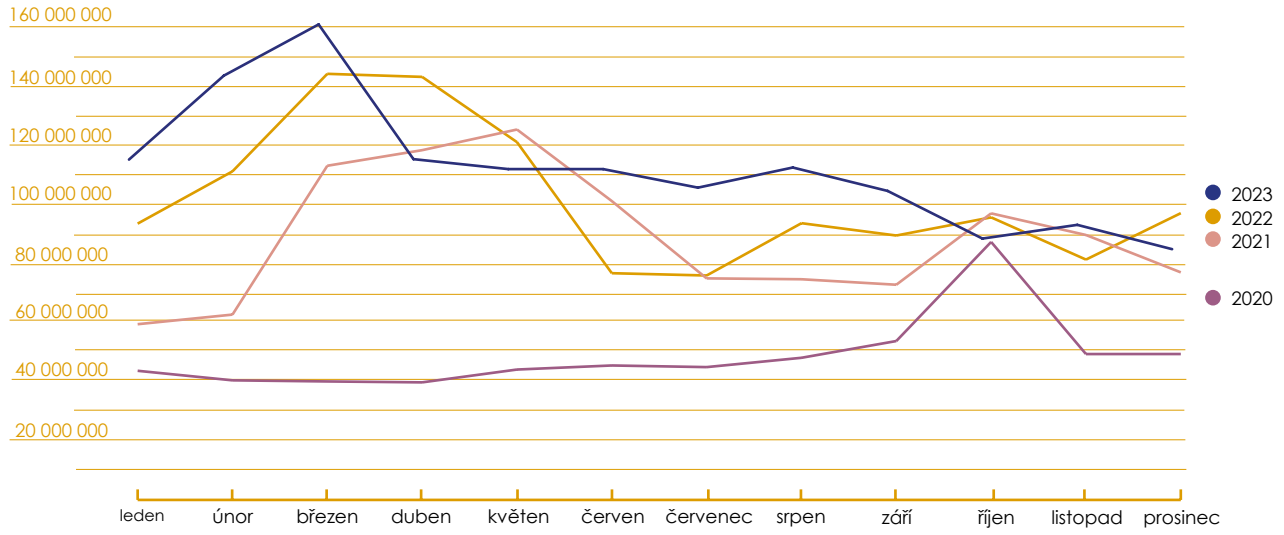
Zdrojové a agendové identifikátory fyzických osob / IS ORG

Úřad je správcem a provozovatelem autonomního informačního systému základních registrů. Ten zajišťuje ochranu osobních údajů občanů uložených v základních registrech České republiky. Význam i provozní zatížení IS ORG nadále vzrůstá, což dokládají grafy zpracovaných transakcí za roky 2020 až 2023.

POČET TRANSAKCÍ V LETECH 2020–2023



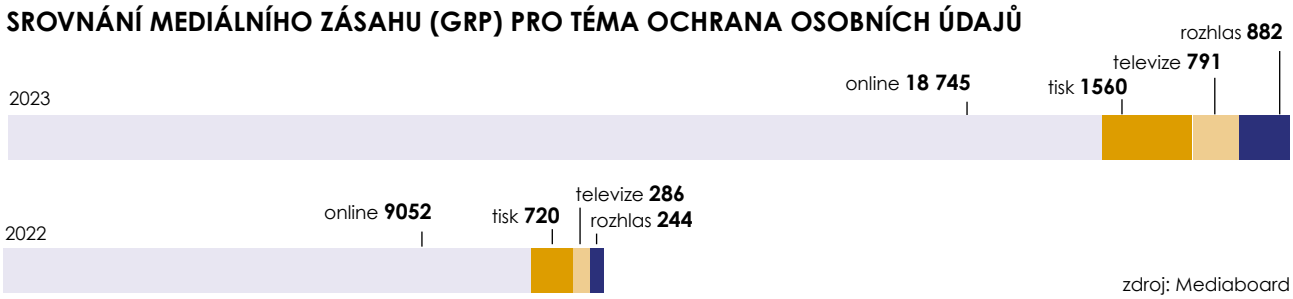
POČET TRANSAKCÍ PO MĚSÍCÍCH V LETECH 2020–2023



7. Média

V oblasti mediální komunikace Úřad na základě nezávislé analýzy vykázal výrazné posílení mediálního dopadu pro téma ochrany osobních údajů. V celkovém hodnocení s nárůstem o 113% oproti roku 2022. Stejně tak tomu bylo i v případě významného navýšení četnosti mediálně publikovaných informací o tématu ochrany osobních údajů.

SROVNÁNÍ MEDIÁLNÍHO ZÁSAHU (GRP) PRO TÉMA OCHRANA OSOBNÍCH ÚDAJŮ



zdroj: Mediaboard

Milníky roku 2023

COOKIES

V roce 2023 významně narostl počet rozhodnutí Úřadu, která se týkala zpracování osobních údajů prostřednictvím souborů cookies. Úřad k tomuto kroku přistoupil, neboť někteří správci nedostatečně reagovali na vytýkací dopisy, které Úřad v této souvislosti zasílal s konkrétními vytýkanými nedostatky. Úřad se na tuto problematiku bude dále zaměřovat, protože zpracování osobních údajů prostřednictvím souborů cookies pro běžného uživatele internetu probíhá skrytě na pozadí, a je tak potencionálně velmi nebezpečné. Více v kapitole Výzva roku.

CEF 2023

Úřad se v roce 2023 opětovně zapojil do koordinované dozorové akce evropských úřadů (CEF), jejímž iniciátorem je Evropský sbor pro ochranu osobních údajů (EDPB). Tématem akce byla úloha a postavení pověřenců pro ochranu osobních údajů. V rámci této akce oslovil Úřad všechna ministerstva. Více v kapitole Dozorová činnost a další odborné aktivity.

EVROPSKÝ NÁVRH PROCESNÍHO NAŘÍZENÍ DOPLŇUJÍCÍHO GDPR

V červenci 2023 představila Evropská komise návrh nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679. Má se jednat o reakci na dosavadní zkušenosti s aplikací GDPR v přeshraničních případech a jeho dosud nejvýznamnější legislativní doplnění. Kromě podrobného nastavení procesních pravidel a lhůt pro součinnost dozorových úřadů mají být výrazně posílena procesní práva stěžovatelů a vyšetřovaných stran. Z vyhodnocení vyplynulo, že návrh vychází z takové koncepce řízení, která bude obtížně slučitelná s dosavadní praxí a principy českého správního práva. Úřad se kromě toho obává zvýšení administrativní zátěže a celkové těžkopádnosti vedených přeshraničních řízení. Ke schválení návrhu dojde patrně již v roce 2024. Více v podkapitole Unijní legislativa.

RÁMEC OCHRANY SOUKROMÍ MEZI EU A USA

10. července 2023 vstoupilo v platnost rozhodnutí Evropské komise o odpovídající ochraně osobních údajů poskytované Rámcem ochrany soukromí mezi EU a USA. Toto rozhodnutí uznává, že úroveň ochrany osobních údajů předávaných do Spojených států amerických společnostem účastnícím se programu Rámec ochrany soukromí (Data Privacy Framework) je srovnatelná s úrovní ochrany osobních údajů v Evropské unii. Díky tomu vývozci údajů nemusejí vytvářet žádné zvláštní záruky pro předávání osobních údajů do USA těmto společnostem. Více v kapitole Vývoj v oblasti předávání údajů do třetích zemí.

NÁVRH ZÁKONA O DIGITÁLNÍ EKONOMICE

V druhé polovině roku začalo Ministerstvo průmyslu a obchodu intenzivně připravovat implementaci nařízení o digitálních službách (Digital Services Act, DSA), části aktu o správě dat (Data Governance Act, DGA) a zpřesnění regulace šíření obchodních sdělení do českého právního řádu pod názvem zákon o digitální ekonomice. Uvedené představuje jednu z nejvýznamnějších nových regulací elektronického obchodu. Hlavním dozorovým úřadem bude Český telekomunikační úřad; Úřad s ním však bude spolupracovat zejména na poli dozoru elektronické reklamy. Více v kapitole Národní legislativa.

NAŘÍZENÍ O PŘEDCHÁZENÍ POHLAVNÍMU ZNEUŽÍVÁNÍ DĚTÍ A BOJ PROTI NĚMU

Úřad v roce 2023 odmítl návrh Evropské komise na dvouleté prodloužení účinnosti prozatímního nařízení Evropského parlamentu a Rady, kterým se mění nařízení Evropského parlamentu a Rady (EU) 2021/1232 o dočasné odchylce od některých ustanovení směrnice 2002/58/ES za účelem boje proti pohlavnímu zneužívání dětí online (CSA – Child Sexual Abuse), a to na základě plošnosti a nepřiměřenosti zamýšlených opatření včetně celkového dopadu na ztrátu soukromí uživatelů internetu. Potřeba prodloužení účinnosti prozatímního nařízení byla způsobena tím, že nebyla dosud nalezena shoda na schválení návrhu stálého nařízení Evropského parlamentu a Rady, kterým se stanoví pravidla pro prevenci a boj proti pohlavnímu zneužívání dětí (CSAM). Proti jeho schválení se na české straně postavila řada resortů (včetně ÚOOÚ) a na půdě Rady EU některé členské státy. Více v kapitole Unijní legislativa.

PRAVOMOCNÁ POKUTA ZA APLIKACI KARANTÉNA

Úřad udělil první pravomocnou pokutu za porušení předpisů upravujících ochranu osobních údajů v režimu tzv. trestněprávní směrnice, a to za neoprávněné zpracování osobních údajů osob, jimž byla v rámci opatření proti šíření onemocnění COVID-19 nařízena izolace Policií ČR v rámci databáze Karanténa. Více v kapitole Z rozhodnutí předsedy Úřadu.

Ochrana osobních údajů

VÝZVA ROKU 2023 – SPRÁVNÍ TRESTÁNÍ A DOBRÁ PRAXE V OBLASTI COOKIES

Rok 2023 byl pro Úřad mimo jiné ve znamení zesílené dozorové činnosti ve vztahu ke zpracování osobních údajů prostřednictvím tzv. cookies souborů.

Cookies soubory jsou datové informace ukládané do koncových zařízení subjektů údajů nebo sloužící k získání přístupu k údajům uloženým v koncových zařízeních subjektů údajů ve smyslu § 89 odst. 3 zákona o elektronických komunikacích. Tyto soubory mohou sloužit buď k řádnému chodu internetových stránek, nebo mohou sloužit ke sběru informací o uživatelích pro statistické, analytické, marketingové či jiné účely. Cookies soubory obsahují jedinečné identifikátory či jiné informace, které jsou osobními údaji ve smyslu obecného nařízení, a proto spadá tato problematika do působnosti Úřadu.

Zpracování osobních údajů prostřednictvím cookies souborů vnímá Úřad jako potenciálně velmi problematické, což je dáno několika důvody. Předně si subjekty údajů často nemusí být vědomy, že prostřednictvím cookies souborů dochází ke zpracování osobních údajů. Je to záležitost vyžadující určité technické povědomí, navíc se tak děje na pozadí a pro návštěvníky webových stránek v zásadě „neviditelně." Běžný uživatel internetu si ani nemusí být nijak vědom, že jsou do jeho počítače nahrány tyto soubory, a i kdyby si toho byl vědom, může být mimo jeho uživatelské znalosti rozlišit, o jaké cookies soubory se jedná, k čemu slouží, jaké údaje o něm shromažďují, po jak dlouhou dobu, a kdo všechno má k těmto údajům přístup. Je to pak právě tato neviditelnost zpracování osobních údajů prostřednictvím cookies, jež vyžaduje o to větší pozornost Úřadu.

Zpracování osobních údajů prostřednictvím cookies souborů je v rámci Evropské unie upraveno směrnicí o soukromí a elektronických komunikacích. Ta vyžaduje, aby provozovatelé internetových platforem získali od návštěvníků výslovný souhlas s využíváním cookies pro zpracování osobních údajů, a to na základě tzv. principu opt-in. Výjimku představují pouze tzv. technické cookies, které jsou nezbytné pro správnou funkci internetových aplikací.

V českém zákoně o elektronických komunikacích však před jeho novelizací do konce roku 2021 nebyl požadavek na výslovný souhlas zcela přesně formulován a provozovatelé, stejně jako odborná veřejnost, jej často vykládali v opačném smyslu, tedy jako princip tzv. opt-out. Tedy, co není výslovně odmítnuto, je odsouhlaseno.

Schválením novely zákona o elektronických komunikacích byly s účinností k 1. lednu 2022 odstraněny jakékoli nejasnosti, provozovatelé internetových platforem tak mohou shromažďovat osobní údaje od návštěvníků pouze na základě jejich prokazatelného souhlasu, podle principu opt-in.

Úřad se touto problematikou zvýšenou měrou zabýval už v předcházejícím období, kdy se zaměřoval především na osvětovou činnost, přičemž těžiště jeho činnosti bylo v rámci vytýkacích dopisů. Množství správců však k nápravě přistoupilo nedostatečně, ve výjimečných případech dokonce vůbec, Úřad tedy v roce 2023 přistoupil k vydávání rozhodnutí o pokutě, a to většinou v kombinaci s ukládáním konkrétních opatření k odstranění nedostatků, aby bylo dosaženo souladného stavu s obecným nařízením. Při ukládání pokut Úřad postupuje zcela v intencích pokynů EDPB 4/2022 o výpočtu administrativních pokut podle GDPR.

Správní řízení nicméně nejsou jedinou aktivitou, kterou Úřad na poli cookies provádí. V roce 2023 vydal podstatně rozšířené „otázky a odpovědi" pro oblast cookies souborů. Též se zúčastnil evropského workshopu pořádaného EDPB, a to právě se zaměřením na cookies, kde Úřad úspěšně prezentoval nástroje vlastní provenience, jež užívá v rámci šetření zaměřených na cookies.

Úřad bude i nadále pokračovat v šetřeních v oblasti cookies, nicméně již po prvním roce udělování pokut v této oblasti lze shledat, že správci zaregistrovali aktivitu Úřadu a například možnost odmítnout udělení souhlasu v první vrstvě cookie lišty se již stává standardem. Totéž platí pro plnění informační povinnosti, neboť ubývá případů „neklasifikovaných" cookies souborů či informací poskytovaných jen v anglickém jazyce.

Nejčastější pochybení v souvislosti s cookies

Na základě provedených šetření identifikoval Úřad jako nejčastější především následující nedostatky:

1) **Nahrávání cookies souborů do koncových zařízení uživatelů internetových stránek, a to bez jejich souhlasu ve smyslu § 89 odst. 3 zákona o elektronických komunikacích**

   Jedno ze základních pravidel, které platí nejen v oblasti cookies, zní, že každé zpracování osobních údajů musí být prováděno zákonným způsobem. V kontextu cookies souborů to znamená, že aby bylo zpracování osobních údajů prostřednictvím cookies zákonné, musí ve smyslu § 89 odst. 3 zákona o elektronických komunikacích každý, kdo hodlá používat nebo používá sítě elektronických komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních uživatelů (tedy i prostřednictvím cookies), získat od těchto uživatelů předem prokazatelný souhlas s rozsahem a účelem jejich zpracování. Jediná výjimka z této povinnosti se týká cookies souborů často označovaných jako technické, jež slouží pro technické ukládání nebo přístup výhradně pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací, nebo jsou-li nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem.

   V případě nedodržení této povinnosti shledával Úřad přestupek spočívající v nezákonném zpracování osobních údajů, konkrétně porušení zásady zákonnosti podle čl. 5 odst. 1 písm. a) obecného nařízení. Prozatím všechny pravomocné pokuty (včetně obou nejvyšších pravomocných pokut, a to pokut ve výši 898 000 Kč a 602 000 Kč) byly uděleny i v souvislosti s tímto porušením, jakkoliv se nejednalo o jediné porušení, pro které byly uděleny.

2) Nedostatky souhlasu se zpracováním osobních údajů

Obecné nařízení ve svém čl. 4 bodu 11) stanoví základní požadavky na souhlas, kterým se rozumí „jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů." Podmínky vyjádření souhlasu jsou dále rozvedeny v čl. 7 obecného nařízení.

Pokud nejsou tyto přísné požadavky naplněny, souhlas se zpracováním osobních údajů může ve svém důsledku být neplatný a správci (provozovateli webu) pak zpravidla nebude svědčit právní titul ke zpracování. Taková situace zakládá porušení čl. 6 obecného nařízení, které stanoví, že zpracovávat osobní údaje lze pouze na základě některého z právních titulů uvedených v tomto ustanovení.

V praxi se Úřad setkal například se situací, kdy souhlas neobsahoval žádné informace o tom, že po jeho udělení dojde i k nahrání cookies souborů třetích stran, pouze obsahoval informace o cookies souborech správce (tedy cookies souborech první strany). Tento souhlas musel být vyhodnocen jako neinformovaný a bylo shledáno porušení čl. 6 odst. 1 obecného nařízení, neboť správci nesvědčil ani žádný jiný titul pro takové zpracování osobních údajů.

3) Nedostatečné plnění informační povinnosti

Velmi častým problémem jsou nedostatky v plnění informační povinnosti. Právě s ohledem na to, jak je zpracování osobních údajů prostřednictvím cookies souborů pro uživatele internetu (subjekty údajů) hůře představitelné (či až „neviditelné"), přikládá Úřad plnění informační povinnosti především ve smyslu čl. 12, 13 obecného nařízení mimořádný význam. Aby těmto povinnostem dostál, musí správce podle čl. 12 obecného nařízení poskytnout informace uživatelům internetových stránek stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků.

Poskytnutí povinných informací (přičemž je nutné uvést, že v zásadě poskytnutí všech informací uvedených v čl. 13 je nutno hodnotit jako povinné) pak musí zahrnovat všechny cookies, lhostejno zda se jedná o technické cookies soubory či nikoliv. Ostatně i technické cookies soubory zpracovávají osobní údaje a § 89 odst. 3 zákona o elektronických komunikacích zakotvuje výjimku stran technických cookies souborů toliko stran souhlasu s jejich nahráním. Není pak v rozporu s obecným nařízením, pokud není informace například o účelu zpracování poskytnuta jednotlivě pro každý soubor cookies, ale je poskytnuta dostatečná informace pro více konkrétně uvedených cookies souborů najednou (typicky rozdělení cookies souborů na statistické či analytické). Za této situace však musí být informace dostatečně konkrétní, aby byla aplikovatelná na každou cookie, a vždy je nutno trvat na tom, aby správce poskytl seznam všech cookies, jež jsou do koncových zřízení nahrávána.

Případy, které Úřad trestal, zahrnovaly jednak situace, kdy správce některý z cookies souborů neuvedl vůbec, informace o cookies souborech nebyly úplné, jak vyžaduje čl. 13 obecného nařízení, nebo nebyly v českém jazyce, což bylo v rozporu s požadavky čl. 12 odst. 1 obecného nařízení. V jednom případě byly informace o 58 cookies souborech uvedeny v anglickém jazyce. Obdobným problémem je, že správci účel zpracování pro některé cookies soubory definovali jako „neklasifikované" či „nevyřízeno". Takové popsání účelu v žádném případě nemůže obstát.

Specifickým problémem jsou tzv. neklasifikované cookies soubory. Některé typy cookie lišt (většinou dočasně) nedovedou zařadit určité cookies soubory, které pak jsou zařazovány ručně správcem, či až v následující aktualizaci lišty. Je tak vytvořena zvláštní kategorie cookies souborů (zvaná neklasifikované či nezařazené), které obvykle neobsahují žádný popisek (nebo je z něj zřejmé, že jsou teprve ve stádiu klasifikace) a také je většinou nelze samostatně povolit či odmítnout. Tyto cookies soubory tak postrádají ve svém důsledku jakoukoli informaci o účelu, což je v rozporu s čl. 13 odst. 1 písm. c) obecného nařízení.

4) **Nemožnost (či výrazné zkomplikování možnosti) odvolat souhlas se zpracováním osobních údajů prostřednictvím cookies**
Nedílnou součástí podmínek udělení souhlasu je druhá strana téže mince, a to možnost souhlas odvolat, přičemž jak stanoví čl. 7 odst. 3 obecného nařízení: „Odvolat souhlas musí být stejně snadné jako jej poskytnout."

Praxe ukázala případy, kdy nebylo možné takovým způsobem souhlas odvolat, neboť nebylo dostatečně snadné nalézt na internetové stránce správce nastavení cookies souborů poté, co již uživatel prostřednictvím cookie lišty souhlasil se zpracováním osobních údajů. Jako příklad best-practice lze v této souvislosti uvést možnost vyvolání vhodné nabídky prostřednictvím odkazu na patičce webu.

5) **Umístění možnosti volby pro „souhlas" a „nesouhlas" se zpracováním osobních údajů prostřednictvím cookies souborů do různých vrstev v rámci cookie lišty**
Taková praxe se nazývá Deceptive Design Patterns / Klamavý designový vzor či Dark Patterns. Účelem takového designu (nastavení cookie lišty) je návštěvníkovi internetové stránky podbízet určitou volbu, jež je preferovanou volbou správce. V kontextu cookies souborů je návštěvníkovi stránky takovýmto designem podbízeno, aby zvolil možnost souhlasu se zpracováním osobních údajů prostřednictvím cookies.

Jak však Úřad konstantně rozhoduje, takové nastavení cookie lišty na webové stránce *„neoprávněně ztěžuje subjektu údajů možnost odmítnout netechnické cookies soubory, a to tím, že v první vrstvě cookie lišty se zobrazuje pouze tlačítko umožňující udělení souhlasu se zpracováním osobních údajů prostřednictvím netechnických souborů cookies […], aniž by se současně zobrazila možnost netechnické cookies soubory stejně jednoduchým způsobem (tedy jedním krokem) neakceptovat. Zjevná nerovnost možností udělit a odmítnout udělit souhlas se zpracováním osobních údajů, konkrétně situace, kdy je účastníkem řízení jako správcem předkládán souhlas se zpracováním osobních údajů jako primární a v první vrstvě jediná viditelná možnost, a odmítnutí udělení takového souhlasu je v zásadě skryto do vrstvy druhé (přičemž subjekt údajů si ani nemusí být vědom, že v další vrstvě bude mít možnost odmítnout udělit souhlas, neboť první vrstva toto nijak neindikuje), porušuje podmínku souhlasu ve smyslu čl. 4 bodu 11 nařízení (EU) 2016/679, tedy podmínku, aby souhlas byl svobodný. Pro tento nedostatek nelze takto udělený souhlas se zpracováním osobních údajů považovat za platný. Na podporu uvedeného závěru lze analogicky použít čl. 7 odst. 3 nařízení (EU) 2016/679, podle kterého odvolat souhlas musí být stejně snadné, jako jej poskytnout, který je nutno obdobně aplikovat i na okamžik, kdy je souhlas udělován. Tedy i nastavení cookie lišty musí být provedeno tak, aby udělení a odmítnutí udělení tohoto souhlasu bylo stejně snadné, což v situaci, kdy je souhlas vyjadřován výběrem příslušné varianty v rámci cookie lišty, vyžaduje zobrazení obou těchto volitelných variant současně, tedy v téže úrovni cookie lišty."*

Úřad pak v rámci rozhodování o cookies neukládá pouze pokuty za shledaná porušení obecného nařízení, ale zároveň ukládá konkrétní nápravná opatření, aby docílil stavu souladného s obecným nařízením.

Základní rady pro správce i uživatele

Zkušenosti Úřadu lze zobecnit do několika základních rad pro správce i pro uživatele internetu.

Základní rady pro provozovatele internetových stránek (tedy správce osobních údajů)

1) **Je třeba dávat pozor na „ready-made" či obdobná řešení**
Odpovědnost za zpracování osobních údajů v rámci internetových stránek má jejich provozovatel, přičemž do tohoto zpracování patří i zpracování osobních údajů prostřednictvím cookies souborů. Pokud např. provozovatel internetového obchodu zakoupí řešení internetových stránek od třetí společnosti či je třetí společnost spravuje, není odpovědnost za zpracování osobních údajů přenesena na tuto společnost. Ta je stále na straně

provozovatele internetového obchodu. Úřad si je vědom případů, kdy tyto třetí společnosti dodávají texty týkající se zpracování osobních údajů prostřednictvím internetové stránky, avšak tyto texty jsou obecné, v zásadě nereflektující úpravy provedené např. na žádost provozovatele internetového obchodu, nehledě na (zpravidla nikoli vysokou) kvalitu takovýchto textů z pohledu požadavků obecného nařízení.

Je třeba pamatovat na to, aby informace poskytované v souladu s čl. 13 obecného nařízení reflektovaly skutečné zpracování probíhající na konkrétní internetové stránce, tj. aby popisovaly reálně probíhající zpracování a všechny cookies soubory využívané internetovou stránkou. Lze jen doporučit, aby správce sám využil některý z volně dostupných nástrojů na analýzu souborů cookies, a přesvědčil se, zda jsou informace uváděné na internetové stránce v souladu s tím, jaké cookies soubory jsou skutečně využívány.

2) **Nutnost uzavřít zpracovatelskou smlouvu v určitých případech**
S výše uvedeným úzce souvisí nutnost v některých případech uzavřít zpracovatelskou smlouvu ve smyslu čl. 28 obecného nařízení. V praxi se bude například jednat o případy, kdy třetí společnost zcela spravuje internetové stránky správce osobních údajů, včetně hostingu. Tato smlouva by měla zahrnout i zpracování osobních údajů prostřednictvím cookies.

3) **Nutnost plnění informační povinnosti i při využívání cookies souborů třetích stran**
Na základě zkušeností Úřadu je třeba upozornit na to, že při využívání cookies souborů třetích stran (samozřejmě za předpokladu, že jsou splněny všechny podmínky obecného nařízení pro takové zpracování) je stále povinnost plnit informační povinnost na straně provozovatele internetové stránky, na níž jsou takové cookies soubory nasazeny. Provozovatel internetové stránky bude i v takové situaci zpravidla správcem osobních údajů. Nelze pak zcela spoléhat na to, že pouhé překopírování informací uvedených třetí stranou bude dostačující z hlediska požadavků čl. 13 obecného nařízení.

4) **Pokud web cílí i na zahraniční klientelu, je nutné plnit informační povinnost i v příslušném jazyce**
Pokud nabízí webová stránka jazykovou mutaci, například z toho důvodu, že cílí na zahraniční klientelu, je nutné uvést všechny potřebné informace týkající se zpracování osobních údajů i v příslušném jazyce.

5) **I technické cookies soubory zpracovávají osobní údaje**
I technické cookies soubory v sobě obsahují jedinečné identifikátory, tedy osobní údaje. Na to je nutné pamatovat v rámci plnění informační povinnosti.

Základní rady pro uživatele internetu (tedy subjekty údajů)

1) **Pokud web neinformuje o zpracování osobních údajů prostřednictvím cookies, je nepravděpodobné, že osobní údaje takovým způsobem skutečně nezpracovává**
Pokud internetová stránka při prvním vstupu na ni neinformuje o zpracování osobních údajů prostřednictvím cookies souborů (např. prostřednictvím cookie lišty), není pravidlem, že by nedocházelo ke zpracování osobních údajů prostřednictvím cookies, ke kterým je třeba souhlasu s jejich nahráním do koncových zařízení. Zkušenosti Úřadu ukazují, že ve velké části případů k takovému zpracování osobních údajů dochází.

2) **I při zpracování osobních údajů prostřednictvím cookies souborů má subjekt údajů práva podle obecného nařízení**
Zpracování osobních údajů prostřednictvím cookies souborů je stále zpracování jako každé jiné a subjekt údajů má právo např. na informace (čl. 13 příp. 14 obecného nařízení), právo na přístup (čl. 15) či právo na výmaz (čl. 17).

3) **Práce s prohlížeči**
Internetové prohlížeče v sobě standardně obsahuji vývojářské nástroje, prostřednictvím

kterých mohou uživatelé sami rychle zjistit, jaké cookies soubory určitá webová stránka nahrává do jejich zařízení.

Doporučuje se používání prohlížečů, které mají zabudovanou ochranu proti sledování, spočívající například v blokování určitých druhů cookies, k jejichž nahrání do koncových zařízení je třeba souhlasu. Řada prohlížečů také obsahuje ochranu proti tzv. fingerprintingu (shromažďování dat o softwaru a nastavení zařízení prostřednictvím prohlížeče uživatele internet). Lze doporučit tyto funkce ponechat zapnuté a používat prohlížeče, které je podporují. Je vhodné zvážit i zákaz cookies souborů třetích stran, mazat je při každém zavření prohlížeče či zvolit nastavení, aby nebyla ukládána data za účelem přizpůsobení reklamy. Vhodné může být i využití anonymních režimů prohlížečů a instalace doplňků pro ochranu soukromí z důvěryhodných zdrojů.

ZÁVĚRY Z KONTROL

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

Důsledky opomenutí zásady „privacy by design“

Úřad v rámci kontroly zjistil, že kontrolovaná osoba poskytovala doplněk služeb platformy zajišťující provozování e-shopů. Pomocí tohoto doplňku mohl zákazník platformy (provozovatel e-shopu) vidět statistiky týkající se návštěvnosti a chování svých zákazníků, kteří e-shop navštívili. Tyto statistiky vytvářela kontrolovaná osoba z dat stažených z platformy, a následně je poskytovala provozovatelům e-shopů.

Pro zajištění fungování doplňku poskytla platforma kontrolované osobě exportní URL adresy, pomocí kterých kontrolovaná osoba mohla stahovat z platformy data týkající se konkrétního e-shopu, a na základě smlouvy uzavřené s provozovatelem e-shopu tak zajišťovala fungování doplňku a vykreslování statistik a přehledů. Aby bylo možné data stáhnout, měla kontrolovaná osoba povinnost se identifikovat. V takovém případě algoritmus vyhodnotil, že se jedná o tuto osobu, a umožnil stažení jen těch dat, ke kterým měla mít kontrolovaná osoba přístup.

Pokud následně provozovatel e-shopu ukončil smlouvu s kontrolovanou osobou a o tomto kroku neinformoval platformu, nebylo nijak zajištěno vzájemné informování platformy a kontrolované osoby, a exportní URL tak nebyla zablokována. O tom však provozovatel e-shopu nevěděl. Pokud odinstalování doplňku oznámil provozovatel e-shopu naopak pouze platformě, nedozvěděla se o tomto kroku zase kontrolovaná osoba a nadále v seznamu exportních adres tuto URL ponechávala.

Při automatickém stahování byla identifikace zajištěna automaticky, avšak při ručním zásahu (stahování) neodhalilo nastavené zabezpečení nestandardní chování pro případ, že řádek pro identifikaci zůstal prázdný. V takovém případě byla stažena všechna data ze všech URL adres, kterými kontrolovaná osoba disponovala. Stačila tedy jedna lidská chyba, když se při testování v rámci finálního přechodu na novou technologii kontrolovaná osoba v příslušném řádku neidentifikovala (ponechala jej prázdný), a došlo ke stažení dat zákazníků, kteří si již doplněk odinstalovali (ale kontrolovaná osoba o tom nevěděla a nevyřadila tak jejich exportní URL ze svého seznamu), i zákazníků, u kterých zase na druhou stranu platforma nevěděla, že s kontrolovanou osobou ukončili spolupráci, a exportní URL proto nezablokovala.

Kontrolovaná osoba ani platforma problém v danou chvíli nezjistily. Porušení zabezpečení osobních údajů ohlásila platforma až po několika týdnech od incidentu, na základě upozornění provozovatelů e-shopů, kteří v notifikacích ve svých účtech zjistili podezřelé stažení dat. Následně ohlásilo porušení zabezpečení osobních údajů několik desítek dalších provozovatelů e-shopů.

Po zjištění incidentu platforma ukončila s kontrolovanou osobou spolupráci.

Kontrolou bylo zjištěno, že kontrolovaná osoba při zpracování (exportu) osobních údajů zákazníků celkem 115 provozovatelů e-shopů, se kterými již měla ukončený smluvní vztah, poru-

šila čl. 6 odst. 1 obecného nařízení, neboť pro předmětné zpracování (kterým bylo stažení osobních údajů zákazníků) neměla řádný právní titul podle čl. 6 odst. 1 obecného nařízení. Úřad v rámci kontroly zjišťoval i to, zda byla tato neoprávněně zpracovaná data v mezidobí smazána, což kontrolovaná osoba neprodleně po incidentu učinila.

Uvedené zásadním způsobem ukazuje důležitost principu „privacy by design", tedy principu záměrné ochrany osobních údajů, formulovaného v čl. 25 odst. 1 obecného nařízení. Ten stanoví, že s přihlédnutím ke stavu techniky, nákladům na provedení, k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jejichž účelem je provádět zásady ochrany údajů účinným způsobem a začlenit do zpracování nezbytné záruky tak, aby splnil požadavky obecného nařízení a ochránil práva subjektů údajů. Jinými slovy je nutno ochranu osobních údajů nastavit ještě v době před započetím zpracování osobních údajů.

Kontrola zpracovatelských smluv uzavíraných obcemi

Úřad provedl kontroly smluv o zpracování osobních údajů u 7 obcí z 5 různých krajů České republiky. Jednalo se o 5 malých obcí s počtem obyvatel do 1000 a 2 středně velké obce s počtem obyvatel do 3000. Bylo posuzováno 22 zpracovatelských smluv, resp. 20 (ve 2 případech nebyla smlouva vůbec uzavřena). Žádná ze smluv nebyla vyhodnocena jako zcela správná, a pouze 3 smlouvy obsahovaly méně závažná porušení.

Při posuzování souladu každého smluvního vztahu s obecným nařízením hodnotil úřad celkem 13 kritérií odpovídajících požadavkům čl. 28 obecného nařízení. Ze všech hodnocených kritérií byla téměř polovina chybně či absentovala zcela. Nejvíce chyb bylo ve smlouvách obsaženo v části, kde je třeba upravit přijetí vhodných opatření podle čl. 32 obecného nařízení. Více bylo chybováno i v úpravě podmínek pro zapojení dalšího zpracovatele či umožnění auditů a inspekcí, dále také v úpravě náležitostí podle čl. 28 odst. 3 věta první obecného nařízení.

Bylo zjištěno, že zpracovatelem byl v drtivé většině poskytovatel IT služeb, software a hardware (18), dále knihovna (2) a dále poskytovatelé služeb souvisejících s vodovody a odečty spotřeb vody a tepla (2). Z celkové chybovosti ve vztahu k tomu, že většina zpracovatelů byly společnosti poskytující IT služby, vyplynulo, že se obce jako do jisté míry slabší strana takového vztahu ne zcela vhodně spoléhají na odbornost a erudici těchto smluvních partnerů. Někteří poskytovatelé IT služeb uzavřeli smlouvy s více obcemi a bylo poměrně překvapivé, že různé verze zpracovatelských smluv s jedním zpracovatelem vykazovaly různé druhy (co do typu a závažnosti) porušení. V tomto směru lze jen doporučit, aby správci při uzavírání zpracovatelských smluv striktně vyžadovali naplnění čl. 28 obecného nařízení.

Jako pomůcku pro správné nastavení vztahů mezi správcem a zpracovatelem lze doporučit například Prováděcí rozhodnutí Komise (EU) 2021/915 ze dne 4. června 2021 o standardních smluvních doložkách mezi správci a zpracovateli podle čl. 28 odst. 7 obecného nařízení.

Úřad pokračuje v kontrolách zpracovatelským smluv uzavíraných v rámci veřejného sektoru, přičemž v roce 2023 zahájil kontrolu všech krajů. Cílem Úřadu je zmapovat využívání zpracovatelských smluv a jejich kvalitu s výhledem na vytvoření materiálu, který dotčeným osobám v této problematice může pomoci se orientovat.

Kontrola zpracování osobních údajů v Portálu občana

Již ve Výroční zprávě 2022 Úřad informoval o koordinované dozorové akci (CEF 2022), jejímž iniciátorem byl Evropský sbor pro ochranu osobních údajů (EDPB), a která probíhala napříč evropskými dozorovými úřady. V návaznosti na její první fázi byla Úřadem zahájena kontrola Portálu občana jakožto transakční části Portálu veřejné správy. Kontrolu Úřad provedl ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB).

S ohledem na povahu a rozsah zpracování osobních údajů se kontrola zaměřila na provedené posouzení vlivu na ochranu osobních údajů (tzv. DPIA). Bylo shledáno, že absentuje materiální posouzení nezbytnosti a přiměřenosti operací z hlediska účelů (požadavek podle čl. 35 odst. 7 obecného nařízení). V předloženém posouzení vlivu na ochranu osobních údajů také nebyla uvedena opatření přijatá ke snížení ohodnocených rizik (požadavek podle čl. 35 odst. 7 písm. d) obecného nařízení). Ve vztahu k posouzení vlivu na ochranu osobních údajů navíc nebylo prokázáno vyžádání posudku pověřence pro ochranu osobních údajů (povinnost daná zněním čl. 35 odst. 2 obecného nařízení) a kontrolovaná osoba též nedostatečně prováděla přezkum posouzení vlivu na ochranu osobních údajů (tj. porušila povinnost vyplývající z čl. 35 odst. 11 obecného nařízení).

Dále se kontrola zaměřila na uzavřené zpracovatelské smlouvy, zejména na smlouvu upravující vztah a povinnosti mezi Ministerstvem vnitra v roli správce osobních údajů a Národní agentury pro komunikační a informační technologie (NAKIT) v roli zpracovatele. Kontrolou bylo konstatováno porušení povinností stanovených čl. 28 odst. 3 obecného nařízení, neboť z předložených dokumentů nevyplývala úprava některých oblastí, které obecné nařízení předpokládá (např. jasně stanovený předmět a doba trvání zpracování, jeho účel a povaha, typ zpracovávaných osobních údajů, dále nebylo dostatečně smluvně ošetřeno zapojení dalšího zpracovatele do zpracování, nebylo též zohledněno provozování Portálu občana v rámci cloudového řešení). Pochybení byla způsobena zejména přílišnou obecností předložené zpracovatelské smlouvy, která dostatečně nezohlednila specifika Portálu občana.

Náležitosti souhlasu se zpracováním osobních údajů

Úřad provedl kontrolu zaměřenou na nastavení souhlasu se zpracováním osobních údajů pro marketingové účely u společnosti s ručením omezeným.

Společnost (správce osobních údajů) umožňovala provádět objednávky zboží poštou, a to prostřednictvím objednávkových kupónů. Svým podpisem objednávky však zákazník zároveň souhlasil se zpracováním osobních údajů pro účely marketingu, přičemž nebylo možné provést objednávku bez udělení tohoto souhlasu.

Úřad v rámci kontroly zjistil, že se jednalo o systémově špatné nastavení udělování souhlasu se zpracováním osobních údajů, navíc zároveň zjistil, že v případě, kdy by zákazník hodlal využít svého práva na opravu osobních údajů (práva na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se týkají subjektu údajů), mohl učinit prostřednictvím společností nabízený formulář označený jako „Vyjádření souhlasu o změnu údajů v adrese“. Nedílnou součástí tohoto formuláře byl, překvapivě pro subjekty údajů, souhlas se zpracováním osobních údajů pro účely marketingu.

Popsanou praxi vyhodnotil Úřad jako v rozporu s podmínkami uvedenými v čl. 4 bod 11 a v čl. 7 odst. 4 obecného nařízení, tedy tak, že souhlas se zpracováním osobních údajů nebyl svobodný, a tudíž nebyl platný. V důsledku toho Úřad dále shledal, že společnost nedisponovala (ve vztahu k subjektům údajů, kteří svůj souhlasu udělili neplatně) platným právním titulem pro zpracování osobních údajů pro marketingové účely. Ani jeden z dokumentů navíc neobsahoval informaci o právu udělený souhlas kdykoliv odvolat, což založilo další porušení obecného nařízení.

Úřad dále vyhodnotil, že společnost porušila též povinnost informovat subjekty údajů o právním základů zpracování osobních údajů.

Podmínky kladené ze strany obecného nařízení na kvalitu souhlasu jsou poměrně přísné, nevybočují však z toho, jak je institut souhlasu chápán v českém právním řádu. Přesto jeho užití v českém prostředí vede často k problémům. Jako praktický návod pro zajištění souladu s obecným nařízením při užívání právního titulu souhlasu vydal Evropský sbor pro ochranu osobních údajů (EDPB) dne 4. května 2020 Pokyny č. 05/2020 k souhlasu podle nařízení 2016/679.

Ničení záznamů odposlechů

Úřad se v rámci kontroly realizované u Policie ČR zaměřil na dodržování povinností při zpracování osobních údajů v souvislosti s uchováváním záznamů odposlechů, vyplývající z § 88 odst. 7 trestního řádu, který stanoví, že: „*Pokud při odposlechu a záznamu telekomunikačního provozu nebyly zjištěny skutečnosti významné pro trestní řízení, je policejní orgán po souhlasu soudu a v přípravném řízení státního zástupce povinen záznamy bezodkladně zničit po třech letech od pravomocného skončení věci.*“ Z hlediska ochrany osobních údajů je nutno upozornit, že součástí záznamu odposlechu může být i hovor nesouvisející s trestní věcí, kvůli níž je odposlech nasazen, a zpracování osobních údajů se proto dotýká širšího okruhu osob.

Úřad identifikoval případy, ve kterých mělo být podle § 88 odst. 7 trestního řádu postupováno, k včasnému výmazu však nedošlo, a ačkoli v některých případech bylo postupováno v souladu s tímto ustanovením trestního řádu, je zřejmé, že tato skutečnost je zcela závislá na konkrétním zpracovateli spisu, resp. jeho vedoucím pracovníkovi. Ačkoliv trestní řád nestanoví jasná kritéria, v době kontroly interní předpis kontrolované osoby bez dalšího odkazoval na ustanovení trestního řádu a neexistovala závazná metodika, která by poskytovala dostatečná vodítka pro individuální posouzení jednotlivých případů. Neexistovala žádná ústřední evidence či nástroj umožňující plošný dohled nad postupem podle § 88 odst. 7 trestního řádu. Zřejmá nejednotnost v postupu napříč útvary Policie ČR a nedostatky či zmatečnost odpovědí kontrolované osoby byly kontrolujícími v rámci kontroly vyhodnoceny nikoli jako pochybení konkrétního jednotlivce, ale jako důsledek absence relevantních ustanovení v závazných interních aktech řízení a metodického vedení.

Kontrolou proto bylo konstatováno, že Policie ČR nezavedla odpovídající opatření nezbytná pro posouzení, zda má dojít k návrhu na likvidaci podle § 88 odst. 7 trestního řádu, a nezbytná pro realizaci navazujících procesů, v důsledku čehož může docházet (a minimálně v jednotkách případů došlo) k opožděnému zničení záznamu odposlechu (resp. záznamu telekomunikačního provozu), při kterém nebyly zjištěny skutečnosti významné pro trestní řízení. Takový stav byl vyhodnocen jako porušení povinnosti stanovené § 32 odst. 2 písm. c) zákona č. 110/2019 Sb., tj. povinnosti přijmout technická a organizační opatření s cílem omezovat zpracování osobních údajů, které není nezbytné kvůli době jejich uložení.

Informační systém OČISTA

Informační systém OČISTA je poznatkovou databází, v níž Policie ČR shromažďuje poznatky a uchovává informace získané na úseku extremismu a toxikomanie, trestné činnosti mládeže, trestné činnosti páchané na mládeži, mravnostní trestné činnosti, trestné činnosti páchané v souvislosti s diváckým násilím. Tyto poznatky, včetně osobních údajů, jsou zpracovávány s cílem jejich využití při plnění úkolů Policie ČR v oblasti preventivních činností, odhalování latentní kriminality a objasňování trestných činů podle problematik.

Z ustanovení § 82 odst. 1 zákona o Policii České republiky vyplývá Policii ČR povinnost nejméně jednou za tři roky prověřit, jsou-li zpracovávané osobní údaje nadále potřebné pro plnění jejích úkolů v oblasti předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Ačkoli je tato povinnost promítnuta do interních předpisů, jimiž se Policie ČR při zpracování osobních údajů v informačním systému OČISTA řídí, a ačkoli je v rámci samotného informačního systému nastaven mechanismus pro automatické upozornění na uplynutí této lhůty a výmaz neaktualizovaného záznamu, Policie ČR v rámci kontroly nedoložila, zda ve stanovených lhůtách skutečně dochází k přezkumu potřebnosti dalšího zpracování osobních údajů po materiální stránce. O prověřování potřebnosti dalšího zpracování osobních údajů nejsou vedeny záznamy a informační systém OČISTA neumožňuje zobrazit historii záznamu, ze které by byl zřejmý způsob a rozsah aktualizace, po které je automaticky nastavena nová tříletá lhůta pro provedení přezkumu, aniž by bylo zřejmé, zda bylo dané zpracování osobních údajů fakticky přezkoumáno.

Kontrolou bylo konstatováno, že kontrolovaná osoba v rozporu s § 32 odst. 1 zákona

č. 110/2019 Sb. nepřijala taková technická a organizační opatření, aby doložila splnění svých povinností při ochraně osobních údajů, a to konkrétně povinnosti dané § 32 odst. 2 písm. c) zákona, tj. povinnosti přijmout technická a organizační opatření s cílem omezovat zpracování osobních údajů, které není nezbytné kvůli době jejich uložení.

Kontroly Vízového informačního systému

V roce 2023 Úřad ukončil dvě kontroly zpracování osobních údajů při vízovém procesu, resp. tedy dvě kontroly týkající se Vízového informačního systému. Úřadu je provádění nezávislého dohledu nad zákonností zpracování osobních údajů ve Vízovém informačním systému uloženo čl. 41 odst. 1 nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS), z ustanovení čl. 41 odst. 3 nařízení (ES) č. 767/2008 vyplývá povinnost provádění periodických kontrol. Z ustanovení čl. 43 odst. 9 nařízení Evropského parlamentu a Rady (ES) č. 810/2009 ze dne 13. července 2009 o kodexu Společenství o vízech (vízový kodex) dále vyplývá povinnost Úřadu monitorovat činnost externích poskytovatelů služeb.

Kontroly se zaměřily na zpracování osobních údajů při vyřizování žádostí o krátkodobá (schengenská) víza. Schengenská víza jsou jedním z prvků společné vízové politiky Evropské unie a umožňují státním příslušníkům třetích zemí pobývat na území Schengenského prostoru po dobu nepřesahující 90 dnů během jakéhokoliv období 180 dnů. Tato víza jsou zpravidla vydávána konzuláty členských států ve třetích zemích, přičemž postupy a podmínky jejich udělování upravuje zejména vízový kodex. Členské státy mohou při vízovém procesu využít služeb externích poskytovatelů, kteří provozují tzv. vízová centra. Při kontrolách byla realizována místní šetření na zastupitelských úřadech České republiky a též v příslušných vízových centrech, a to ve třech zemích mimo EU – ve Spojeném království Velké Británie a Severního Irska (Londýn), v Kazachstánu (Astana) a ve Spojených arabských emirátech (Abú Dhabí). Při výběru konkrétních zastupitelských úřadů Úřad přihlížel zejména ke statistikám (celkový počet podaných žádostí o víza, podíl zamítnutých žádostí), které Úřadu poskytuje Ministerstvo zahraničních věcí.

V rámci první kontroly, která byla provedena na tamním zastupitelském úřadu České republiky v Londýně, bylo na základě nepředložení příslušné dokumentace konstatováno, že kontrolovaná osoba (Ministerstvo zahraničních věcí) neprokázala plnění povinnosti stanovené čl. 43 odst. 11 vízového kodexu, tj. povinnosti provádět pravidelné kontroly na místě v prostorách externího poskytovatele služeb, přičemž vízovým kodexem je stanoveno, že tyto kontroly musí být prováděny nejméně každých devět měsíců. Bylo dále zjištěno dílčí pochybení v oblasti fyzického zabezpečení ve smyslu čl. 32 GDPR, a v dané souvislosti též konstatováno porušení povinnosti čl. 32 odst. 1 písm. d) GDPR, tj. povinnosti pravidelně sledovat, testovat, posuzovat a hodnotit účinnost technických a organizačních opatření pro zajištění bezpečnosti zpracování. Kontrolou bylo nadto zjištěno, že kontrolovaná osoba subjekty údajů dostatečně podrobným způsobem neinformovala o totožnosti správce ve smyslu čl. 37 odst. 1 písm. a) nařízení (ES) č. 767/2008. S ohledem na skutečnost, že pochybení v oblasti informování do určité míry navazuje mimo jiné na způsob vymezení správce Vízového informačního systému zákonem o pobytu cizinců na území České republiky, a jedná se tak o hlubší problém, inicioval Úřad v návaznosti na kontrolní zjištění diskuze o správci národní součásti Vízového informačního systému a v roce 2023 realizoval tři setkání se zástupci Ministerstva zahraničních věcí, Ministerstva vnitra a Policie ČR ve snaze napomoci nápravě neuspokojivého stavu.

Při druhé kontrole bylo místní šetření v roce 2023 realizováno na českých zastupitelských úřadech a ve vízových centrech v Astaně a v Abú Dhabí. Také v rámci této kontroly bylo konstatováno pochybení v oblasti plnění informační povinnosti, v rozsahu shora uvedeném. Plnění povinnosti dané čl. 43 odst. 11 vízového kodexu ve věci pravidelných kontrol v prostorách externího poskytovatele služeb bylo kontrolovanou osobou prokázáno pouze částečně, přičemž kontrolující museli zohlednit skutečnost, že externí poskytovatel služeb provozuje v dané

zemi pro zastupitelský úřad více než jedno vízové centrum. Také v rámci místních šetření realizovaných v roce 2023 Úřad během kontroly zjistil pochybení při plnění povinností v oblasti zabezpečení osobních údajů, stanovených čl. 32 GDPR, a to různé úrovně závažnosti. S ohledem na konkrétní zjištění Úřadu bylo v jednom případě na místě zahájeno okamžité prošetření věci zastupitelským úřadem České republiky a též externím poskytovatelem služeb provozujícím vízové centrum, nadto následně (ještě v průběhu kontroly) došlo k realizaci několika významných opatření (např. změny personálního charakteru vč. suspendace pracovníků, nově zavedená organizační i technická opatření) a o celé záležitosti byla informována též skupina místní schengenské spolupráce tak, aby mohly být příslušné postupy prověřeny též zastupitelskými úřady dalších členských států Schengenu. Lze shrnout, že kontrola konstatovala porušení povinností stanovených čl. 32 odst. 1 písm. a), b) a d) GDPR a čl. 43 odst. 8 a 11 písm. b), c) a d) vízového kodexu, přičemž některá opatření k nápravě zjištěného stavu byla kontrolovanou osobou přijata již v době kontroly, jak je shora popsáno.

ZÁVĚRY ZE SPRÁVNÍCH PRVOSTUPŇOVÝCH ROZHODNUTÍ

Obecní kamerový systém

Úřad prověřoval možné protiprávní zpracování osobních údajů, jehož se měla dopouštět obec, a to prostřednictvím kamerového systému monitorujícího veřejná prostranství nacházející se na jejím území. Součástí tohoto kamerového systému bylo více než 40 kamer, některé z nich s funkcí rozpoznávání SPZ a obličeje řidiče.

Úřad po zjištění dalších skutečností zahájil s obcí řízení o uložení opatření k odstranění nedostatků spočívajícího v ukončení zpracování osobních údajů výše uvedenými prostředky za účelem monitorování veřejného pořádku. Důvodem zahájení řízení byla skutečnost, že obci jakožto správci dotčených osobních údajů pro právě uvedený účel zpracování osobních údajů nemůže svědčit žádný z právních důvodů zpracování podle čl. 6 odst. 1 písm. a) až f) nařízení (EU) 2016/679. Specifičnost tohoto zpracování osobních údajů se projevuje v tom, že jej lze provádět pouze v případech, kdy je správce k takovému zpracování osobních údajů oprávněn na základě zákona (např. Policie České republiky podle § 62 zákona č. 273/2008 Sb., obecní policie podle § 24b zákona č. 553/1991 Sb.). Po vydání předběžného opatření nařizujícího zdržet se shromažďování osobních údajů prostřednictvím uvedeného kamerového systému obec dotčené zpracování osobních údajů ukončila a jednala o uzavření dodatku k veřejnoprávní smlouvě podle § 3a zákona č. 553/1991 Sb., a o uzavření koordinační dohody podle § 16 odst. 1 zákona č. 273/2008 Sb., jejichž předmětem by bylo provozování předmětného kamerového systému.

Obec nemůže bez konkrétního zákonného zmocnění zpracovávat osobní údaje prostřednictvím kamerového systému za účelem monitorování veřejného pořádku. V rámci obce uvedenými prostředky a za uvedeným účelem může na základě § 24b odst. 1 zákona č. 553/1991 Sb. osobní údaje zpracovávat obecní policie. Obec, která nemá zřízenou obecní policii, pak může zpracovávat osobní údaje prostřednictvím kamerového systému za týchž podmínek jako jakýkoli „běžný" správce osobních údajů, tedy například za účelem ochrany svého majetku, splňuje-li takové zpracování podmínky stanovené nařízením (EU) 2016/679, tj. zejména lze-li jej založit na některém z právních důvodů podle čl. 6 odst. 1, přičemž v úvahu zde přichází zejména právní důvod zpracování podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679.

Rozesílání písemných nabídek k odkupu pohledávek

Úřad na základě množství obdržených stížností obdobného obsahu provedl kontrolu společnosti, která se zabývá odkupem pohledávek, přičemž předmětem této kontroly bylo zpracování osobních údajů vlastníků pohledávek, a to za účelem jejich oslovení s nabídkou k odkupu. Na základě zjištění učiněných v rámci kontroly pak Úřad zahájil společné řízení o přestupcích a uložení opatření k odstranění nedostatků.

V pravomocném rozhodnutí ve věci Úřad konstatoval, že předmětná společnost jakožto správce osobních údajů zpracovávala osobní

údaje fyzických osob (v rozsahu jméno, příjmení, adresa bydliště, datum narození, výše pohledávky a specifikace smlouvy, na jejímž základě pohledávka vznikla), jimž adresovala listinnou nabídku na odkup jejich pohledávky, a to bez právního důvodu podle čl. 6 odst. 1 nařízení (EU) 2016/679. Současně Úřad konstatoval, že společnost nijak neinformovala o daném zpracování osobních údajů vlastníky pohledávek a nesplnila tak vůči nim informační povinnost podle čl. 14 odst. 1 a 2 nařízení (EU) 2016/679. Porušením těchto povinností se společnost dopustila přestupků podle § 62 odst. 1 písm. b) a c) zákona č. 110/2019, za což jí Úřad uložil pokutu.

Společnost zakládala zpracování osobních údajů dotčených vlastníků pohledávek na právním důvodu uvedeném v čl. 6 odst. 1 písm. f) obecného nařízení, tj. na tzv. oprávněném zájmu správce osobních údajů. Úřad však dospěl po přezkoumání tzv. balančního testu k závěru, že v tomto konkrétním případě mají přednost zájmy nebo základní práva a svobody subjektů údajů vyžadující ochranu osobních údajů před zájmem správce osobních údajů. Z hlediska tohoto posouzení byla významná mimo jiné skutečnost vyplývající z bodu 47 obecného nařízení, a to že mezi správcem osobních údajů a jednotlivými subjekty údajů neexistoval žádný relevantní předchozí vztah, a proto subjekty údajů nemohly očekávat, že by jejich osobní údaje předmětná společnost zpracovávala. V neprospěch potenciálního kladného výsledku balančního testu přispěla i výše uvedená skutečnost, že společnost dotčené subjekty údajů neinformovala ve stanovené lhůtě o zpracování jejich osobních údajů, čímž jim znemožnila případné uplatňování jejich práv vůči ní do chvíle, než je oslovila s nabídkou. K tomu však došlo později, než je stanovená nejzazší lhůta pro poskytnutí informací subjektům údajů o zpracování jejich osobních údajů.

Přestože zpracování osobních údajů za účelem přímého marketingu je v obecné rovině na základě právního důvodu podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 možné, je třeba, aby se správce osobních údajů zabýval všemi relevantními kritérii z hlediska posouzení, zda v konkrétním případě nad jeho zájmy nepřevažují zájmy nebo základní práva a svobody subjektů údajů.

Z ROZHODNUTÍ PŘEDSEDY ÚŘADU – ROZHODNUTÍ II. STUPNĚ

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

Povinnosti spravujícího orgánu (aplikace Karanténa)

Rozhodnutími Úřadu vydanými pod sp. zn. UOOU-02569/22 byla Česká republika – Ministerstvo vnitra uznána vinnou ze spáchání přestupku podle § 63 odst. 1 písm. a) zákona č. 110/2019 Sb., o zpracování osobních údajů. Uvedený přestupek byl spáchán tím, že Policie České republiky jako spravující orgán podle § 24 odst. 3 zákona č. 110/2019 Sb., v souvislosti s provozem aplikace Karanténa využívané při namátkových kontrolách osob v období od 1. dubna 2021 do 8. března 2022 shromáždila osobní údaje více než 2 milionů osob, jimž byla v rámci opatření proti šíření onemocnění COVID-19 nařízena izolace, a to v rozsahu: jméno a příjmení, datum narození, rodné číslo, označení, že je daná osoba v izolaci, datum počátku a konce izolace a adresa pro výkon izolace.

Zákon č. 273/2008 Sb., o Policii České republiky, v ustanovení § 79 odst. 3 výslovně omezuje možnost Policie ČR shromažďovat osobní údaje o zdravotním stavu, rasovém nebo etnickém původu, náboženském, filozofickém nebo politickém přesvědčení, členství v odborové organizaci, sexuálním chování nebo sexuální orientaci. Tyto specifické osobní údaje smí Policie ČR shromažďovat, pouze pokud je to nezbytné pro účely šetření konkrétního trestného činu nebo přestupku, nebo při poskytování ochrany osob (kdy je Policie ČR oprávněna disponovat citlivými osobními údaji těch osob, jimž poskytuje ochranu, např. v případě ochrany svědků v rámci trestního řízení).

Přestože zákon o Policii ČR nepřipouští, aby si Policie ČR osobní údaje spadající do výše uvedených zvláštních kategorií shromažďovala plošně a předem bez vztahu k šetření konkrétního případu, shromažďovala Policie ČR v rámci provozu aplikace Karanténa preventivně informace o veškerých osobách s nařízenou izolací, a tedy s prokázaným onemocněním COVID-19,

čímž výrazně vybočila z limitů oprávnění pro nakládání s osobními údaji o zdravotním stavu, vymezených zákonem o Policii ČR, a tím došlo k naplnění skutkové podstaty přestupku podle § 63 odst. 1 písm. a) zákona č. 110/2019 Sb. o zpracování osobních údajů.

Policie ČR, stejně jako všechny ostatní orgány veřejné moci, má zákonem vymezenou působnost, tedy okruh úkolů jí svěřených, a rovněž pravomoc, tedy soubor prostředků určených k realizaci této působnosti. Policii ČR, jakožto bezpečnostnímu sboru, právní řád stanoví poměrně širokou pravomoc, zahrnující řadu oprávnění. Tím spíše je v rámci právního státu respektujícího základní principy ochrany lidských práv a svobod důležité také přesné vymezení hranic této pravomoci a neméně důležité je jejich důsledné dodržování. Jestliže zákon zapovídá Policii ČR plošné „preventivní" shromažďování osobních údajů o zdravotním stavu, nemohou ani specifické okolnosti pandemie onemocnění COVID-19 poskytnout dostatečné odůvodnění pro zásadní překročení zákonných limitů pravomocí Policie ČR. Nelze také opomenout, že osobní údaje o nařízených izolacích začala Policie ČR v aplikaci Karanténa zpracovávat až od dubna 2021, tedy až cca po roce od počátku pandemie onemocnění COVID-19, proto na toto zpracování ani na pochybení, která Úřad v tomto jednání Policie ČR shledal, nelze pohlížet jako na (případně omluvitelný) exces související s počátečním obdobím pandemie, pro které byla charakteristická určitá živelnost postupů.

Pro úplnost je třeba dodat, že vedení evidence osob s nařízenou izolací z důvodu nakažlivého onemocnění, popř. vedení evidence osob v dočasné pracovní neschopnosti z důvodu takového onemocnění, je za předpokladu splnění zákonných podmínek možné. Primární podmínkou je vedení takové evidence tím orgánem veřejné moci, kterému takový způsob zpracování osobních údajů o zdravotním stavu ukládá či umožňuje zákon. Rovněž nebylo vyloučeno prověřování informací, zda konkrétní (kontrolované) osobě byla nařízena izolace, či nikoliv, prováděné ze strany Policie ČR – pokud by se tak dělo vždy ve vztahu ke konkrétnímu prověřovanému případu, jak § 79 odst. 3 zákona o Policii ČR předpokládá.

Kromě výše zmíněného přestupku Úřad shledal spáchání dalších tří přestupků, konkrétně přestupku podle § 63 odst. 1 písm. d) zákona č. 110/2019 Sb., podle § 63 odst. 1 písm. k) zákona č. 110/2019 Sb. Tyto přestupky spočívaly v tom, že Policie v rozporu s § 27 písm. c) zákona č. 110/2019 Sb. nezveřejnila účel tohoto zpracování osobních údajů, dále že v rozporu s ustanovením § 37 zákona č. 110/2019 Sb. nezpracovala dokument ohledně posouzení vlivu tohoto zpracování na ochranu osobních údajů a že nepodala Úřadu řádnou žádost o projednání předmětného zpracování, čímž porušila ustanovení § 38 odst. 1 písm. b) zákona č. 110/2019 Sb.

V tomto kontextu je možno poukázat na vzájemnou souvislost uvedených přestupků. Pokud by Policie ČR před zahájením zpracování osobních údajů osob s nařízenou izolací provedla posouzení vlivu zamýšleného zpracování na ochranu osobních údajů a projednala ho s Úřadem, mohl by být včas vyjasněn právní režim připravovaného zpracování a s ním související právní povinnosti a omezení, a k překročení zákonných limitů zpracování osobních údajů o zdravotním stavu ze strany Policie ČR by pravděpodobně ani nedošlo. Řádné splnění infomační povinnosti ve vztahu k subjektům údajů by zase dalo subjektům údajů reálnou možnost pro efektivní uplatnění svých práv.

Za výše uvedené přestupky Úřad uložil pokutu 975 000 Kč. Pokutu za přestupek na úseku ochrany osobních údajů bylo v tomto případě možné Ministerstvu vnitra jako orgánu veřejné moci udělit, protože se jednalo o zpracování osobních údajů prováděné Policií ČR za účelem předcházení, vyhledávání a odhalování trestné činnosti (porušení režimu izolace mohlo mj. naplnit skutkovou podstatu trestného činu šíření nakažlivé nemoci, protože onemocnění COVID-19 bylo v té době na seznamu takových nemocí zařazeno), které upravuje hlava III. zákona o zpracování osobních údajů resp. zpracování osobních údajů spadá do režimu tzv. trestněprávní směrnice. Na rozdíl od zpracování osobních údajů v režimu GDPR není ve vztahu k takovému zpracování ukládání trestů veřejným subjektům vyloučeno.

Uvedená rozhodnutí však byla napadena správní žalobou a výsledky tohoto řízení ke dni zpracování výroční zprávy nejsou známy.

NÁRODNÍ JUDIKATURA

V roce 2023 bylo několik rozhodnutí Úřadu podrobeno soudnímu přezkumu v rámci správního soudnictví. Pokud jde o ukončená soudní řízení, lze poukázat zejména na rozsudek týkající se podmínek vyvážení ochrany soukromí veřejně činných osob (ale i dalších dotčených osob) a veřejného zájmu na přístup k informacím o nich.

Ochrana soukromí veřejně činných osob

Městský soud v Praze svým rozsudkem čj. 5 A 73/2019-50 ze dne 27. února 2023, proti němuž nebyla podána kasační stížnost, potvrdil pokutu ve výši 140 000 Kč, kterou Úřad uložil vydavatelské společnosti za spáchání přestupku ještě podle § 45a odst. 1 a 3 zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.), spočívajícího v neoprávněném zveřejnění informací pocházejících z odposlechu a záznamu telekomunikačního provozu velmi významných veřejně (politicky) činných osob, pořízených v rámci trestního řízení. Jak je třeba připomenout, jednalo se o déle trvající řízení; původní rozhodnutí Úřadu ve věci z roku 2014, jímž byla vyměřena pokuta ve výši 240 000 Kč, a které následně potvrdil i Městský soud v Praze, Nejvyšší správní soud svým rozsudkem čj. 2 As 304/2017-42 ze dne 3. května 2018 zrušil a věc vrátil k dalšímu řízení.

Jak Nejvyšší správní soud v rozsudku čj. 2 As 304/2017-42 ze dne 3. května 2018, tak Městský soud v Praze v rozsudku čj. 5 A 73/2019-50 ze dne 27. února 2023, vyzvedly povinnost provést před každým zveřejněním konkretizovaný test proporcionality mezi veřejným zájmem o informace a zájmem na ochranu soukromí, a to ve vztahu ke všem dotčeným osobám a ke všem zveřejněným informacím.

Soudní rozhodnutí potvrdila právní závěry Úřadu, tedy že i veřejně činná osoba má právo na soukromí, přičemž veřejný zájem na přístup k informacím týkajícím se takové veřejně činné osoby může převážit nad jejím zájmem na ochranu soukromí pouze tehdy, jsou-li osobní údaje potřebné pro utváření politických názorů veřejnosti anebo posuzování aktivit veřejně činných osob ze strany veřejnosti. Zároveň musí být zvláště dbáno na práva dalších osob, které nejsou veřejně činné (asistentky, řidiči) a které by mohly být zveřejněním dotčeny.

Stejně tak je důležitá i forma publikace. Informace proto nesmějí být podávány v hrubě urážlivé formě, respektive spíše ve snaze o vyvolání senzace, byť by se jednalo o doslovný přepis hovorů.

Samotný pojem zveřejnění pak zahrnuje každé uvedení informace na veřejnost. To, že obdobná informace již byla publikována, tedy nepředstavuje žádnou překážku pro vedení sankčního řízení, může mít však význam z hlediska výměry sankce.

HLAVNÍ 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 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 obecného nařízení a § 31 zákona č. 110/2019 Sb. na nedostatky při zpracování jeho osobních údajů. Úřad se zabývá rovněž jinými podněty, aby ověřil zákonnost zpracování osobních údajů.

Zveřejnění údajů ve veřejném seznamu držitelů datových schránek

V souvislosti s povinným zřízením datových schránek pro podnikající fyzické osoby počátkem roku 2023 se na Úřad obrátilo několik set podatelů se stížností na zveřejnění jejich osobních údajů ve veřejném seznamu držitelů datových schránek spolu se žádostí o výmaz z tohoto veřejného seznamu. Seznamy datových schránek fyzických osob i podnikajících fyzických osob byly totiž zveřejněny nejen v podobě formuláře pro vyhledávání konkrétní datové schránky na stránkách www.mojedatovaschranka.cz, ale současně také v rámci systému tzv. „otevřených dat“. Seznamy držitelů datových schránek tak byly zveřejněny „způsobem umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu“. Zjednodušeně řečeno byly tyto otevřené datové sady přizpůsobeny pro neomezené stahování a kopírování stejně jako pro další

využití. Tato funkcionalita byla přitom dostupná komukoli, a to bez jakékoli kontroly nebo regulace takového užití. Zjistit adresu trvalého pobytu fyzické osoby mohl tedy kdokoliv, aniž by této osobě chtěl poslat datovou zprávu.

V návaznosti na skokový nárůst výše uvedených stížností Úřad upozornil zřizovatele a správce systému datových schránek (Ministerstvo vnitra) na to, že s ohledem na zásady zpracování osobních údajů podle obecného nařízení – zejména pak ve vztahu k zásadě minimalizace a důvěrnosti zpracování osobních údajů –, je uveřejnění zejména seznamu údajů fyzických osob nepřijatelné. Agendu datových schránek od 1. dubna 2023 převzala Digitální a informační agentura,[1] která na výzvu Úřadu reagovala obratem a jako nový garant provozu datových schránek (a tedy i správce osobních údajů uvedených v daném seznamu) okamžitě zahájila kroky k odstranění seznamu nepodnikajících fyzických osob ze systému otevřených dat, jenž byl do té doby zveřejněn na webu Datových schránek a v Národním katalogu otevřených dat.

Úřad každého jednotlivého podatele zpravil o zákonné úpravě, tj. že povinnost vést veřejný seznam fyzických osob, podnikajících fyzických osob, právnických osob a orgánů veřejné moci, které mají zřízenu a zpřístupněnu datovou schránku, tzn. seznam držitelů datových schránek, který je přístupný způsobem umožňujícím dálkový přístup, je dána ustanovením § 14b odst. 1 zákona o elektronických úkonech a autorizované konverzi dokumentů (zákon č. 300/2008 Sb.), a o tom, že tento seznam vede Digitální a informační agentura a v souladu s ustanovením § 2 odst. 2 tohoto zákona zřizuje a spravuje datové schránky a je zároveň správcem informačního systému datových schránek podle ustanovení § 14 odst. 2 tohoto zákona. Pokud fyzická osoba nesouhlasí s uvedením svých údajů ve veřejném seznamu držitelů datových schránek, měla podle ustanovení § 14b odst. 4 zákona č. 300/2008 Sb. právo na vymazání údajů z tohoto seznamu. Tuto možnost však neměly podnikající fyzické osoby, jimž byly datové schránky zřízeny ze zákona č. 300/2008 Sb. Znepřístupnění bylo možné pouze ze zákonem vymezených důvodů (např. z důvodu výmazu subjektu ze zákonem stanovené evidence ukončení podnikání, úmrtí, omezení na osobní svobodě, apod.).

Kromě výše uvedeného odstranění seznamů nepodnikajících fyzických osob byla na společném jednání zástupců Úřadu pro ochranu osobních údajů a Digitální a informační agentury dohodnuta příprava odpovídající úpravy stávající legislativy směřující k posílení ochrany osobních údajů. Dne 3. listopadu 2023 byl zákon č. 327/2023 Sb., kterým se mění zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, vyhlášen ve Sbírce zákonů s nabytím účinnosti 1. února 2024. Nová právní úprava nemění rozsah údajů zveřejňovaných v seznamu držitelů datových schránek, ale nahrazuje princip opt-out principem opt-in. Tedy namísto automatického zápisu na seznam a nezbytné žádosti o vymazání může fyzická osoba nebo podnikající fyzická osoba požádat naopak o zápis na seznam. Nově se tedy i pro podnikající fyzickou osobu umožňuje postup výmazu ze seznamu, jelikož může-li osoba požádat o zápis, je žádoucí, aby mohla kdykoliv změnit názor a požádat též o výmaz. Ke dni účinnosti tohoto zákona údaje vedené v seznamu držitelů datových schránek o fyzické nebo podnikající fyzické osobě, která má zřízenu a zpřístupněnu datovou schránku, mají být zlikvidovány.

Zpracování osobních údajů obcemi

Podstatná část podání směřujících proti obcím se obdobně jako v předchozích letech týkala zveřejňování osobních údajů občanů obce na webových stránkách obcí. Nejčastěji obce zveřejňovaly osobní údaje žadatelů a informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v souvislosti s plněním povinností povinného subjektu podle § 5 odst. 3 tohoto zákona. Případně se jednalo o případy, kdy obec zveřejnila dokument v jiné souvislosti bez provedení řádné a dostatečné anonymizace/pseudonymizace předmětného dokumentu nebo zvolila metodu, která umožňovala zpřístupnění osobních údajů a informací vyloučených ze zpřístupněného dokumentu.

1 Do 31. března 2023 seznam vedlo Ministerstvo vnitra. Na základě zákona č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony, vede od 1. dubna 2023 tento seznam Digitální a informační agentura.

Opakovaně byla Úřadu doručena podání poukazující na jednání zastupitele obce, případně další osoby, která nahrávala či zajišťovala nahrávání schůze zastupitelstva, a záznam následně zveřejnila na sociální síti či webových stránkách další osoby, obvykle spolku či politického hnutí. V těchto případech zveřejnění záznamů ze zastupitelstva se ve většině případů jednalo o systematické jednání osoby, které bylo nutné považovat za zpracování osobních údajů pro novinářské účely, a proto muselo být v souladu s požadavky obecného nařízení a speciálních ustanovení zákona o zpracování osobních údajů (konkrétně § 17 až § 22 zákona č. 110/2019 Sb., o zpracování osobních údajů). Zastupitelé (případně další osoby), kteří tímto způsobem zpracovávali osobní údaje (tedy zveřejnili záznam schůze zastupitelstva) se s ohledem na tuto činnost stali správci osobních údajů, a proto byli povinni před zveřejněním záznamů z jednání zastupitelstva provést řádnou a důslednou anonymizaci v záznamu obsažených osobních údajů, které se netýkaly věcí veřejného zájmu. Tedy těch osobních údajů, které nebylo možné považovat za informace o činnosti obce a které vypovídaly pouze o soukromí, osobním životě či poměrech fyzických osob. Úřad v těchto případech postupoval tak, že příslušnému správci osobních údajů ohlásil možné porušení obecného nařízení a vyzval jej k nápravě. Přestože správci osobních údajů po upozornění Úřadem ve většině případů pochybení napravili, Úřad v těchto případech stěžovatele současně s vyrozuměním o prošetření podnětu informoval o jeho právu domáhat se náhrady nemajetkové újmy na správci osobních údajů, a to i soudní cestou.

Vybraná zpracování osobních údajů bankovními institucemi

Na Úřad se stále obrací podatelé ve věci kopírování občanských průkazů bankovními institucemi. V této souvislosti je nutné poukázat na zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (tzv. AML zákon), který upravuje povinnost povinných osob (a tedy i bankovních institucí) identifikovat klienty a provést jejich kontrolu, s čímž může souviset i oprávnění povinných osob zkopírovat doklad, který byl k identifikaci použit. Daná problematika byla předmětem jednání mezi Úřadem pro ochranu osobních údajů a Finančním analytickým úřadem, přičemž Úřad poskytl připomínky na základě dostupné interpretace obecného nařízení v oblasti AML v rámci spolupráce mezi státními orgány. Finančně analytický úřad následně zveřejnil aktualizovaný metodický pokyn Finančně analytického úřadu.

S povinností bankovních institucí provést silné ověření klienta nově eviduje Úřad stížnosti na sledování mobilního zařízení v souvislosti s instalací mobilního bankovnictví. V souladu se zákonnou úpravou jsou bankovní instituce povinny zavést a provozovat transakční monitoring, který je schopen identifikovat známky napadení malwarem nebo vést záznamy o použití softwaru pro přístup. Bez sbírání a analýzy informací o zařízení, na kterém je nainstalována aplikace mobilního bankovnictví, není banka schopna zajistit plnění svých povinností v této oblasti, resp. zajišťovat bezpečnost provádění plateb v mobilní aplikaci. Pochybení v této oblasti shledal Úřad pouze v jednom případě, a to při plnění informační povinnosti, kdy informace poskytnuté správcem osobních údajů byly zavádějící a neúplné. Po upozornění bankovní instituce obsah informací upravila.

Pořizování kopií dokladu totožnosti nebankovními subjekty

V poslední době v souvislosti s tím, jak se přesouvá vyřízení mnohých záležitostí do online prostoru, přibývá stížností na společnosti, které vyžadují poskytnutí (odeslání) kopie dokladu totožnosti elektronickou cestou (scan či fotografie), kdy nelze ověřit zabezpečenost odeslání – nahráním dokladu totožnosti do určitého formuláře či aplikace. Jedná se o služby, kdy je vyžadována určitá forma ověření totožnosti, ale zdaleka se nejedná jen o služby poskytované bankovními institucemi – např. je tato forma ověření identity vyžadována v případě online odbavení cestujících letadlem, pro ověření při nákupu na e-shopu, pro rychlé získání brigády přes různé aplikace, při registraci do služby sdílení vozidel, při objednání služby mobilními operátory, event. pro přístup k osobním údajům např. u jednoho z nebankovních registrů klientských informací.

Vzhledem k zákonné úpravě pořizování kopií některých dokladů totožnosti Úřad posuzuje tento

postup správců osobních údajů z hlediska rozsahu zpracovávaných údajů z dokladu totožnosti. Podle ustanovení § 39 písm. c) zákona o občanských průkazech (zákon č. 269/2021 Sb.) je zakázáno pořizovat kopie občanského průkazu bez souhlasu držitele občanského průkazu. Ovšem i v případě, kdy dá držitel občanského průkazu k pořízení kopie souhlas, je nutné dodržovat základní povinnosti při zpracování osobních údajů podle obecného nařízení.

Podle zásady minimalizace upravené v článku 5 odst. 1 písm. c) obecného nařízení musí být osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. S ohledem na tuto zásadu není správce osobních údajů oprávněn pořídit kopii celého občanského průkazu či jiného dokladu totožnosti s výjimkou případů, kdy tak činí z důvodu plnění právní povinnosti.

Jako vhodné se proto jeví použít šablonu, která nadbytečné osobní údaje zakryje, a zohlednit, aby na pořízené částečné kopii občanského průkazu nebyly strojově čitelné údaje. Zásada minimalizace se použije také při pořizování kopií dalších dokladů totožnosti (např. pas, řidičský průkaz). K pořízení redukované kopie občanského průkazu prostřednictvím „začerňovací" šablony není potřeba souhlas držitele dokladu, neboť se nejedná o plnohodnotnou kopii ve smyslu zákona č. 269/2021 Sb. o občanských průkazech.

Zveřejňování osobních údajů za novinářským účelem

Úřad se zabývá i podáními v této oblasti zpracování osobních údajů. Obdobně jako v jiných případech Úřad podatele před věcným posouzením podnětu/stížnosti poučí o jeho právech, která má vůči správci osobních údajů, v této oblasti specificky na jeho povinnost uplatnit námitku vůči správci osobních údajů před podáním podnětu/stížnosti. Úřad v případě zpracování osobních údajů pro novinářské účely posuzuje, zda zpracování slouží přiměřeným způsobem pro tyto účely. V konkrétním případě Úřad posuzoval stížnost týkající se mediálního domu, který zveřejnil intimní fotografie ženy pro ilustraci k textu souvisejícího článku, kde by pro účely předmětného článku postačovalo zveřejnění anonymizované fotografie (např. s rozostřeným obličejem). V této souvislosti je však vhodné ještě doplnit, že se nejednalo o fotografii původně určenou stěžovatelkou ke zveřejnění komukoliv, ale pouze ke zpřístupnění určité skupině osob (uživatelům internetového portálu). S ohledem na tyto skutečnosti by zveřejnění i tváře stěžovatelky, tedy její identity, nemuselo být přiměřené novinářskému účelu. Stížnost je nadále předmětem šetření Úřadu.

Vyhledávače či jiné platformy

Úřad i v tomto roce obdržel stížnosti na jednoho provozovatele internetového vyhledavače. Stěžovatelé rozporovali požadavek na uvedení svého telefonního čísla v souvislosti s využíváním nabízených služeb (e-mailové schránky). Správce osobních údajů svůj postup odůvodnil zvýšením zabezpečení uživatelských účtů a přístupových hesel pomocí ověření záchranného telefonního čísla, toto číslo tedy mělo sloužit jako prostředek pro obnovení přístupu k uživatelskému účtu. Jako další důvod pro tento požadavek správce osobních údajů uvedl minimalizaci zakládání jednorázových, podvodných či falešných uživatelských účtů (na telefonní číslo je zasílán ověřovací kód). Ke zpracování osobních údajů docházelo v důsledku uzavření smlouvy mezi uživatelem a provozovatelem vyhledávače.

V jiném případě byla namítána povinnost poskytnutí osobních údajů při zapojení uživatele do diskuze. I zde tato povinnost vycházela ze smluvních podmínek pro užívání této služby. Důvody, pro které správce osobních údajů může požádat uživatele o ověření identity, jsou zejména shoda jména a příjmení uživatele se jménem a příjmením slavné osobnosti, podezření, že uživatel vystupuje pod falešnou identitou či bezpečnostní důvody.

V žádném z uvedených případů nebylo shledáno pochybení správce osobních údajů. Zákonnost se v tomto případě odvíjela od smluvního vztahu, a proto byly účely zpracování posouzeny jako legitimní.

Obchodní sdělení zasílaná poštou

Tato podání dlouhodobě tvoří značnou část stížnostní agendy, právním důvodem pro předmětné zpracování osobních údajů může být oprávněný zájem správce osobních údajů. Pod-

mínkou použití tohoto právního důvodu je, aby oprávněné zájmy správce osobních údajů nepřevyšovaly základní práva a svobody subjektů údajů. Oprávněný zájem se odvíjí od toho, zda může subjekt údajů s ohledem na předmět činnosti správce marketingovou nabídku důvodně očekávat. Správce osobních údajů při uplatnění tohoto právního důvodu musí poměřovat své oprávněné zájmy se základními právy a svobodami subjektů údajů.

Správci osobních údajů však často náležitě nereagují na žádosti subjektů údajů o přístup k osobním údajům, vznesení námitky či žádost o výmaz osobních údajů. Úřad v těchto případech správce osobních údajů obvykle pouze upozorňuje na daná pochybení, avšak v případě, že správci osobních údajů neupraví své postupy, přistoupí Úřad k uplatnění dalších dozorových pravomocí.

Využití osobních údajů z katastru nemovitostí

Mezi „stálice" v uplynulém roce patřily i stížnosti na využití osobních údajů realitními společnostmi, event. realitními makléři za účelem zaslání návrhu na odkup nemovité věci nebo podílu na ní. V těchto dopisech někteří správci osobních údajů neposkytují vlastníkům nemovitých věcí (subjektům údajů) povinné informace o zpracování osobních údajů. Nabídky jsou vlastníkům nemovitých věcí rozesílány ve velkém množství a opakovaně, přičemž cenové nabídky podle podatelů často neodpovídají skutečné hodnotě nemovitých věcí, event. je prostřednictvím těchto nabídek vyvíjen určitý tlak na vlastníky. Příkladem citace z úvodu nabídky realitní společnosti zaslané vlastníkovi pozemku:

„Na lesy napadené kůrovcem se vztahuje zákonná povinnost (§ 32 z. č. 289/95 Sb., o lesích), kterou musí majitelé plnit bez rozdílu a pod hrozbou pokuty. Váš podíl na lese odebereme za odpovídající částku. Převezmeme za Vás veškeré zákonné povinnosti. Zbavíte se tak starostí spjatých s vlastnictvím tohoto pozemku."

Takové využití osobních údajů z veřejného rejstříku vzbuzuje u některých podatelů přinejmenším pohoršení, u jiných i obavu ze ztráty majetku. Rozsah působnosti Úřadu v této oblasti je však značně omezen zvláštní úpravou katastrálního zákona (zákon č. 256/2013 Sb., zákon o katastru nemovitostí), který definuje přípustné účely využití údajů z katastru nemovitostí, k jehož závaznému výkladu, ani k vedení řízení, není Úřad oprávněn. Příslušnými pro vedení řízení o přestupcích podle katastrálního zákona jsou v souladu s katastrálním zákonem katastrální úřady, které dovodily, že cílené oslovování konkrétních vlastníků (či spoluvlastníků) nemovitých věcí s určitou nabídkou (k odkupu, prodeji apod.) je v rozsahu využití údajů pro hospodářské účely. Jednání právnických a fyzických osob nabízejících odkup/prodej nemovitých věcí tedy dosud katastrální úřady posuzují jako jednání, které není v rozporu s katastrálním zákonem.

Úřad je však v rozsahu své působnosti oprávněn posuzovat, zda správci osobních údajů (zasílatelé nabídek) plní řádně informační povinnost či reagují na žádosti subjektů údajů, kterými vykonávají svá práva v souladu s obecným nařízením a v tomto rozsahu také zaslané stížnosti prověřuje.

Povinnosti správců osobních údajů při výkonu práv subjektu údajů

V roce 2023 bylo rovněž častým předmětem doručených stížností neposkytnutí odpovědi správci osobních údajů k žádosti subjektu údajů o výkon práv podle obecného nařízení. Případně bylo předmětem stížností nerespektování již uplatněného práva na výmaz osobních údajů, kterému již správce vyhověl (typicky pro marketingové účely). V případě těchto stížností Úřad volil cestu upozornění příslušného správce osobních údajů, případně si vyžádal informace k prováděnému zpracování osobních údajů. Opakovaně z poskytnutých odpovědí správců osobních údajů vyplynulo, že správce osobních údajů chybně nevyhodnotil obdržené podání jako žádost o výkon práv podle obecného nařízení, které byl povinen vyřídit ve lhůtě jednoho měsíce. V druhém případě, který představovaly situace, kdy správci osobních údajů nerespektovali právo na výmaz osobních údajů, kterému již vyhověli (zejména výmaz osobních údajů pro účely marketingu), bylo častým pochybení řádné nevyřízení žádosti, kdy správce osobních údajů neprovedl

výmaz osobních údajů ze všech existujících databázích, které spravuje.

Zpracování osobních údajů prostřednictvím kamerových systémů

Se stížnostmi na zpracování osobních údajů prostřednictvím kamerových systémů, dveřních digitálních kukátek nebo fotopastí, ať již v souvislosti s dlouhodobými sousedskými nebo rodinnými spory, případně provozovaných fyzickými nebo právnickými osobami k ochraně majetku, bezpečnosti a zdraví osob, se každoročně na Úřad obrací řádově několik set podatelů, a to přesto, že Úřad v této oblasti šíří dlouhodobě osvětu na svém webu (Kamerové systémy). Rok 2023 dané pravidlo potvrdil. Jak Úřad opakovaně uvádí, možnosti Úřadu uspokojivě řešit stížnosti na kamerové systémy provozované fyzickou osobou z obydlí jsou velmi omezené, neboť dozorové kompetence Úřadu neumožňují kontrolovat obydlí, která nejsou užívaná k podnikatelské činnosti anebo k provozování jiné hospodářské činnosti, a tudíž ani řešit většinu občanských neshod a sousedských sporů, a to zejména proto, že kontrolující není oprávněn vstupovat do obydlí, které neodpovídá vymezení v ustanovení § 7 zákona č. 255/2012 Sb. o kontrole (kontrolní řád), a proto nemůže ověřit režim provozu kamerového systému. Úřad proto v těchto případech pouze informuje provozovatele kamerového systému o jejich povinnostech správce osobních údajů, podatele pak o možnosti řešit věc primárně podáním podnětu na zahájení přestupkového řízení proti občanskému soužití, který je oprávněna řešit obec s rozšířenou působností, a též o možnosti účinně se bránit prostřednictvím občanskoprávní žaloby na ochranu osobnosti u příslušného soudu.

Úřad své dozorové a nápravné pravomoci v případě kamerových systémů provozovaných z obydlí, které neodpovídá vymezení v ustanovení § 7 zákona č. 255/2012 Sb., může účinně uplatnit pouze v případech následného zpracování osobních údajů obsažených v kamerových záznamech z takového zařízení, a to zejména v případech nevhodného zveřejnění nebo jiného zneužití kamerových záznamů obsahujících zachycené podoby identifikovatelných osob, kdy okolnosti nasvědčují tomu, že dochází k porušení povinností správce osobních údajů podle obecného nařízení a základních zásad při zpracování údajů. Takové stížnosti však představují pouze nepatrný zlomek podání směřujících proti zpracování osobních údajů prostřednictvím kamerových systémů.

Vymáhání pohledávek

V této oblasti zpracování osobních údajů je obvyklým předmětem stížností (obvykle podaných dlužníky) předání osobních údajů inkasním společnostem a následné využití údajů pro kontaktování podatele stížnosti. Daný postup věřitele je však legitimní, inkasní společnost je v pozici zpracovatele osobních údajů a osobní údaje zpracovává na základě zpracovatelské smlouvy uzavřené se správcem osobních údajů (věřitelem).

Podatelé se dále obracejí na Úřad v souvislosti s předáním osobních údajů postupitelem pohledávky postupníkovi. I takové zpracování je však oprávněné a vychází z právní úpravy institutu postoupení pohledávky obsažené v občanském zákoníku (zákon č. 89/2012 Sb.).

Zpracování osobních údajů společenstvími vlastníků jednotek a bytovými družstvy

Stížnosti na tyto správce osobních údajů jsou Úřadu zasílány opakovaně. Tito správci osobních údajů často řádně neplní informační povinnost vůči dotčeným fyzickým osobám, jejichž osobní údaje zpracovávají, nevyřizují příslušným způsobem žádosti subjektů údajů (typicky členů) o výkon jejich práv v souladu s obecným nařízením, a běžně dochází ke zveřejňování osobních údajů na přístupné nástěnce v domě či jejich zpřístupňování v rámci internetové aplikace dalším členům, a to bez právního důvodu. Vzhledem ke skutečnosti, že ve vedení těchto společenství vlastníků a bytových družstev bývají osoby, které se ochranou osobních údajů nezabývají, považuje Úřad v těchto případech za prospěšnější upozornění správce osobních údajů na jeho pochybení a vysvětlení jeho povinností podle obecného nařízení. Obvykle správci osobních údajů pochybení napraví a přijmou příslušná opatření.

PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

V roce 2023 Úřad obdržel 383 ohlášení porušení zabezpečení osobních údajů, jde tedy o určitý nárůst oproti předchozím letům. Nejčastější příčinou porušení, kterou ohlašovatelé uváděli, byl podobně jako v uplynulých letech kybernetický útok, nejčastěji ransomware, event. jiný typ externího útoku. Z těchto ohlášení za rok 2023 vyplývá, že útočníci začali využívat ke svým kybernetickým útokům zranitelnosti nultého dne, tzv. zero-day attack, což je útok, který zneužívá chyby (zranitelnosti) v softwaru, která není všeobecně známá a pro kterou ještě neexistuje záplata (patch). Tento způsob napadení byl ve velké míře zaznamenám u společností (napříč Evropou a USA), které měly na svých serverech nainstalovaný software MOVEit. Systém MOVEit je vytvořený společností Progress Software Corporation.

Narostl také počet neoprávněných přístupů k osobním údajům ze strany zaměstnanců, státních zaměstnanců a v četných případech i příslušníků bezpečnostních a záchranných sborů do informačních systémů, které standardně využívají k plnění svých služebních a pracovních úkolů. Jedná se o jednotlivce, kteří takto získané informace používají k soukromým účelům, popř. je předají dalším osobám. Tyto incidenty jsou primárně řešeny orgány činnými v trestním řízení.

Lze konstatovat, že přetrvává neznalost povinnosti ohlašovat porušení zabezpečení osobních údajů podle článku 33 obecného nařízení především u orgánů státní správy – obecních i krajských úřadů. V této souvislosti Úřad při výkonu své působnosti vůči orgánům veřejné moci naráží na napětí vytvořené zákonodárcem mezi zákonem o zpracování osobních údajů a textem obecného nařízení, resp. mezi účely obecným nařízením předvídanými uvážením národního zákonodárce a jejich konkrétním provedením v adaptačním zákoně (zákon č. 110/2019 Sb., o zpracování osobních údajů).

Zákonodárce zde využil možnost danou čl. 83 odst. 7 obecného nařízení, podle které může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty *orgánům veřejné moci a veřejným subjektům* usazeným v daném členském státě. V návaznosti na tento článek byla schválena úprava v ustanovení § 62 odst. 5 zákona č. 110/2019 Sb., která ukládá Úřadu, aby upustil od uložení jakéhokoli správního trestu také tehdy, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 obecného nařízení.

Navzdory této skutečnosti lze konstatovat, že ohlašovatelé porušení zabezpečení osobních údajů z oblasti orgánů veřejné moci poskytují Úřadu ve většině standardní součinnost. Ojediněle lze zaznamenat určité případy pouze formálního plnění povinností při ohlášení porušení zabezpečení ze strany těchto správců, kdy jsou si vědomi nemožnosti uložení správního trestu.

KONZULTAČNÍ ČINNOST ÚŘADU

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 2023.

Zasílání obchodních sdělení (tzv. dotazníků spokojenosti) třetí stranou

Úřad se zabýval zasíláním dotazníků spokojenosti prostřednictvím e-mailů. Tyto e-maily jsou podle dlouhodobé dozorové praxe Úřadu obchodními sděleními ve smyslu ustanovení § 2 písm. f) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů. Jsou zasílány ze strany společnosti, která zákazníkovi doručuje zboží pouze na základě smlouvy s prodejcem/dodavatelem zboží, tj. bez přímé smluvní vazby s adresátem zásilky. Předmětné e-maily se týkaly pouze doručovacího procesu.[2]

S ohledem na uvedenou skutečnost, že adresát zásilky je zákazníkem prodejce/dodavatele, nikoliv doručovatele, nelze považovat předmětný dotazník za součást doručovacího procesu, v rámci kterého by právním titulem byla uzavřená smlouva podle ustanovení článku 6 odst. 1 písm. b) obecného nařízení. Nejedná se ani o oprávněný zájem podle článku 6 odst. 1 písm. f) citovaného nařízení. V daném případě by zasílání předmětných sdělení bylo možné na základě § 7 odst. 2 zákona č. 480/2004 Sb., tj. s předchozím souhlasem adresátů.

Doručování rozhodnutí veřejnou vyhláškou v řízení s velkým počtem účastníků

Úřad se v rámci konzultační činnosti zabýval situací, kdy správní orgán při doručování rozhodnutí veřejnou vyhláškou v řízení s vysokým počtem účastníků pro lepší přehlednost výroku rozhodnutí uvádí účastníky s jejich osobními údaji na zvláštním listu, který je přílohou rozhodnutí. Rozhodnutí včetně přílohy je vyvěšeno na úřední desce, seznam s osobními údaji účastníků je tak dostupný komukoliv.

Z hlediska všeobecně uznávaného výkladu označení účastníků řízení s údaji umožňujícími jejich identifikaci je náležitostí výroku rozhodnutí podle § 68 odst. 2 správního řádu (zákon č. 500/2004 Sb.). Účastník řízení, kterému správní orgán doručuje rozhodnutí veřejnou vyhláškou vyvěšením na úřední desce a jeho zveřejněním též způsobem umožňujícím dálkový přístup, má právo z výrokové části rozhodnutí získat informaci také o tom, kdo jsou další účastníci řízení. Neuvedení účastníků řízení na úřední desce či případná anonymizace jejich osobních údajů správním orgánem by znamenala odepření tohoto práva.

V případě, že správní orgán při doručování veřejnou vyhláškou účastníkům řízení postupuje v souladu s příslušnými zvláštními zákony a správním řádem, které takový postup stanovují, jde o zpracování osobních údajů podle článku 6 odst. 1 písm. c) GDPR a § 5 písm. a) zákona o zpracování osobních údajů. Toto zpracování osobních údajů je totiž nezbytné pro splnění právní povinnosti, která se na správce vztahuje.

Provozování kamerového systému pouze s online přenosem

Zpracováním osobních údajů podle článku 4 odst. 2 obecného nařízení se mj. rozumí zpřístupnění přenosem. V oblasti kamerových systémů se zpřístupněním přenosem rozumí možnost sledování především video záznamu v reálném čase. V takovém případě nelze vyloučit ani určité riziko pořízení záznamu ze strany osoby, jež předmětný záznam aktuálně sleduje na svém zařízení, případně na zařízení, které mu je dáno k dispozici.

V souladu s uvedeným lze konstatovat, že citované nařízení dopadá na všechna zpracování prováděná prostřednictvím kamerového systému, ať už s pořizováním kamerového záznamu, nebo v režimu bez záznamu (online). To však pouze v případě, že zasahují do práv a svobod identifikovaných nebo identifikovatelných fyzických osob (především snímají fyzické osoby) a nejsou určena výhradně pro osobní potřebu.

V případě, kdy určitý subjekt zpracovává osobní údaje pro správce (subjekt, který stanovil účely a prostředky zpracování), je nutno uzavřít zpracovatelskou smlouvu podle článku 28 obecného nařízení.

Smluvní pokuta ve zpracovatelské smlouvě

Úřad se rovněž vyjadřoval k možnosti uvedení smluvní pokuty v rámci tzv. zpracovatelské smlouvy podle článku 28 odst. 3 obecného nařízení.

2 V legislativním procesu je návrh zákona o digitální ekonomice, kterým je plánováno nahradit zákon č. 480/2004 Sb., výše uvedené se týká právní úpravy účinné v roce 2023.

Zpracovatel při zpracování osobních údajů je povinen dodržovat a plnit nejen povinnosti stanovené obecným nařízením ohledně zpracování osobních údajů, ale také povinnosti jemu stanovené podle ustanovení článku 28 odst. 3 tohoto nařízení ve zpracovatelské smlouvě. Těmito povinnostmi zakotvenými ve zpracovatelské smlouvě správce zajišťuje při zpracování osobních údajů, které zpracovatel provádí pro tohoto správce, dodržování a plnění povinností stanovených obecným nařízením.

Ustanovení článku 28 odst. 3 obecného nařízení stanoví pouze demonstrativní výčet povinností, které zpracovatelská smlouva musí obsahovat a které je zpracovatel povinen dodržovat a plnit. Tudíž ve zpracovatelské smlouvě mohou být zakotveny i další povinnosti zpracovatele, které zajišťují dodržování a plnění povinností při zpracování osobních údajů zpracovatelem stanovené v obecném nařízení. Tyto povinnosti, jestliže takto byly sjednány mezi správcem a zpracovatelem, musí zpracovatel při zpracování osobních údajů pro tohoto správce také dodržovat a plnit.

Obecné nařízení ani zákon o zpracování osobních údajů nezakazují zajistit správcem dodržování a plnění povinností stanovených obecným nařízením při zpracování, jež provádí zpracovatel pro správce ve zpracovatelské smlouvě, smluvní pokutou. Jde o smluvní pokutu, kterou upravuje občanský zákoník (zákon č. 89/2012 Sb.) v případě uzavíraných smluvních vztahů mezi smluvními stranami. Zpracovatelská smlouva je totiž také jedním ze smluvních vztahů uzavíraných mezi smluvními stranami, jimiž jsou správce a zpracovatel. Tato smlouva se řídí nejen ustanovením článku 28 odst. 3 obecného nařízení, ale také příslušnými ustanoveními občanského zákoníku, tudíž se na ni aplikuje nejen toto ustanovení obecného nařízení, ale aplikují se na ni také příslušná ustanovení občanského zákoníku.

S ohledem na uvedené lze konstatovat, že jednou z dalších povinností, kterou lze zakotvit do zpracovatelské smlouvy, jež není uvedena v ustanovení článku 28 odst. 3 obecného nařízení, je povinnost uložená zpracovateli správcem v této zpracovatelské smlouvě, a sice uhradit smluvní pokutu správci. A to pro případ, že zpracovatel při zpracování osobních údajů, které provádí pro správce, neplní povinnosti stanovené mu ve zpracovatelské smlouvě, správcem s ním uzavřené. Tedy i tímto způsobem může správce zajistit dodržování a plnění povinností stanovených obecným nařízením ohledně zpracování osobních údajů při jejich zpracování zpracovatelem.

Omezení výkonu práv subjektu údajů podle článku 23 obecného nařízení v kontextu zákona č. 171/2023 Sb., o ochraně oznamovatelů

V případě, kdy správce osobních údajů obdrží žádost o uplatnění práv subjektu údajů (podle článku 12 až 22 obecného nařízení), a této žádosti v kontextu § 20 odst. 1 zákona č. 171/2023 Sb., o ochraně oznamovatelů, nevyhoví, resp. omezí práva subjektu údajů s ohledem na článek 23 obecného nařízení a § 11 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, je povinen tuto skutečnost bez zbytečného odkladu ohlásit Úřadu. Tato povinnost vyplývá z § 11 odst. 2 zákona o zpracování osobních údajů. Uvedené lze konstatovat mj. i proto, že zákon o ochraně oznamovatelů předmětnou povinnost nevylučuje ani neobsahuje speciální úpravu.

Zpracování biometrických údajů za účelem provozování docházkového systému

Úřad se mj. zabýval zpracováním biometrických údajů za účelem docházkového systému, a sice konkrétně otisku prstů fyzických osob vstupujících do provozů potravinářského průmyslu.

Biometrické údaje jsou podle ustanovení článku 9 odst. 1 obecného nařízení zvláštní kategorii osobních údajů, mezi které patří také otisky prstů. Tuto kategorii osobních údajů je podle citovaného ustanovení zakázáno zpracovávat, není-li aplikována jedna z výjimek z tohoto zákazu uvedených v rámci čl. 9 odst. 2 obecného nařízení. Jelikož právním řádem České republiky není zpracování otisků prstů prostřednictvím docházkového systému za uvedeným účelem povoleno, nelze v České republice podle ustanovení článku 9 odst. 2 písm. b) obecného nařízení zpravidla tyto údaje zpracovávat. Ani hygienické ohledy (kontaminované klíče, karty) nejsou

dostatečným důvodem pro zavedení ověřování za pomoci otisků prstů, které mj. může znamenat obdobné riziko kontaminace.

Udělení výslovného souhlasu podle ustanovení článku 9 odst. 2 písm. a) obecného nařízení se zpracováním biometrických údajů v tomto případě s ohledem na přísné podmínky stanovené především článkem 4 bod 11 a článkem 7 citovaného nařízení není vhodné. V praxi je z pohledu správce především obtížně naplnitelná podmínka svobodného projevu vůle subjektu údajů, jelikož se v rámci uvedené problematiky v drtivé většině případů jedná o zaměstnance, kteří jsou ve vztahu vůči zaměstnavateli obecně považováni za slabší stranu. Rovněž je vzhledem k účelu docházkového systému problematická realizace práva subjektu údajů udělený souhlas kdykoliv odvolat tak snadno, jako byl udělen.

Žádost o poskytnutí kopie telefonické nahrávky v kontextu uplatnění práva subjektu údajů na přístup k osobním údajům podle článku 15 obecného nařízení

Povinností správce podle ustanovení článku 15 obecného nařízení je poskytnout subjektu údajů, který jej požádal o přístup k osobním údajům, osobní údaje jej se týkající. Pokud obsahem nahrávky vzájemného telefonního hovoru pořízeného správcem jsou pouze osobní údaje týkající se tohoto subjektu údajů, jimiž jsou také osobní údaje týkající se fyzické osoby, která jménem správce se subjektem údajů ohledně např. jím uvažovaného či řešeného obchodního vztahu vzájemný telefonní hovor vedla, pak podle ustanovení článku 15 odst. 3 obecného nařízení je povinností správce subjektu údajů poskytnout kopii předmětné nahrávky vzájemného telefonního hovoru v plném rozsahu.

V případě, že by uvedená nahrávka vzájemného telefonního hovoru ohledně např. uvažovaného nebo řešeného obchodního vztahu daného subjektu údajů s tímto podnikatelem obsahovala také osobní údaje, které se netýkají subjektu údajů, který o poskytnutí mu kopie telefonické nahrávky správce požádal, pak povinností správce je před poskytnutím tomuto subjektu údajů této vzájemné nahrávky telefonního hovoru osobní údaje, které se jej netýkají, v ní anonymizovat. Jejich anonymizace musí být provedena tak, aby v původním tvaru nebo po provedeném zpracování tyto osobní údaje nebylo možné vztáhnout k fyzické osobě, resp. k fyzickým osobám, jež vzájemná nahrávka telefonního hovoru také obsahuje, ale netýkají se tohoto subjektu údajů.

V některých případech může být z technických důvodů nezbytné uvést v žádosti o poskytnutí vzájemných nahrávek telefonních hovorů datum pořízení těchto vzájemných telefonních nahrávek a případně také předmět každého z těchto vzájemných telefonních hovorů, a to především za účelem jejich vyhledání.

V této souvislosti je vhodné uvést, že obsahem práva na přístup k osobním údajům podle ustanovení článku 15 obecného nařízení, jímž je podle ustanovení článku 15 odst. 3 obecného nařízení rovněž poskytnutí kopie zpracovávaných osobních údajů, není míněno poskytnutí kopií všech kompletních dokumentů, např. smluv, obsahujících osobní údaje. V určitých případech je postačující uvedení konkrétního soupisu zpracovávaných osobních údajů spolu s vymezením, ve kterých dokumentech jsou předmětné osobní údaje uvedeny.

ANALYTICKÁ ČINNOST ÚŘADU

Inteligentní měření spotřeby energií pohledem ochrany osobních údajů

V kontextu aktuálních evropských snah o efektivní a udržitelné hospodaření s energiemi má významné místo inteligentní měření spotřeby v prostředí inteligentních sítí. V praxi systémy inteligentního či chytrého měření (*smart metering*)[3] zaznamenávají spotřebu energie v oblasti dodávek elektrické energie, vody, teplé vody, tepla či plynu a tato data automaticky poskytují do centrály ke zpracování za různými účе-

3 Pokud jde o použití výrazů inteligentní měřič, inteligentní měřící systém a inteligentní energie (anglické výrazy smart meters a smart metering, smart energy), je z důvodu srozumitelnosti a jednotnosti používána terminologie české verze Směrnice Evropského parlamentu a Rady 2012/27/EU ze dne 25. října 2012 o energetické účinnosti, o změně směrnic 2009/125/ES a 2010/30/EU a o zrušení směrnic 2004/8/ES a 2006/32/ES (Úř. věst., L 315, 14.11.2012), dále jen „směrnice 2012/27/EU o energetické účinnosti".

ly. Zatímco klasické systémy měří jen celkovou spotřebu, inteligentní měřící zařízení mají široké uplatnění. Zákazníkovi, správci domu i poskytovateli energetických služeb přináší pravidelné a detailní informace o aktuálním stavu spotřeby, motivaci k hospodárnosti či další prospěšné funkce.[4] Z anonymizovaných údajů je možné vytvářet agregovaná data o celkové spotřebě, která mohou být využívána orgány EU i ČR pro energetické audity[5] s cílem energetických úspor.

Inteligentní měření je v současné době zaváděno v členských státech EU v návaznosti na harmonizaci evropských směrnic o energetické účinnosti, pilířem je směrnice Evropského parlamentu a Rady 2012/27/EU o energetické účinnosti. V ČR jsou poskytovatelé služeb tepla a centralizovaně poskytované teplé vody povinni od 1. ledna 2024 provádět na základě § 8a zákona č. 67/2013 Sb.[6] dálkový odečet a pravidelně informovat příjemce služeb o spotřebě energií v minimálně měsíčním intervalu, pokud mají instalována dálkově odečitatelná měřidla.[7] Informace o zjištěné spotřebě tepla a teplé vody doručuje poskytovatel služeb příjemci služeb za období kalendářního měsíce, pokud není ujednáno jinak, nikoli však za období delší než jeden měsíc (naopak lze sjednat kratší dobu). Dálkovým odečtem dochází k předávání dat včetně osobních údajů.[8]

Ačkoli je zavedení inteligentního měření spojováno s očekáváním pozitivních přínosů, zároveň může představovat rizika pro ochranu soukromí a osobních údajů. Systémy inteligentního měření totiž umožňují shromažďovat množství detailních osobních údajů z domácností, které by mohly v případě nedostatečného zabezpečení vést nejen ke zjištění dat o spotřebě energie, ale rovněž k detailnímu sledování ve vztahu k soukromí členů domácnosti. V tomto ohledu právní úprava inteligentního měření v EU výslovně odkazuje na požadavek zpracování osobních údajů v souladu s právním rámcem ochrany osobních údajů, především s obecným nařízením na ochranu osobních údajů.

Inteligentní měření zajišťuje více subjektů, které za účelem plnění konkrétních úkolů zpracovávají odpovídající data.[9] V procesu zpracování

4 Mezi přínosy se uvádí vyšší spolehlivost dodávek, možnost úspor na rychle se měnících trzích s energiemi, vzdálené odečítání měření, vývoj nových tarifů a služeb založených na energetických profilech, možnost zjistit výpadek elektrické energie ze sítě či havárii na vodovodním potrubí či přesnější odhad nákladů při hospodaření.

5 Článek 8 směrnice 2012/27/EU o energetické účinnosti předpokládá, že členské státy budou provádět energetické audity.

6 Zákon č. 424/2022 Sb., kterým se mění zákon č. 67/2013 Sb., kterým se upravují některé otázky související s poskytováním plnění spojených s užíváním bytů a nebytových prostorů v domě s byty, ve znění pozdějších předpisů. Tento zákon byl přijat 1. 12. 2022 s účinností od 1. 1. 2023, nicméně ustanovení § 8a o povinnosti dálkového odečtu nabylo účinnosti dnem 1. ledna 2024.

7 Pokud spotřebitelé nemají instalována dálkově odečitatelná měřidla, musí povinnost stanovenou § 8a zákona č. 67/2013 Sb., kterým se upravují některé otázky související s poskytováním plnění spojených s užíváním bytů a nebytových prostorů v domě s byty, splnit nejpozději do konce roku 2027. Ustanovení § 8a odst. 1 a 2 zákona č. 67/2013 Sb. upravuje dálkové odečítání tepla (odstavec 1) a teplé vody (odstavec 2): „Jsou-li instalována dálkově odečitatelná měřidla měřící spotřebu tepla nebo dálkově odečitatelná zařízení pro rozdělování nákladů na vytápění, doručuje poskytovatel služeb příjemci služeb informace o jeho zjištěné spotřebě tepla (teplé vody). Neujedná-li poskytovatel služeb s dvoutřetinovou většinou nájemců v domě jinak, nebo nerozhodne-li jinak družstvo, nebo společenství, poskytuje se informace o zjištěné spotřebě tepla za období kalendářního měsíce a poskytovatel služeb ji doručuje příjemci služeb do konce následujícího kalendářního měsíce."

8 Článek 9 odst. 2 písm. b) směrnice 2012/27/EU o energetické účinnosti: „[Členské státy] zajistí zabezpečení inteligentních měřičů a sdělování údajů a soukromí konečných zákazníků v souladu s příslušnými právními předpisy Unie týkajícími se ochrany údajů a soukromí."

9 Může se jednat např. o poskytovatele energetických služeb, maloobchodní prodejce energie, poskytovatele rozúčtovacích služeb, společenství vlastníků jednotek či družstva.

osobních údajů mohou mít postavení správců, společných správců, zpracovatelů či příjemců dat, pro které obecné nařízení stanoví specifické povinnosti.[10] Před zahájením zpracování je třeba posoudit nezbytnost daného shromažďování osobních údajů ke stanovenému účelu zpracování, který musí být dostatečně určitý. Pokud je tomu tak, je třeba uplatnit obecné zásady a jiné povinnosti ve smyslu obecného nařízení,[11] zvlášť je třeba upozornit na princip minimalizace osobních údajů. Za ochranu osobních údajů během zpracování dat je odpovědný správce,[12] který má k dispozici informace o podrobnostech konkrétního zpracování a o technologii měření, přičemž prokázání souladu zařízení s ochranou osobních údajů by měl správce požadovat po dodavatelích a ti po výrobcích těchto zařízení. V kontextu inteligentního měření je třeba využít nástroje ochrany osobních údajů, jimiž jsou posouzení vlivu, použití principu *privacy by design*, oznámení porušení či sjednání kodexů chování. Ve vztahu k subjektům údajů se uplatní informační povinnost včetně poučení o možnosti uplatnění jejich práv.[13]

Zvlášť efektivním nástrojem ochrany osobních údajů v oblasti inteligentního měření energií je institut posouzení vlivu na ochranu osobních údajů, jehož použití je vhodné v případě složitých a rozsáhlých zpracování osobních údajů. Dozorové úřady pravidelně doporučují využití posouzení vlivu v oblasti inteligentního měření, při splnění podmínek obecného nařízení[14] se jedná o obligatorní požadavek. Významnou pomoc při posuzování vlivu na ochranu osobních údajů může správcům poskytnout Šablona pro posouzení vlivu na ochranu osobních údajů pro chytré sítě a chytré měření, jejíž vznik byl iniciován Evropskou komisí. Ačkoli se nejedná o právně závazný dokument, jde o důležitý a užitečný nástroj pro identifikaci, hodnocení a snižování rizik vyplývajících ze zpracování osobních údajů v oblasti inteligentního měření.

Lze uzavřít, že aktuálnost problematiky inteligentního měření je dána potřebou dosažení udržitelnosti využívání energetických zdrojů, za předpokladu zajištění souladu s ochranou osobních údajů se jedná o žádoucí a prospěšnou regulaci. Zároveň musí být inteligentní měření a systémy inteligentních sítí jako celek navrhovány a provozovány v souladu s jak obecnými, tak se specifickými zárukami ochrany osobních údajů.

Prokazování totožnosti občanskými průkazy

V každodenním životě řada subjektů, veřejných i soukromých, běžně ověřuje totožnost občanů prostřednictvím předložení občanského průkazu či jiných úředních dokladů. Prokazování totožnosti prostřednictvím občanského průkazu, tedy identifikace osoby prostřednictvím zpracování osobních údajů v občanském průkazu ověřující osobou, je považováno za důležité téma ochrany osobních údajů i s ohledem na nové způsoby elektronického prokazování totožnosti. Důvodem je to, že občanský průkaz obsahuje značný rozsah osobních údajů, které mohou být v případě jejich potenciálního úniku zneužity (krádež identity, nevyžádaná obchodní sdělení). Osobní údaje musí být zpracovány v souladu s právním rámcem ochrany osobních údajů, především s obecným nařízením na ochranu osobních údajů. Z této skutečnosti plyne řada požadavků na zpracování osobních údajů, v první řadě musí být zpracování osobních údajů nezbytné a mohou být požadovány pouze osobní údaje přiměřené danému účelu

10 EDPB. Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR. Verze 2.0. Přijato dne 7. července 2021 [online]. [cit. 2024-03-13]. Tyto pokyny mají zásadní význam pro správné nastavení postavení správce, společného správce a zpracovatele při konkrétním zpracování.

11 Zpracování osobních údajů se řídí zásadou zákonnosti, korektnosti a transparentnosti, účelového určení, minimalizace údajů, přesnosti, omezení uložení, integrity a důvěrnosti a odpovědnosti správce.

12 EDPB. Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR. Verze 2.0. Přijato dne 7. července 2021 [online]. [cit. 2024-03-13]. Tyto pokyny mají zásadní význam pro správné nastavení postavení správce, společného správce a zpracovatele při konkrétním zpracování.

13 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) (Úř. věst., L 119, 4.5.2016), dále jen „obecné nařízení". Jedná se o články 12 až 23 obecného nařízení.

14 Článek 35 obecného nařízení.

zpracování. Správce osobních údajů by měl mít již před zahájením zpracování osobních údajů, které je založeno na prokázání totožnosti prostřednictvím předložení občanského průkazu, jasno v aplikaci pravidel ochrany osobních údajů ve vztahu k danému konkrétnímu zpracování, za něž je odpovědný, a měl by o něm rovněž transparentně informovat subjekt údajů.[15]

Z pohledu ochrany osobních údajů je potom rozhodné, jaké osobní údaje identifikující fyzickou osobu jsou požadovány, jakým způsobem dochází k jejich zpracování a jak jsou splněny požadavky, které právní úprava na takové zpracování klade. Správce musí postupovat v souladu se zásadami obecného nařízení, především se zásadou zákonnosti, korektnosti a transparentnosti, účelového omezení, minimalizace osobních údajů ve vztahu k rozsahu osobních údajů, se zásadou přesnosti, resp. aktualizace, omezení doby uložení, principem integrity spočívajícím v organizačním a technickém zabezpečení a zásadou odpovědnosti.[16] Musí rovněž existovat vhodné záruky práv a svobod daného subjektu údajů.[17] Z praktického pohledu zpracování osobních údajů bude přitom relevantní, zda jde o prokazování totožnosti vůči orgánům veřejné moci či o soukromoprávní vztahy. Občan ve vztahu k danému zpracování může uplatnit svá práva podle čl. 12 až 22 obecného nařízení, jimiž jsou především právo na přístup, právo na výmaz či právo podat námitku.

V případě zpracování osobních údajů v občanském průkazu se uplatní právní úprava zákona č. 269/2021 Sb. o občanských průkazech ze dne 1. 7. 2021, která zakazuje nedovolené nakládání s občanským průkazem, za něž výslovně považuje odebírat občanský průkaz při vstupu do objektů nebo na pozemky, přijímat občanský průkaz jako zástavu, pořizovat kopii občanského průkazu bez souhlasu držitele občanského průkazu a zpracovávat údaje uvedené v občanském průkazu s výjimkou nahlédnutí do občanského průkazu v souvislosti s ověřováním totožnosti.[18] Popsaná jednání mohou být přestupky podle zákona o občanských průkazech.[19] Tím není dotčena působnost dozorového úřadu na ochranu osobních údajů podle obecného nařízení.[20]

S rozvojem reprodukční techniky a používáním mobilních telefonů se velmi rozšířilo pořizování kopií listinných dokumentů včetně průkazů totožnosti jako důkazu, že osobní údaje byly z veřejné listiny zaznamenány správně. Pořizování kopií (skenování) je často nadužíváno. Většinou by přitom vyžadující osobě postačovalo předložení originálu veřejné listiny a zaznamenání pouze nezbytných údajů, včetně čísla průkazu totožnosti a kým byl vydán. Podle občanského zákoníku platí, že je-li nějaká skutečnost potvrzena ve veřejné listině, zakládá to vůči každému plný důkaz o původu listiny od orgánu nebo osoby, které ji zřídily, o době pořízení listiny, jakož i o skutečnosti, o níž původce veřejné listiny potvrdil, že se za jeho přítomnosti udála nebo byla provedena, dokud není prokázán opak.[21] Orgány veřejné moci při kontrole totožnosti fyzické osoby zpravidla pořizovat kopii průkazu totožnosti nepotřebují a zákon jim takový postup neukládá. Ustanovení § 39 písm. c) zákona o občanských průkazech uvádí výčet nedovoleného nakládání s občanským průkazem, mj. zakazuje pořizovat kopii občanského průkazu bez souhlasu držitele občanského průkazu. Poruší-li osoba, jíž byl občanský průkaz vydán, některý ze zákazů uvedených v daném ustanovení, dopustí se přestupku podle § 65 odst. 1 písm. b) až e) citovaného zákona.

Pokud jde o problematiku prokazování totožnosti prostřednictvím občanského průkazu či jiných platných úředních dokladů, pro občany je dobré vědět, kdy jsou povinni předložit občanský průkaz a kdy je naopak jeho poskytnutí v jejich dispozici, případně namísto občanského průkazu mohou poskytnout jiný doklad nebo

15 Pracovní skupina zřízená podle článku 29. Pokyny k transparentnosti podle nařízení 2016/679 (WP260 rev.01). Přijaty dne 29. listopadu 2017 ve znění naposledy revidovaném a přijatém dne 11. dubna 2018 [online]. [cit. 2024-03-13].

16 Články 5 a 6 obecného nařízení.

17 Článek 87 obecného nařízení.

18 Ustanovení § 39 zákona č. 269/2021 Sb., o občanských průkazech.

19 Ustanovení § 65 odst. 1 písm. b), c) a d) zákona č. 269/2021 Sb., o občanských průkazech.

20 Článek 55 obecného nařízení.

21 Ustanovení § 568 odst. 1 zákona č. 89/2012 Sb., občanský zákoník.

jinak prokázat totožnost. Měli by být rovněž informováni, že podle platné právní úpravy je za nedovolené nakládání s občanským průkazem považováno odebírání občanského průkazu při vstupu do objektů nebo na pozemky, přijímání občanského průkazu jako zástavy či pořizování kopie občanského průkazu bez souhlasu jeho držitele, pokud se nejedná o výjimku stanovenou zákonem. V případě pochybností by se měli dotázat správce osobních údajů či dozorového úřadu na ochranu osobních údajů, zda je zamýšlené zpracování osobních údajů nezbytné a zda je v souladu se zásadami ochrany osobních údajů, případně zda je není možné nahradit jiným postupem jako je např. nahlédnutí nebo zaznamenání potřebného osobního údaje nezbytného v daném kontextu.

Analýza národních identifikačních čísel (rodných čísel) pro veřejný sektor

Rodné číslo je jednoznačným významovým a neměnným identifikátorem fyzické osoby, který je upraven ve zvláštním zákoně, tj. v zákoně o evidenci obyvatel, kde jej upravuje § 13 až 17ca v hlavě III zákona. Stručná zákonná definice rodného čísla uvedená v § 13 tohoto zákona uvádí, že v informačním systému je rodné číslo identifikátorem fyzické osoby, která splňuje podmínky pro jeho přidělení podle zákona.

Rodné číslo se od svého zavedení v roce 1953 stalo klíčovým údajem pro identifikaci občanů a je součástí datových souborů naprosté většiny veřejnoprávních i soukromoprávních agend. Veřejná správa i soukromé subjekty jej používají i pro prvotní ztotožnění klienta při zahájení komunikace. Základním problémem je „všudypřítomnost" a „neměnnost" údaje o rodném čísle, přičemž tomu napomáhá jeho plošné použití v čísle pojištěnce zdravotního pojištění, stejně jako jeho použití v položce DIČ u podnikajících fyzických osob. V dnešní době tak stačí pouze běžné vybavení výpočetní technikou a propojení jednotlivých zařízení globální datovou sítí, aby docházelo k nežádoucímu propojování jednotlivých datových fondů. Výsledné informace pak mohou být „zneužívány" k různým obchodním, marketingovým či jiným účelům v neprospěch osoby nositele rodného čísla. Z pohledu ochrany osobních údajů se jedná o nežádoucí stav a občané mají minimální možnosti obrany. V okamžiku, kdy dojde k případnému nekontrolovanému rozšíření tohoto údaje prostřednictvím internetové sítě, je tento proces zpravidla nevratný; nadto kompromitované rodné číslo nelze nahradit, neboť je až na výjimky neměnným údajem. Úřad s ohledem na tato rizika dlouhodobě navrhuje nahrazení rodných čísel bezvýznamovým identifikátorem či identifikátory.

Regulativní přístup jednotlivých členských států EU k národním identifikačním číslům se značně liší.[22] Typově lze hovořit o dvou skupinách identifikátorů. Některé země používají jedinečný identifikátor (*unique identifier*), resp. národní identifikační číslo s obecnou působností, které se používá ve všech oblastech veřejného sektoru. Sem patří například Francie, Belgie, Švédsko, Španělsko, Nizozemí nebo Německo. V některých případech se jedná o významový identifikátor, z něhož lze zjistit i další osobní údaje osoby, zpravidla pohlaví osoby, datum narození, někdy i místo narození – to je případ Francie, Belgie, Slovenska i Švédska. Naproti tomu, Španělsko, Německo a Nizozemí používají bezvýznamový obecný identifikátor. Na Slovensku byl v roce 2019 schválen návrh zákona o základních identifikátorech fyzické osoby, který měl zavést systém nových identifikátorů fyzických osob. Mělo by se jednat o tzv. BIFO (bezvýznamový identifikátor fyzických osob), který by nahradil současná rodná čísla, a tzv. SIFO (sektorový identifikátor fyzické osoby), který by měl být využíván při elektronické komunikaci mezi orgány veřejné správy. Zákon však prozatím nebyl schválen parlamentem. Německá právní úprava obecně nezná obdobu rodného čísla občanů. Veřejné orgány využívaly do přijetí zákona o mo-

22 KUNER, Christopher, BYGRAVE, Lee A. a DOCKSEY, Christopher. The EU General Data Protection Regulation (GDPR): A Commentary [online]. Oxford University Press, 2020, s. 1223-1228 [cit. 2024-03-13]. ISBN 9780191932267.
VANDEZANDE, Niels. Identification numbers as pseudonyms in the EU public sector [online]. 2011(Vol. 2, No. 2) [cit. 2024-03-13].
Parlamentní institut francouzského Senátu. Le numéro unique d'identification des personnes physiques (Jedinečné identifikační číslo fyzických osob): Étude de législation comparée n° 181 (Srovnávací legislativní studie č. 181) [online]. 2007 [cit. 2024-03-13].

dernizaci rejstříků[23] v rámci příslušné agendy své „vlastní" identifikátory, například číslo sociálního pojištění. Nakonec bylo přistoupeno k variantě obecného (bezvýznamového) identifikátoru s tím, že základem pro tento jednotný identifikátor je již existující daňové identifikační číslo.

Jinou skupinou jsou země, které v rámci veřejného sektoru používají zvláštní sektorová nebo agendová čísla (*sector-based identifiers*), přičemž je používají pouze v rámci jednoho konkrétního odvětví (např. daňové identifikační číslo nebo číslo sociálního pojištění) a staví se proti používání jednotných identifikátorů. Sem patří Rakousko nebo Portugalsko. Rakousko nezná obdobu našeho rodného čísla, existují ale identifikátory pro specifickou oblast, přičemž nejrozšířenějším je číslo sociálního pojištění. Portugalsko je jedinou zemí, kde přímo Ústava výslovně zakazuje přidělování jedinečného identifikačního čísla fyzickým osobám.[24] Používání národního identifikačního čísla a přístup k němu je mezi členskými státy upraveno rovněž odlišně. Například v Belgii lze použít národní identifikační číslo (z vnitrostátního rejstříku) pouze k výslovně upraveným účelům, pokud je povoleno zákonným nebo prováděcím předpisem. Obdobně to funguje ve Francii, kde musí být použití upraveno v právním předpise.[25] Lze nicméně zaznamenat trend, že používání obecných významových identifikátorů se v čase snižuje.

V České republice ve veřejném sektoru již několik let probíhá z pohledu ochrany osobních údajů žádoucí proces utlumování využívání rodných čísel. Prvním krokem pro snížení četnosti používání rodných čísel ve veřejném sektoru bylo přijetí zákona č. 111/2009 Sb., o základních registrech, který zavedl systém základních registrů (4 základní registry a informační systém základních registrů). Zákon zavedl koncepci, kdy jsou fyzickým osobám v agendových informačních systémech přiděleny jedinečné a bezvýznamové identifikátory (tzv. AIFO), tj. jedna osoba je v jednotlivých agendách vedena pod různými identifikátory. Jednotný a nezměnitelný identifikační údaj (rodné číslo) o fyzické osobě byl nahrazen zdrojovým identifikátorem fyzické osoby (ZIFO) a mnoha agendovými identifikátory fyzické osoby (AIFO). Pokud jde o soukromý sektor, byl v ČR od července 2022 zaveden bezvýznamový směrový identifikátor (BSI),[26] který by mohl představovat účinnou alternativu k využívání rodných čísel a mohl by být obdobou AIFO pro soukromý sektor.

Dne 1. ledna 2024 ovšem nabyl účinnosti zákon č. 430/2023 Sb., který změnil zákon o občanských průkazech a insolvenční zákon. Zákon umožňuje i po 31. prosinci 2024 zapisovat rodná čísla do občanských průkazů. Podle důvodové zprávy se bude rodné číslo do občanského průkazu zapisovat povinně a bez časového omezení. Tím z pohledu Úřadu došlo k odklonu od dosavadního vývoje utlumování rodných čísel. Úřad již dříve uvedl, že uvádění rodného čísla v občanském průkazu představuje závažná rizika z hlediska ochrany osobních údajů a soukromí, a to mj. v souvislosti s jejich dostupností a možnostmi propojování dat a jejich zneužití ve virtuálním prostoru. Velikým problémem v ČR totiž zůstává snadné předávání občanských průkazů a další nakládání s těmito průkazy, zejména kopírování, fotografování a skenování, a to jak ze strany veřejnoprávních, tak soukromoprávních subjektů. Přes výše uvedenou legislativní změnu lze nicméně doufat, že v budoucnu dojde s postupným prosazováním ochrany osobních údajů k přehodnocení používání rodného čísla, které bude nahrazeno bezvýznamovým identifikátorem.

23 Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG). (Německý) Zákon o zavedení a používání identifikačního čísla ve veřejné správě a o změně některých zákonů (zákon o modernizaci rejstříků – RegMoG).

24 Článek 35 odst. 5 portugalské Ústavy výslovně uvádí: „Přidělení jediného národního čísla kterémukoli občanovi je zakázáno." (oficiální anglický překlad)

25 Dekret francouzské Státní rady č. 2019–341 z 19. dubna 2019 o provádění zpracování zahrnující použití registračního čísla v národním registru pro identifikaci fyzických osob nebo vyžadujícího nahlížení do tohoto registru.

26 Nový § 12a byl zaveden zákonem č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci. Konkrétně se jedná o část sto šedesátou pátou (čl. 178) - změna zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění zákona č. 36/2021 Sb.

NÁRODNÍ LEGISLATIVA

Rok 2023 byl rokem poloviny volebního období Poslanecké sněmovny, pro níž je typicky připraveno do připomínkového řízení značné množství právních předpisů. Setrvala zvýšená aktivita v podobě osnov právních předpisů, obdobně jako v roce 2022, kdy byl s Úřadem projednáván jeden návrh věcného záměru zákona, 59 návrhů zákonů, 25 návrhů vládního nařízení, 49 návrhů vyhlášek a 22 nelegislativních dokumentů. Za rok 2023 to byly dva návrhy věcného záměru zákona, 67 návrhů zákona, 18 návrhů nařízení vlády, 57 návrhů vyhlášek, 10 mezinárodních smluv a 22 nelegislativních dokumentů. Největší množství návrhů bylo do připomínkového řízení zasláno Ministerstvem financí. Ministerstvo vnitra se soustředilo na bilaterální smlouvy o policejní spolupráci (s Filipínami, se Slovenskem, s Mongolskem, se Spojenými arabskými emiráty, s Thajskem, s Koreou, s Egyptem a s Uzbekistánem). Zatím nezodpovězenou otázkou zůstává, zda by nebylo vhodnějším řešením sjednání multilaterální smlouvy o policejní spolupráci.

S ohledem na ochranu osobních údajů lze považovat za zásadní návrh zákona, kterým se mění zákon č. 269/2021 Sb., o občanských průkazech, ve znění zákona č. 471/2022 Sb., a zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů[27], který je z pohledu Úřadu krokem zpět a poškozuje navržený model eGovernmentu, proto k tomuto návrhu nemohl Úřad zaujmout pozitivní stanovisko. Navrhuje se totiž zrušit dosud platné ustanovení, které počítá s koncem zapisování rodných čísel do občanských průkazů od roku 2025.[28] Tento návrh rovněž pomíjí skutečnost, že již byla vytvořena ucelená koncepce identifikátorů (ZIFO, AIFO, KIFO a BSI), kterou v tomto roce převzala Digitální informační agentura a dále ji plánuje rozvíjet. V praxi dochází běžně k předávání občanských průkazů, jejich kopírování, fotografování a skenování. Přitom je nemožné zabránit pořízení další kopie či zneužití rodného čísla. To se přitom děje nejen v České republice, ale ve vztahu k našim občanům i v rámci Evropské unie v oblasti volného pohybu osob. Uvádění rodného čísla v občanském průkazu představuje závažná rizika z hlediska ochrany osobních údajů, a to mj. v souvislosti s propojováním dat a možnosti jejich zneužití ve virtuálním prostoru, kde existují jen velmi obtížné možnosti kontroly a nápravy. Při dnešních schopnostech výpočetní techniky doplněných propojením jednotlivých zařízení globální datovou sítí je možné datové fondy nekontrolovaně spojovat a výsledné informace využívat k nejrůznějším komerčním, marketingovým či jiným účelům v neprospěch osoby jejich držitele. To je nejen z pohledu ochrany osobních údajů nežádoucí stav, kterému se nelze účinně bránit, protože v okamžiku nekontrolovaného rozšíření či dokonce zveřejnění rodného čísla není (vyjma zcela mimořádných případů) možné jej běžným způsobem změnit. Neuvádění rodného čísla v občanském průkaze přitom neznamená jeho zrušení, ale pouze to, že se výrazně omezí možnost jeho potenciálního zneužití. Takové opatření by představovalo podstatné zvýšení standardu ochrany jednotlivce z pohledu základního práva na ochranu osobních údajů.

Naopak pozitivně s ohledem na ochranu osobních údajů hodnotí Úřad přípravu reformy

27 Sněmovní tisk 546.

28 Přitom již byly stanoveny 4 termíny pro ukončení zápisu rodného čísla do občanských průkazů:
a) Článek IX bod 2 novely č. 424/2010 Sb. zněl: „Zápis rodného čísla do občanského průkazu se ukončuje dnem 31. prosince 2019."
b) Druhý termín stanovila novela č. 370/2019 Sb. do 31. prosince 2021.
c) Třetí termín stanovila novela č. 261/2021 Sb. (DEPO) do 31. prosince 2023. Paralelně stejnou lhůtu stanovil § 72 odst. 10 zákona č. 269/2021 Sb., o občanských průkazech.
d) Čtvrtý termín stanovila novela č. 471/2022 Sb. do 31. prosince 2024.

digitálního prostředí zpracovanou Ministerstvem průmyslu a obchodu v návrhu zákona o digitální ekonomice. Tento právní předpis implementuje nařízení o digitálních službách (DSA), částečně rovněž Akt o správě dat (DGA) a směrnici o soukromí a elektronických komunikacích (ePD). Navrhovaná právní úprava má přispět k zajištění správného fungování vnitřního trhu v oblasti digitální a datové ekonomiky prostřednictvím zajištění jasného a předvídatelného právního rámce pro vymáhání povinností plynoucích ze souvisejících právních předpisů EU a provést s tím spojenou adaptaci právního řádu České republiky na DGA (kromě kapitoly II) a DSA. To zahrnuje jednak určení příslušných orgánů, které odpovídají za vymáhání DGA a DSA a stanovení pravidel týkajících se sankcí za porušení DGA a DSA, ale také zajištění sjednoceného právního rámce pro služby informační společnosti a datovou ekonomiku. Jako orgán odpovědný za dozor a vymáhání DGA a DSA byl navržen Český telekomunikační úřad. Jako další příslušný orgán pro dozor a vymáhání nařízení o digitálních službách byl navržen Úřad pro ochranu osobních údajů, a to pro články 26 a 28 odst. 2 DSA, tedy konkrétně mu má být svěřen dozor a vymáhání nařízení v oblasti šíření obchodních sdělení, reklamy na online platformách a ochrany nezletilých osob na internetu.

Komplikované je připomínkové řízení v případě úpravy šíření údajů z katastru nemovitostí, kde prozatím mezi Českým úřadem zeměměřickým a katastrálním a Úřadem pro ochranu osobních údajů nepanuje shoda. Úřad pro ochranu osobních údajů k této problematice zaujímá stanovisko, že veřejnoprávní rejstříky obsahují nuceně poskytnuté osobní údaje, tedy že subjekty údajů se nemohou rozhodnout, zda v něm jejich osobní údaje budou, či nebudou uvedeny, pokud chtějí být nositeli určitého oprávnění. V tomto konkrétním případě nemohou být nositelem věcného práva k nemovité věci bez zápisu v katastru nemovitostí. Proto Úřad pro ochranu osobních údajů nesouhlasil s vytvořením soukromoprávních kopií veřejnoprávních rejstříků, což je v rozporu s názorem Českého úřadu zeměměřického a katastrálního, který naproti tomu chce v určité podobě podnikaní s daty o vlastnících a jiných nositelích věcných práv k nemovitým věcem umožnit.

Dalším předpisem, který se bezprostředně dotýkal působnosti Úřadu, byl návrh nového cizineckého zákona, který upravuje i justiční a policejní spolupráci v rámci EU. Úřad k tomuto předpisu uplatnil řadu připomínek, kde k nejvýznamnějším patřil požadavek na vyhodnocení dodatečných informací k záznamu v Schengenském informačním systému a vyjasnění správy Vízového informačního systému mezi Policií ČR a Ministerstvem zahraničních věcí. Připomínky byly projednány s Ministerstvem vnitra a vedly k úpravám tohoto rozsáhlého návrhu.

V oblasti organizace a fungování Úřadu bylo pro Úřad zásadní připomínkové řízení k návrhu změny zákona č. 234/2014 Sb., o státní službě, a návrh nařízení vlády, kterým se mění nařízení vlády č. 92/2015 Sb., o pravidlech pro organizaci služebního úřadu, které v předloženém znění představují ohrožení nezávislosti Úřadu zejména tím, že by pro státní zaměstnance zařazené v Úřadu byly závazné služební předpisy nejvyššího státního tajemníka, a dále tím, že by Úřad musel zásadně změnit svou organizační strukturu, aby dostál novým pravidlům pro velikost organizačních útvarů. Zatímco na závaznosti služebních předpisů nejvyššího státního tajemníka předkladatel nadále trvá a je tedy mezi ním a Úřadem rozpor, po dohodě se sekcí pro státní službu novela nařízení vlády nebude mít na Úřad tak zásadní negativní dopad, jak vyplývalo z původně navržené verze, byť je jisté, že Úřad bude s účinností od 1. července 2024 nucen přistoupit ke změnám organizační struktury.

Zásadní vliv na fungování Úřadu má i konsolidace veřejných rozpočtů, která je v první fázi založena na plošných škrtech na výdajové stránce, nicméně jako vhodnější způsob konsolidace veřejných rozpočtů se jeví rušení nepotřebných agend, které by ale mělo následovat až ve druhé fázi. V případě Úřadu mají plošné škrty na výdajové stránce vliv na fungování Úřadu jako nezávislého ústředního správního úřadu pro oblast ochrany osobních údajů, zejména vzhledem k personálnímu obsazení, které je již řadu let v nepoměru k rozsahu vykonávaných agend a stále se rozšiřující působnosti Úřadu. Personální zabezpečení Úřadu je pak obsahem samostatné kapitoly této výroční zprávy.

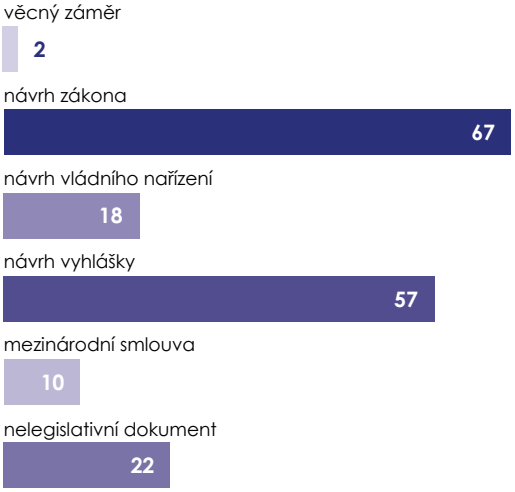
Úřad rozporoval některé návrhy Ministerstva spravedlnosti, a to zejména redefinici znásilnění a absolutní zákaz veškerého trestání dětí, tělesného i psychického, v nichž zejména poukazoval na nevhodnost změny tak zakořeněných právních institutů. V druhém případě se shodl s Nejvyšším soudem, který rovněž upozornil na úskalí deklaratorně imperfektní právní normy. Změna právní regulace výchovy dětí může navíc vést k nežádoucím zásahům do soukromí rodiny.

Závěrem této části Úřad ještě považuje za vhodné uvést, že se neztotožňuje se snahami považovat každou regulaci za právní předpis, a to zejména s ohledem na skutečnost, že se velmi často jedná pouze o obecně konkrétní akt nebo o individuálně abstraktní akt, tedy o všeobecné opatření – opatření obecné povahy v souladu s názvoslovím správního řádu. Typickým příkladem všeobecného opatření jsou formuláře, které jsou v souladus nálezem ÚS z 12. listopadu 2019, sp. zn. Pl. ÚS 19/17, a rozsudkem NSS z 31. ledna 2023, čj. 2 Afs 395/2020–55 stále více vydávány v podobě vyhlášek nebo popisů datových rozhraní pro komunikaci mezi veřejnou správou a jejími adresáty. S ohledem na výše uvedené skutečnosti a v souvislosti se změnou legislativních pravidel vlády, která mimo jiné upravují podrobnější strukturu zhodnocení dopadů na soukromí, včetně dopadů v ochraně osobních údajů (DPIA), v návrzích právních předpisů v souladu s GDPR nebo trestněprávní směrnicí, připravil Úřad pro veřejnou diskusi nový návod pro vypracování DPIA. Tento návrh návodu pro vypracování DPIA se setkal se širokým zájmem veřejnosti, který vedl k řadě komentářů, které v současné době Úřad vyhodnocuje a v případě relevantních komentářů přistoupí k úpravě návrhu.

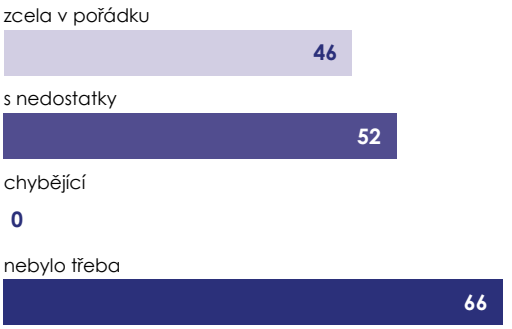
UNIJNÍ LEGISLATIVA

V případě unijní legislativy věnoval Úřad nejvíce pozornosti návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679 (DPPR), který se formálně týká pouze přeshraničních případů dozoru nad zpracová-

DRUHY PŘIPOMÍNKOVANÝCH NÁVRHŮ



VYHODNOCENÍ POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ – DPIA



ním osobních údajů, avšak lze očekávat, že soudy mohou základní principy, na kterých je tento návrh postaven, rozšířit i na případy dozoru nad zpracování osobních údajů v rozsahu národního zpracování osobních údajů. Jeví se proto jako nezbytné, aby Rada EU omezila věcnou působnost DPPR na zvláště významné případy s precedentní hodnotou a náležitě definovala institut stížnosti jako podání ve vlastní věci, kde podatel sleduje svůj vlastní zájem ve stížnosti náležitě vymezený. Stížnost se tak ještě více připodobní žalobě, včetně dispoziční zásady.

V prosinci 2023 bylo dosaženo shody nad textem nařízení o umělé inteligenci (angl. Artificial Intelligence Act, AIA)[29], který má stanovit komplexní celoevropská pravidla pro používání systémů využívajících AI technologii. Účinnost předpisu bude za 2 roky (některé povinnosti nabydou účinnosti i dříve). Podle návrhu by měly být zakázány systémy, které manipulují s lidským chováním tak, aby obešly svobodnou vůli uživatele, systémy pro takzvané sociální hodnocení (social scoring) nebo systémy pro prediktivní hodnocení lidí. Úřad upozorňoval na rizika spojená zejména s využíváním biometrické identifikace ve veřejných prostorách v reálném čase. Výsledný text je kompromisem, který toto zakazuje s výjimkami schválenými na celostátní úrovni.

Překvapivý vývoj měla jedna z priorit českého předsednictví Rady EU v roce 2022, a to návrh nařízení Evropského parlamentu a Rady, který by měl stanovit pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu (CSA). Vzhledem ke skutečnosti, že se proti jeho schválení na české straně postavila řada resortů (včetně ÚOOÚ) a na půdě Rady EU některé členské státy, španělskému předsednictví se nepodařilo prosadit původně zamýšlený obecný přístup Rady. Evropská komise proto 30. listopadu 2023 navrhla prodloužení účinnosti prozatímního nařízení o 2 roky. Úřad s tím vyjádřil nesouhlas kvůli vadám nařízení (jedná se zejména o problém plošnosti a nepřiměřenosti zamýšlených opatření a celkový dopad na ztrátu soukromí uživatelů).

29 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.

UNIJNÍ JUDIKATURA

V prosinci 2023 vydal Soudní dvůr EU dvě rozhodnutí se zásadním dopadem na ukládání pokut za porušení obecného nařízení právnickým osobám. Jde konkrétně o rozsudky Soudního dvora (velkého senátu) o předběžné otázce ze dne 5. prosince 2023 ve věcech C-683/21 (Nacionalinis visuomenės sveikatos centras) a C-807/21 (Deutsche Wohnen).

Věc C-683/21 (Nacionalinis visuomenės sveikatos centras v. Valstybinė duomenų apsaugos inspekcija)[30]

V roce 2020 litevské orgány v souvislosti s pandemií onemocnění Covid-19 zamýšlely zavést mobilní aplikaci pro evidenci a sledování údajů o osobách vystavených viru SARS-CoV-2. Národní středisko pro veřejné zdraví při litevském ministerstvu zdravotnictví (Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, dále jen „NVSC“), které bylo pověřeno pořízením mobilní aplikace, se proto obrátilo na společnost „IT sprendimai sėkmei“ (dále jen „společnost ITSS“) a požádalo ji o vytvoření takové mobilní aplikace. Zaměstnanci NVSC následně této společnosti zaslali e-maily týkající se zejména otázek, které měly být v této aplikaci uvedeny. Přestože NVSC neudělilo povolení se zpřístupněním mobilní aplikace, kterou společnost ITSS vyvinula, veřejnosti ani s ním nesouhlasilo, byla mobilní aplikace v období od dubna do května 2020 zpřístupněna ke stažení prostřednictvím internetových obchodů Google Play Store a Apple App Store. Aplikaci využilo celkem 3 802 osob, jež poskytly různé osobní údaje požadované uvedenou aplikací. Z důvodu nedostatku finančních prostředků však NVSC nezadalo společnosti ITSS žádnou veřejnou zakázku na oficiální pořízení této mobilní aplikace a příslušné řízení ukončilo. Litevský dozorový úřad zahájil v mezidobí šetření týkající se zpracování osobních údajů plynoucího z používání uvedené aplikace, přičemž po skončení šetření rozhodnutím uložil NVSC pokutu 12 000 eur a společnosti ITSS, která byla považována za společného správce, pokutu 3 000 eur.

30 Rozsudek je dostupný na stránkách Soudního dvora curia.europa.eu

NVSC rozhodnutí napadlo u Krajského správního soud ve Vilniusu (Vilniaus apygardos administracinis teismas), který předložil Soudnímu dvoru žádost o rozhodnutí o předběžné otázce, a to s otázkami týkajícími se výkladu pojmu „správce", „společní správci" a „zpracování", a také možnosti ukládání pokut správci, pokud k porušení povinnosti stanovené GDPR nedošlo úmyslně nebo z nedbalosti. Právě odpověď na poslední položenou otázku představuje koncepčně odlišný náhled, než jakým se řídí ukládání pokut za správní delikty (přestupky) právnických osob v českém právním řádu: Soudní dvůr konstatoval, že „*článek 83 nařízení 2016/679 musí být vykládán v tom smyslu, že správní pokutu lze na základě tohoto ustanovení uložit pouze tehdy, je-li prokázáno, že se správce dopustil porušení uvedeného v odstavcích 4 až 6 tohoto článku úmyslně nebo z nedbalosti*", tedy zaviněně, přičemž podle Soudního dvora unijní normotvůrce neponechal členským státům prostor pro uvážení, pokud jde o hmotněprávní podmínky, které musí dozorový úřad dodržet, rozhodne-li se uložit správci správní pokutu na základě tohoto ustanovení.

Soudní dvůr dále dospěl k závěru, že takovou pokutu lze správci uložit v souvislosti s operacemi zpracování osobních údajů, které pro něj provedl zpracovatel, ledaže tento zpracovatel v rámci těchto operací provedl zpracování pro vlastní účely nebo zpracoval tyto údaje způsobem neslučitelným s rámcem nebo postupy zpracování, jak byly stanoveny správcem, nebo takovým způsobem, že nelze mít důvodně za to, že by s ním tento správce souhlasil. V takovém případě musí být zpracovatel považován za odpovědného za takové zpracování.

Věc C-807/21 (Deutsche Wohnen SE v. Staatsanwaltschaft Berlin)[31]

Deutsche Wohnen SE (dále jen „společnost DW") je kotovaná realitní společnost se sídlem v Berlíně, která prostřednictvím podílů v různých dceřiných společnostech nepřímo vlastní cca 163 000 bytových jednotek a 3 000 komerčních prostor. DW v souvislosti se svojí podnikatelskou činností společně s dceřinými společnostmi zpracovávají osobní údaje nájemců těchto prostor a jednotek. V roce 2017 dozorový úřad v Berlíně (Berliner Beauftragte für den Datenschutz) v rámci kontroly zjistil, že společnosti v rámci skupiny DW uchovávají dokumenty obsahující osobní údaje nájemců v elektronickém archivačním systému, u něhož nelze ověřit, zda je toto uchovávání nezbytné, a zajistit, aby údaje, které již nejsou potřebné, byly vymazány, proto dozorový úřad společnost DW požádal, aby do konce roku 2017 tyto dokumenty z předmětného systému vymazala, což DW odmítla s tím, že výmaz není z technických a právních důvodů možný a že hodlá vytvořit nový systém pro uchovávání dat. Berlínský dozorový úřad provedl v ústředí společnosti DW opětovnou kontrolu v roce 2019, při které DW sdělila, že předmětný elektronický archivační systém už byl vyřazen z provozu a neprodleně bude provedena migrace údajů do nového systému pro uchovávání dat. Návazně na toto zjištění uložil dozorový úřad společnosti DW pokutu ve výši 14 385 000 eur za úmyslné porušení čl. 5 odst. 1 písm. a), c) a e) a čl. 25 odst. 1 obecného nařízení, a 15 dalších pokut ve výši od 3 000 do 17 000 eur za porušení čl. 6 odst. 1 obecného nařízení.

Společnost DW podala žalobu k Zemskému soudu v Berlíně (Landgericht Berlin), který shledal, že napadené rozhodnutí nemůže být podkladem pro uložení pokuty, mj. protože ukládání pokuty právnické osobě je vyčerpávajícím způsobem upraveno v § 30 OWiG , který se podle § 41 odst. 1 spolkového zákona o ochraně údajů vztahuje na porušení uvedená v čl. 83 odst. 4

31 Rozsudek je dostupný na stránkách Soudního dvora curia.europa.eu

až 6 obecného nařízení. Podle § 30 OWiG[32] však lze spáchání správního deliktu konstatovat pouze vůči fyzické osobě, a nikoli vůči osobě právnické. Kromě toho právnické osobě lze přičíst pouze jednání členů jejích orgánů nebo jejích zástupců. Přestože odstavec 4 zmíněného § 30 za určitých podmínek umožňuje zahájení samostatného řízení o správním deliktu vůči právnické osobě, nic to podle soudu nemění na skutečnosti, že i v tomto případě se vyžaduje, aby bylo možné spáchání správního deliktu konstatovat ve vztahu k členům orgánů nebo zástupcům dotyčné právnické osoby.

Proti rozhodnutí Zemského soudu v Berlíně podalo Státní zastupitelství v Berlíně (Staatsanwaltschaft Berlin) odvolání k Vrchnímu zemskému soudu v Berlíně (Kammergericht Berlin), který předložil Soudnímu dvoru žádost o rozhodnutí o předběžné otázce týkající se podmínek ukládání pokut na základě obecného nařízení právnickým osobám. Soudní dvůr se tak zabýval otázkou, zda členské státy mohou uložení správní pokuty právnické osobě podmínit tím, že porušení obecného nařízení bylo předtím přičteno identifikované fyzické osobě, a dále zda musí k sankcionovanému porušení ustanovení obecného nařízení dojít úmyslně nebo z nedbalosti.

Soudní dvůr dospěl k závěru, že obecné nařízení brání vnitrostátní právní úpravě, podle které lze uložit správní pokutu právnické osobě jakožto správci za porušení tohoto nařízení pouze tehdy, pokud bylo toto porušení předtím přičteno identifikované fyzické osobě. Soudní dvůr v této souvislosti konstatoval, že obecné nařízení nerozlišuje pro účely určování odpovědnosti správce za porušení obecného nařízení mezi fyzickými a právnickými osobami, tato odpovědnost je pak podmíněna pouze tím, že tyto osoby samy nebo společně s jinými určují účely a prostředky zpracování osobních údajů, a tedy že každá osoba splňující uvedenou podmínku v zásadě odpovídá mimo jiné za jakékoli porušení obecného nařízení, kterého se dopustila sama nebo bylo spácháno jejím jménem. To podle Soudního dvora znamená, že právnické osoby jsou odpovědné nejen za porušení, kterých se dopustili jejich zástupci, řídící pracovníci nebo manažeři, ale i jakékoliv jiné osoby, které jednají v rámci obchodní činnosti těchto právnických osob jejich jménem a že pokud lze právnické osoby považovat za správce, musí být možné jim v případě takových porušení přímo uložit správní pokuty podle obecného nařízení. Z žádného ustanovení obecného nařízení nelze podle Soudního dvora dovodit, že by podmínkou uložení správní pokuty právnické osobě jakožto správci bylo předchozí konstatování, že se tohoto porušení dopustila identifikovaná fyzická osoba, a bylo by v rozporu s účelem obecného nařízení, kdyby jakožto nezbytnou podmínku pro uložení správní pokuty správci, který je právnickou osobou, podle článku 83 obecného nařízení, členské státy mohly jednostranně požadovat, aby dotčené porušení předtím bylo nebo mohlo být přičteno identifikované fyzické osobě. Pojem „podnik" ve smyslu článků 101 a 102 Smlouvy o fungování Evropské unie je přitom relevantní pouze při určování výše pokuty, nikoliv pro určení, zda a za jakých podmínek může být správci, který je právnickou osobou, uložena pokuta podle obecného nařízení.

I v tomto rozhodnutí pak Soudní dvůr potvrdil výše uvedený náhled, že pokuty lze na základě článku 83 obecného nařízení správci, který je zároveň právnickou osobou a podnikem, uložit pouze za taková porušení obecného nařízení, kterých se dopustil úmyslně nebo z nedbalosti.

PŘEHLED POKYNŮ EDPB

Sbor vydává různé typy dokumentů, z nichž pro odbornou i laickou veřejnost nejvýznamnějšími jsou pokyny (guidelines), které mají podporovat porozumění zákonným požadavkům GDPR a napomáhat jeho harmonizovanému uplatňování. V roce 2023 Sbor schválil následující pokyny:

- Pokyny 03/2022 ke klamavým prvkům v uživatelském rozhraní platforem sociálních médií (tzv. temné vzorce): jak je rozpoznat a vyvarovat se jim,

32 Zákon o správních deliktech (Gesetz über Ordnungswidrigkeiten) ze dne 24. května 1968 (BGBl. 1968 I, s. 481), ve znění sdělení ze dne 19. února 1987 (BGBl. 1987 I, s. 602) a zákona ze dne 19. června 2020 (BGBl. 2020 I, s. 1350.

- Pokyny 05/2021 o souhře mezi uplatňováním článku 3 a ustanoveními o mezinárodním předávání údajů podle kapitoly V GDPR,
- Pokyny 07/2022 týkající se vydávání osvědčení jako nástroje pro předávání údajů,
- Pokyny 09/2022 k oznamování porušení zabezpečení osobních údajů podle GDPR,
- Pokyny 01/2022 k právům subjektů údajů – právo přístupu,
- Pokyny 8/2022 pro určení vedoucího dozorového úřadu správce nebo zpracovatele,
- Pokyny 05/2022 k použití technologie rozpoznávání obličejů v oblasti prosazování práva,
- Pokyny 03/2021 k uplatnění článku 65 odst. 1 písm. a GDPR,
- Pokyny 04/2022 k výpočtu správních pokut podle GDPR,
- Doporučení 01/2022 k žádosti o schválení a k prvkům a zásadám, které musí být součástí závazných podnikových pravidel pro správce (čl. 47 GDPR),
- Pokyny 01/2023 k článku 37 trestněprávní směrnice.

Další pokyny jsou upravovány podle připomínek z veřejné konzultace, popřípadě jsou k veřejné konzultaci otevřeny.

Anotace vybraných pokynů

Pokyny 03/2022 ke klamavým temným vzorcům v rozhraních platforem sociálních médií: jak je rozpoznat a vyvarovat se jim

Dokument představuje sadu praktických doporučení poskytovatelům a tvůrcům služeb sociálních médií, jakož i jejich uživatelům, jak posoudit a vyhnout se klamavým temným vzorcům. Míní se jimi způsoby ovlivňování uživatelů, aby učinili nezamýšlené, nedobrovolné a potenciálně škodlivé rozhodnutí. To může být překážkou účinné ochrany osobních údajů a schopnosti činit vědomý výběr a rozhodnutí. Dozorové úřady mohou tedy použití těchto klamavých praktik sankcionovat, pokud vyhodnotí, že porušují zásady obecného nařízení, například zásadu korektního, zákonného a transparentního zpracování podle článku 5 odst. 1 písm. a) GDPR. Problematika v pokynech je pro ilustraci vysvětlena pomocí šedesáti praktických příkladů včetně doporučení dobré praxe.

Pokyny 09/2022 k ohlašování porušení zabezpečení osobních údajů podle GDPR

Jde o aktualizovanou verzi materiálu vydaného pod označením WP250 rev.01 v roce 2017 bývalou Pracovní skupinou WP29. Aktualizace se mimo jiné týká vyjasnění požadavků na ohlašování porušení zabezpečení osobních údajů, ke kterému dojde u správců, kteří nemají provozovnu v EU. Vedle náležitostí řádného ohlašování případů porušení zabezpečení dozorovému úřadu (článek 33 GDPR) je v pokynech pojednána také povinnost oznamování těchto případů subjektu údajů (článek 34 GDPR).

Pokyny 01/2022 k právům subjektů údajů – právo přístupu

Smyslem práva subjektů údajů na přístup je vybavit jednotlivce možností snadným způsobem obdržet dostatečnou a transparentní informaci o zpracování jeho osobních údajů. Uplatnění tohoto práva dává následně možnost využít i práva na výmaz nebo opravu zpracovávaných dat. Dokument se podrobně zabývá způsobem posuzování žádostí o přístup, jeho rozsahem a formou jeho poskytování, jakož i omezeními tohoto práva, která připouští GDPR.

Pokyny 8/2022 pro určení vedoucího dozorového úřadu správce nebo zpracovatele

Tyto pokyny navazují na dokument vydaný Pracovní skupinou WP29 pod kódem WP244 rev.01 v roce 2017. Vychází z praktických potřeb správců, přičemž aktualizace původního materiálu se hlavně týká kapitoly o společných správcích a vymezení pojmu „hlavní provozovna" v tomto kontextu. Příloha pokynů nabízí návod, jak správce může zjistit, zda provádí přeshraniční zpracování osobních údajů a jak postupovat při určování vedoucího dozorového úřadu a také případných dotčených dozorových úřadů.

Pokyny 05/2022 k použití technologie rozpoznávání obličejů v oblasti prosazování práva

Bezpečnostní orgány používají ve stále rozsáhlejším měřítku technologii rozpoznávání obličejů pro identifikaci osob, například za účelem jejich stíhání nebo sledování. Technologie pracuje s biometrickými daty, mnohdy s podporou umělé inteligence, jedná se tedy o zpracování

zvláštních kategorií osobních údajů. Tyto pokyny jsou určeny především zákonodárcům a dále složkám, které technologii rozpoznávání obličejů používají. Nabízí rovněž pomůcku k vyhodnocení citlivosti použití této technologie v daném konkrétním případě. Poskytují i návod uživatelům a provozovatelům těchto systémů.

Pokyny 04/2022 k výpočtu správních pokut podle GDPR

Účelem dokumentu je sjednocení metodiky, kterou úřady používají při výpočtu výše pokut za porušení GDPR. Navržený postup má pět fází, kterými jsou konkrétně:

- identifikace zpracování a posouzení aplikace článku 83 odst. 3 GDPR,
- v závislosti na druhu a závažnosti porušení jakož i dalších okolností stanovení tzv. výchozího bodu pro další kalkulaci,
- vyhodnocení přitěžujících i polehčujících okolností,
- stanovení zákonných maximálních limitů pro daná porušení,
- analýza účinnosti a přiměřenosti pokuty.

Metodika představená v dokumentu bude v případě potřeby předmětem průběžné aktualizace.

ROZHODNUTÍ EDPB

Závazná rozhodnutí podle čl. 65 GDPR

Závazné rozhodnutí EDPB zajišťuje správné a důsledné uplatňování GDPR vnitrostátními úřady pro ochranu údajů. Pokud nemají shodný názor na návrh rozhodnutí vedoucího dozorového úřadu v konkrétní přeshraniční věci, má v takovém případě EDPB pravomoc přijmout závazné rozhodnutí podle článku 65 GDPR. V minulém roce byla přijata závazná rozhodnutí v následujících případech.

Závazné rozhodnutí 01/2023 – Meta Platforms Ireland Limited (Facebook)

Irský dozorový úřad zjistil, že společnost Meta porušila obecné nařízení v důsledku předávání osobních údajů z Evropské unie do Spojených států amerických (v návaznosti na rozsudek Soudního dvora EU sp. zn. C-311/18 ze dne 16. července 2020 – Schrems II). Po projednání návrhu rozhodnutí však nebylo dosaženo dohody ohledně opatření, která mají být přijata proti společnosti Meta. Věc byla proto postoupena EDPB, který vydal závazné rozhodnutí. Vzhledem k systematickému, opakovanému a nepřetržitému předávání údajů do USA, nařídil EDPB irskému dozorovému úřadu uložit správci pokutu a upravit zpracování a předávání osobních údajů.

Společnost Meta tak byla na základě rozhodnutí EDPB ze dne 13. dubna 2023 pokutována částkou 1,2 miliardy eur za předávání osobních údajů prostřednictvím služby Facebook. Tato rekordní pokuta byla uložena za předávání dat do USA na základě standardních smluvních doložek (SCC) od 16. července 2020. Správci bylo také nařízeno uvést své přenosy dat do souladu s obecným nařízením. Společnost Meta podala dne 13. června 2023 žalobu k Tribunálu Soudního dvora Evropské unie pod spisovou značkou T-325/23 na zrušení závazného rozhodnutí EDPB č. 1/2023.

Závazné rozhodnutí 02/2023 – TikTok Technology Limited

EDPB přijal dne 3. srpna 2023 závazné rozhodnutí, které se týkalo návrhu rozhodnutí irského dozorového úřadu ohledně společnosti TikTok.

Ten předložil návrh rozhodnutí po provedení šetření z vlastního podnětu (ex officio). Šetření se zaměřilo na zpracování osobních údajů registrovaných uživatelů TikToku ve věku 13 až 17 let a také na některé problémy týkající se zpracování osobních údajů dětí mladších 13 let – jednalo se zejména o tzv. nekalé praktiky (dark patterns) a ověřování věku.

Některé dozorové úřady však vznesly proti tomuto návrhu rozhodnutí námitky, a protože nebylo dosaženo shody, bylo EDPB předloženo, aby spor vyřešil. Námitky se týkaly například otázek, zda byla porušena záměrná a standardní ochrana osobních údajů v souvislosti s ověřováním věku a zda byla porušena zásada korektnosti v souvislosti s některými praktikami designu.

Irský dozorový úřad dne 15. září 2023 přijal konečné rozhodnutí, kterým byla společnosti TikTok uložena správní pokuta. Za porušení byla uložena správní pokuta 345 milionů eur a současně byla společnosti TikTok uložena povinnost uvést své zpracování do souladu s obecným nařízením do 3 měsíců. Společnost TikTok podala dne 10. října 2023 žalobu k Tribunálu Soudního dvora Evropské unie pod spisovou značkou T-1030/23 na zrušení závazného rozhodnutí EDPB č. 2/2023 2023 na základě rozhodnutí EDPB irský dozorový úřad pokutoval 390 miliony eur.

Na EDPB se tak v souladu s procedurou čl. 66 odst. 2 GDPR obrátil norský dozorový úřad, který mohl zpracování údajů norských občanů za účelem profilování zastavit pouze dočasně. EDPB byl požádán o rozšíření zákazu profilování uživatelů společností Meta i na všechny ostatní uživatele v Evropském hospodářském prostoru (EHP).

EDPB žádosti vyhověl a 27. října 2023 přijal naléhavé závazné rozhodnutí podle článku 66 GDPR, kterým uložil irskému dozorovému úřadu přijmout konečná opatření týkající se společnosti Meta na základě čl. 58 odst. 2 písm. f) GDPR. Tato opatření zahrnují zákaz zpracování osobních údajů pro účely behaviorální reklamy na právním základě smlouvy a oprávněného zájmu v celém EHP do dvou týdnů. Irský dozorový úřad informoval společnost Meta o rozhodnutí EDPB 31. října 2023 a pokračuje ve vnitrostátním řízení.

Naléhavé závazné rozhodnutí podle čl. 66 GDPR

Článek 66 GDPR umožňuje dozorovému úřadu přijímat ve výjimečných případech dočasná opatření, která mají právní účinky na jeho vlastním území po dobu nejvýše tří měsíců, pokud se domnívá, že je naléhavě nutné jednat. EDPB pak může vydat naléhavé stanovisko nebo případně naléhavé závazné rozhodnutí, aby bylo zajištěno jednotné uplatňování obecného nařízení.

Naléhavé závazné rozhodnutí 01/2023 – Meta Platforms Ireland Limited

Již v prosinci 2022 objasnila závazná rozhodnutí EDPB podle čl. 65, že smlouva není vhodným právním základem pro zpracování osobních údajů, které společnost Meta provádí pro účely behaviorální reklamy (podrobněji analyzováno ve výroční zprávě Úřadu za rok 2022). Od té doby však správce neprokázal splnění pokynů uložených na konci roku 2022, i když jej v lednu

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

Předávání do USA

Nejdůležitější událostí roku 2023 v oblasti předávání osobních údajů do třetích zemí bylo nepochybně přijetí Prováděcího rozhodnutí Komise ze dne 10. července 2023 podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů poskytované Rámcem ochrany soukromí mezi EU a USA.

Rámec ochrany soukromí (Data Privacy Framework) podobně jako jeho předchůdci (Safe Harbor, Privacy Shield) představuje samocertifikační systém spravovaný americkým Ministerstvem obchodu (Department of Commerce) a dozorovaný americkou Federální obchodní komisí (Federal Trade Commission) a Ministerstvem dopravy (Department of Transport). Americké soukromé společnosti, které se jako dovozci osobních údajů z Evropské unie, resp. Evropského hospodářského prostoru, přihlásí do programu Rámce ochrany soukromí, se zavazují dodržovat zásady programu, které jsou přílohou výše uvedeného rozhodnutí Komise.

Komise došla k závěru, že účast dovozce osobních údajů v programu Rámce ochrany soukromí zajišťuje odpovídající úroveň ochrany osobních údajů podle čl. 45 GDPR. Předání osobních údajů do Spojených států amerických společnostem, které jsou zapsány v programu Rámce ochrany soukromí, je tedy možné realizovat za stejných podmínek jako jakékoliv jiné předání osobních údajů v rámci Evropské unie, resp. Evropského hospodářského prostoru.

Předávání osobních údajů společnostem, které nejsou zapsány v programu Rámce ochrany soukromí, bude nadále možné s využitím některého z nástrojů čl. 46 GDPR (typicky standardní smluvní doložky nebo závazná podniková pravidla). Vývozci osobních údajů budou nadále povinni provést vyhodnocení, zda daný nástroj skutečně poskytuje vhodné záruky pro předané údaje (Transfer Impact Assessment), nejlépe podle Doporučení Sboru 1/2020 k opatřením doplňujícím stávající nástroje předávání osobních údajů pro zajištění EU úrovně ochrany osobních údajů. V rámci tohoto vyhodnocení se však nyní mohou opřít o posouzení právního rámce ochrany osobních údajů ve Spojených státech, které Komise provedla v recitálu daného rozhodnutí.

V provedeném posouzení došla Komise i v palčivé otázce přístupu státních orgánů k osobním údajům k obecně platnému závěru, že právní rámec Spojených států amerických po přijetí prezidentského dekretu EO 14086 z října 2022 umožňuje orgánům veřejné moci přístup k předaným osobním údajům v rozsahu, který nejde nad rámec toho, co je nezbytné a přiměřené v demokratické společnosti.

Komisi se podařilo vypořádat mnohé kritické připomínky, které vůči návrhu rozhodnutí vznesl kromě Evropského parlamentu také EDPB ve Stanovisku 5/2023 k návrhu prováděcího rozhodnutí Evropské komise o odpovídající ochraně osobních údajů poskytované Rámcem ochrany soukromí mezi EU a USA. Přesto se zdá, že pochybnosti zůstávají, a to jak v otázce proporcionality přístupu státních orgánů USA k předaným údajům, tak ve věci nezávislosti soudního přezkumu případných stížností subjektů údajů v této věci. Nasvědčují tomu veřejná vyjádření Maxe Schremse a jeho sdružení None Of Your Business (NOYB), že se opět chystají rozhodnutí Komise napadnout u Soudního dvora EU, stejně jako skutečnost, že poslanec francouzského parlamentu Philippe Latombe podal k Tribunálu EU žádost o zrušení rozhodnutí Komise.

Souběh účasti v programu Rámce ochrany soukromí a standardních smluvních doložek

V situaci, kdy není vyloučeno, že rozhodnutí Komise o odpovídající ochraně poskytované Rámcem ochrany soukromí bude zpochybněno, nepřekvapuje, že mnozí dovozci údajů ze Spojených států amerických, a mezi nimi i velcí poskytovatelé IT služeb typu Google či Microsoft, se na jedné straně okamžitě certifikovali pro účast v programu Rámce ochrany soukromí, ale na druhé straně zároveň nadále ve své smluvní dokumentaci ošetřují předání osobních údajů z Evropské unie standardními smluvními doložkami a vypracovávají Transfer Impact Assessment podle návodu daného Doporuče-

ním EDPB 1/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU.

Odborná veřejnost se opakovaně na Úřad obracela s otázkou, zda je takový souběh použití různých nástrojů předávání možný. Úřad v této věci zastává názor, že nikdo nemůže bránit přijetí většího množství záruk ochrany osobních údajů, než zákon vyžaduje, takže nic nebrání těmto společnostem jako dovozcům údajů, aby předání osobních údajů ošetřily zároveň jak svou certifikací v programu Rámce ochrany soukromí, tak navíc i některým z nástrojů podle čl. 46 obecného nařízení, např. smlouvou s vývozci údajů, jejíž součástí jsou standardní smluvní doložky podle prováděcího rozhodnutí Komise ze dne 15. června 2021 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení (EU) 2016/679.

Pokyny 5/2021 a přenos údajů mezi provozovnami podle čl. 3 odst. 1 obecného nařízení

V roce 2023 EDPB vydal definitivní znění Pokynů 5/2021 ke vzájemné souhře mezi čl. 3 a ustanoveními o předávání osobních údajů kapitoly V obecného nařízení. Pro účel těchto pokynů EDPB potvrdil v úvodním § 9 tři kumulativní kritéria, která musejí být splněna, aby bylo možné operaci zpracování považovat za předání podle kapitoly V obecného nařízení. Podle těchto tří kritérií se pokyny zabývají, stručně vyjádřeno, těmi operacemi zpracování, které spočívají v přenosu nebo zpřístupnění údajů ze strany a) správce nebo zpracovatele b) podléhajícího obecnému nařízení podle čl. 3 tohoto nařízení c) jinému správci nebo zpracovateli ve třetí zemi nebo mezinárodní organizaci.

Je zřejmé, že pod tuto definici se vejde naprostá většina scénářů předávání osobních údajů, a to včetně předání osobních údajů správcům nebo zpracovatelům ve třetích zemích, kteří podléhají GDPR podle čl. 3 odst. 2, i předání ze strany takových správců nebo zpracovatelů dalším dovozcům.

Avšak opatrná formulace § 9 pokynů dává najevo, že tato tři kritéria nepodávají vyčerpávající definici předávání osobních údajů. Stranou uvedené definice totiž zůstávají přenosy údajů mezi provozovnami podle čl. 3 odst. 1 obecného nařízení. Problému těchto přenosů mezi provozovnami jednoho správce nebo jednoho zpracovatele se Pokyny záměrně nevěnovaly, a to nejen z toho důvodu, že nebyla nalezena shoda, zda jde, či nejde o předání podle kapitoly V. (ačkoliv většina delegací uznávala, že by tyto přenosy logicky měly být předáním podle kapitoly V.), ale především z důvodu obtížně řešitelných problémů, které uplatnění kapitoly V. na přenosy mezi provozovnami podle čl. 3 odst. 1 přináší.

Prvním problémem je faktická neexistence nástrojů podle čl. 46 GDPR, kterými by předání mezi provozovnami jedné entity, jediného správce nebo jediného zpracovatele, bylo možné ošetřit, a to zvláště v případech, kdy jsou takovými provozovnami odštěpné závody bez právní subjektivity.

Druhým problémem je neexistence kritérií pro rozhodnutí, zda se určitá entita, typicky opět odštěpný závod bez právní subjektivity, nachází vůči své „mateřské“ společnosti v pozici provozovny podle čl. 3 odst. 1 GDPR, v pozici samostatného správce nebo samostatného zpracovatele. Všechny tyto tři scénáře jsou možné, ale všechny tři přinášejí obtížně řešitelné právní problémy, které však nejsou nové, protože se s nimi každý dozorový úřad potýkal více či méně úspěšně i v dobách Směrnice 95/46/ES.

Výklad problematiky přenosů mezi provozovnami podle čl. 3 odst. 1 GDPR tak zůstává desideratem do budoucna.

Odpovědnost správce za předání údajů zpracovatelem dílčím zpracovatelům

V souvislosti s aplikací rozhodnutí Komise o odpovídající ochraně poskytované EU-US Rámcem ochrany soukromí je často vznášena ze strany veřejného i soukromého sektoru otázka, zda v situaci, kdy správci z EU předávají údaje do třetí země na základě rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů zpracovatelům majícím dílčí zpracovatele v jiných třetích zemích s nedostatečnou úrovní ochrany osobních údajů, jsou tito správci z EU odpovědní za posouzení rizik souvisejících s dalším předáváním těmto dílčím zpracovatelům.

Tato otázka byla diskutována podskupinou Sboru pro předávání (International Transfers Subgroup). Východiskem bylo konstatování, vtělené i do textu § 19 Pokynů 5/2021 ke vzájemné souhře mezi čl. 3 a ustanoveními o předávání osobních údajů kapitoly V obecného nařízení, že správce nepochybně zůstává vůči subjektům údajů zodpovědný za zpracování jejich údajů i poté, kdy údaje předá zpracovateli a ten dílčím zpracovatelům, a to bez ohledu na to, zda jsou údaje přenášeny jen v rámci EU nebo zda dochází k předání osobních údajů do třetí země, resp. bez ohledu na to, zda zpracovatel a dílčí zpracovatelé podléhají GDPR či nikoliv.

Proto i v konkrétním případě, kdy údaje předává zpracovatel sídlící ve třetí zemi disponující rozhodnutím Komise o odpovídající úrovni ochrany osobních údajů (takže jím realizované další předání osobních údajů – onward transfer – proběhne se zárukami, která Komise svým rozhodnutím deklarovala za „v zásadě rovnocenné"), je původní správce odpovědný za dále předané údaje. Z toho vyplývá, že přinejmenším teoreticky by správce měl ověřit, že zpracovatel skutečně předává osobní údaje dílčím zpracovatelům se „v zásadě rovnocennými" zárukami, jak je tomu zavázán, ať už právním řádem třetí země, nebo účastí v programu Rámec ochrany soukromí – jinými slovy že zpracovatel plní své závazky.

Analogicky i v případech, kdy je vývozcem údajů obecnému nařízení podléhající zpracovatel, který provádí Transfer Impact Assessment, by měl správce přinejmenším teoreticky ověřit, zda tento Transfer Impact Assessment je proveden správně a odpovídá skutečnosti.

Závazná podniková pravidla a certifikace a kodexy jako nástroj předávání

V roce 2023 EDPB vydal definitivní znění Doporučení 1/2022 k žádosti o schválení a k prvkům a zásadám, které musejí být součástí závazných podnikových pravidel pro správce (čl. 47 obecného nařízení), které nahradilo dosud užívané dokumenty WP264 a WP256. Podskupina Sboru pro předávání (International Transfers Subgroup) zahájila práci na formulování analogického doporučení ve vztahu k BCR pro zpracovatele, které nahradí dosud platný formulář žádosti o schválení BCR pro zpracovatele (WP265) a dokument shrnující prvky a zásady, které musejí být součástí BCR pro zpracovatele (WP257).

Vedle již dříve schválených Pokynů 4/2021 týkajících se kodexů chování jakožto nástrojů pro předávání údajů EDPB v roce 2023 vydal po vypořádání veřejné konzultace rovněž definitivní znění Pokynů 7/2022 týkající se vydávání osvědčení jako nástroje pro předávání údajů verze 2.0 po veřejné konzultaci, čímž byly vytvořeny základní předpoklady pro možnost podávat Sboru návrhy kodexů jako nástrojů předávání podle čl. 40 odst. 3 a čl. 46 odst. 2 písm. e) obecného nařízení i certifikačních kritérií pro certifikace jako nástroje předávání podle čl. 42 odst. 2 a čl. 46 odst. 2 písm. f) obecného nařízení.

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 požadavky na akreditaci subjektů pro vydávání osvědčení, nelze požadavky na akreditaci vyhlásit ve formě vyhlášky, jak předpokládá zákon č. 110/2019 Sb.

Co se týče situace v EU, EDPB dosud vydal stanoviska ke třem národním certifikačním kritériím, a to:

- stanovisko 1/2022 k lucemburským obecným národním certifikačním kritériím CARPA, kde je vlastníkem certifikačního schématu přímo lucemburský dozorový úřad,
- stanovisko 25/2022 k německým národním certifikačním kritériím European Privacy Seal (EuroPrise) certifikace zpracovatelů, kde je vlastníkem certifikačního schématu společnost EuroPriSe Cert GmbH,
- stanovisko 15/2023 k nizozemským obecným národním certifikačním kritériím Brand Com-

pliance certification standard, kde je vlastníkem certifikačního schématu společnost Brand Compliance B.V.

Kromě toho Sbor schválil jako evropskou pečeť ochrany osobních údajů podle čl. 42 odst. 5 obecného nařízení obecná certifikační kritéria Europrivacy, která jsou platná v celé Evropské unii a kde je vlastníkem schématu European Center for Certification and Privacy.

Kodexy chování

Požadavky na akreditaci subjektů pro monitorování kodexů chování Úřad zveřejňuje obdobně jako v případě Požadavků na akreditaci subjektů pro vydávání osvědčení. Je tedy nutné řešit obdobný problém neslučitelnosti jako v případě Požadavků na akreditaci subjektů pro vydávání osvědčení (viz výše). V roce 2023 Úřad neschválil žádný kodex chování. Schválení jakéhokoliv kodexu není možné vzhledem k neexistenci zveřejněných požadavků pro akreditaci subjektů pro monitorování kodexů chování (není možno ustanovit monitorující subjekty a bez toho není možné kodex schválit).

Co se týče nadnárodních kodexů chování, Sbor dosud vydal stanoviska ke dvěma nadnárodním kodexům chování: stanovisko 16/2021 ke kodexu chování poskytovatelů cloudových služeb vlastníka Scope Europe a stanovisko 17/2021 ke cloudovému kodexu chování vlastníka Cloud Infrastructure Service Providers (CISPE). ●

Nevyžádaná obchodní sdělení

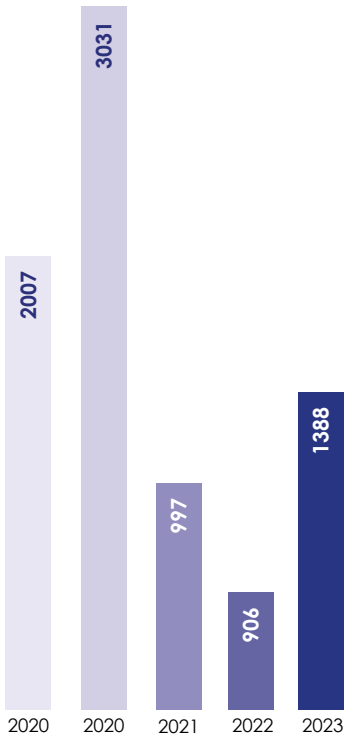
STÍŽNOSTI

Úřad za rok 2023 evidoval celkem 1388 stížností. Oproti předchozím dvěma letům se tedy jedná o více jak čtvrtinový nárůst.

Jedním z důvodů zvýšení počtu stížností by mohla být skutečnost, že firmy ve větší míře využívají internetové portály např. www.firmy.cz, www.zivefirmy.cz k vyhledávání elektronických kontaktů pro zasílání obchodních sdělení. Úřad považuje za důležité upozornit, že takto získané údaje (e-mailové adresy, telefonní čísla) nezakládají právní titul pro rozesílku obchodních sdělení podle zákona o některých službách informační společnosti. Nelze využít ani právního titulu oprávněného zájmu, jelikož tento se vztahuje pouze na elektronické kontakty získané v souvislosti se zákaznickým vztahem a mohou být použity pouze k nabídce vlastních výrobků či služeb, a ani právního titulu souhlasu, neboť nelze udělit souhlas neurčitému okruhu šiřitelů a k neurčitým nabídkám. Pokud tedy bude šiřitel obchodních sdělení zasílat obchodní sdělení na takto získané údaje, bude tak činit v rozporu se zákonem o některých službách informační společnosti.

Dále Úřad obdržel velké množství stížností (v řádu stovek) ve vztahu ke způsobu komunikace, kdy je adresátům doručena na jejich e-mailové adresy zálohová faktura na služby týkající se reklamy, marketingu a internetových prezentací, které si však příjemce nikdy neobjednal. Tato sdělení vzbuzují dojem, že se jedná o skutečně objednané služby a výzvu k zaplacení faktury za provedenou práci. Takto zasílané e-mailové zprávy jsou svým charakterem obchodním sdělením a proti rozesílacím společnostem Úřad vede příslušná kontrolní řízení.

PODANÉ STÍŽNOSTI ZA JEDNOTLIVÉ ROKY



DOZOROVÁ ČINNOST

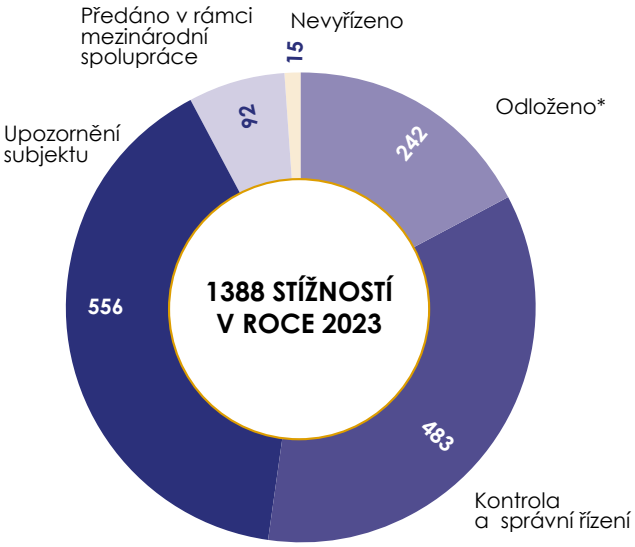
Vzhledem k tomu, že Úřad zaznamenal v minulých letech zvýšený počet stížností na zasílání obchodních sdělení pomocí SMS zpráv, zejména pokud jde o nedodržování náležitostí takových zpráv, ale i dotazy na správnost jejich zasílání z řad veřejnosti, provedl v roce 2023 na základě plánu kontrol, kontrolu dvou vytipovaných

společností. Provedenými kontrolami neshledal Úřad pochybení, pokud jde o právní titul k rozesílkám, neboť tyto společnosti zasílaly svá obchodní sdělení na telefonní čísla uživatelů, kteří buď v minulosti udělili těmto společnostem souhlas nebo se jednalo o jejich zákazníky. Nicméně bylo konstatováno, a to v obou případech, systémové porušení, pokud jde o další podmínky pro šíření obchodních sdělení. Obchodní sdělení nebyla jasně a zřetelně označena, tak aby je adresát mohl odlišit od jiných jemu zasílaných sdělení. Dále společnosti neuváděly v zasílaných sděleních totožnost odesílatele, v jehož prospěch je sdělení zasláno. Zejména pak nebyla dodržena ani podmínka, aby sdělení obsahovalo informaci o tom, jak má příjemce postupovat, pokud si nepřeje další zasílání obchodních sdělení. Obě společnosti již v průběhu prováděných kontrol tyto nedostatky napravily a deklarovaly, že budou při zasílání obchodních sdělení prostřednictvím SMS zpráv postupovat v souladu se zákonem o některých službách informační společnosti. Úřad však v této souvislosti bude s kontrolami dalších společností, u nichž zjistí možné pochybení při šíření obchodních sdělení SMS zprávami, pokračovat i v roce 2024.

Úřad se dále v rámci své dozorové činnosti věnoval i kontrolám na základě podaných stížností, přičemž lze zdůraznit i výše uvedená kontrolní řízení proti společnostem rozesílajícím zálohové faktury, kdy ve vztahu k jedné ze společností bylo podáno více než 200 stížností.

V roce 2023 vedl Úřad celkem 20 kontrolních řízení. Správních řízení pak provedl Úřad 29, celková výše pravomocně uložených sankcí činila 8 623 000 Kč. Správní řízení se, jako v roce 2022, často týkala i opakovaných porušení při zasílání obchodních sdělení, čemuž následně odpovídala i výše uložené sankce. Ve dvou případech byla uložena i pořádková pokuta za nesoučinnost, a to v celkové výši uložené sankce za tyto případy ve výši 75 000 Kč. V případě méně závažných pochybení, kdy je například doručena pouze jedna či dvě stížnosti proti rozesílajícímu subjektu a tento nebyl ještě upozorňován nebo s ním nebylo vedeno řízení, jsou takovým subjektům zasílány upozorňující dopisy, které vždy obsahují i poučení o tom, jak lze zasílat obchodní sdělení elektronickými prostředky v souladu se zákonem o některých službách informační společnosti. Tímto způsobem Úřad upozornil celkem 359 subjektů. Dále Úřad předal v rámci mezinárodní spolupráce podle nařízení EU o ochraně spotřebitelů k provedení donucujících opatření či poskytnutí informací celkem 92 stížností. Nejvíce stížností bylo předáno na Slovensko, dále pak též do Polska, Maďarska, Německa, Francie a na Maltu. Naopak ze zahraničí neobdržel Úřad k provedení příslušných opatření vůči českému podnikatelskému subjektu žádnou stížnost.

JEDNOTLIVÉ ZPŮSOBY VYŘÍZENÍ PŘIJATÝCH STÍŽNOSTÍ



*Důvod odložení:
– Nejedná se o obchodní sdělení
– Nebyl dohledán odpovědný subjekt
– Odpovědný subjekt se nachází mimo EU

Nejvýše udělená pokuta

Úřad v roce 2023 uložil za zasílání obchodních sdělení ve prospěch třetích stran pokutu ve výši 7 700 000 Kč. Společnost zajišťující přepravu šířila od roku 2015 na e-mailové adresy svých zákazníků obchodní sdělení ve prospěch třetích stran, a to aniž by disponovala předchozím souhlasem adresátů.

Zákazníci této přepravní společnosti byli oslovováni prostřednictvím e-mailových zpráv, kdy obchodní sdělení třetích stran bylo uvedeno v potvrzení o provedeném nákupu a zakoupené jízdence. Adresáti tak neměli žádnou možnost tato obchodní sdělení jakýmkoli způsobem odmítnout. Nebyly dodrženy ani další zákonné požadavky, jako je zřetelné a jasné označení takové zprávy či uvedení jednoznačné identifikace subjektu, v jehož prospěch jsou daná obchodní sdělení šířena.

Vzhledem ke skutečnosti, že společnost propagovala v podobě nabídek různých slev a voucherů třetí strany, bylo třeba, aby pro takové šíření obchodních sdělení disponovala předchozím souhlasem adresátů. Bez předchozího souhlasu totiž lze šířit obchodní sdělení pouze na elektronické kontakty získané již dříve v souvislosti s prodejem výrobku či služby, ovšem pouze pro účely nabídky vlastních obdobných výrobků či služeb, nikoli tedy nabídek třetích stran.

Uložená pokuta je dosud nejvyšší pravomocně uloženou pokutou Úřadu v oblasti obchodních sdělení. Její výše odráží zejména rozsah takto oslovených adresátů, kterých bylo přes 40 milionů, a dobu, po kterou byla daná obchodní sdělení zasílána. Úřad tak vyslal jednoznačný signál, že tuto praxi, tedy využívání kontaktních údajů svých zákazníků k zasílání obchodních sdělení třetích stran bez jejich souhlasu, nebude tolerovat.

JUDIKATURA

V roce 2023 byla rozsudkem Nejvyšší správního soudu (6 As 18/2002-43) potvrzena dlouhotrvající praxe Úřadu v oblasti šíření obchodních sdělení, který ve svých rozhodnutích opakovaně zdůrazňoval, že odpovědnost za šíření obchodních sdělení nese kromě samotného rozesílatele i ten, kdo takovou rozesílku ve svůj prospěch inicioval, například objednáním služby, udělením příkazu či jiného pokynu, nebo i využitím affiliate partnerů či nástrojů lead marketingu apod.

Jak soud poznamenal, odpovědnost je v tomto případě objektivní a podnikatelský subjekt, v jehož prospěch je obchodní sdělení šířeno, tak odpovídá i za případný exces rozesílatelů. Je-li tedy na základě zjištěného skutkového stavu zřejmé, že učiněné přestupkové jednání je přičitatelné právnické osobě, není nezbytné, aby bylo najisto postaveno, která fyzická osoba se jednání dopustila.

LEGISLATIVA

Úřad se účastnil přípravy reformy digitálního prostředí zpracované Ministerstvem průmyslu a obchodu v návrhu zákona o digitální ekonomice. O této problematice je blíže pojednáno v části Národní legislativa.

Z pohledu šíření obchodních sdělení je však podstatné uvést, že tento nový právní předpis (zákon o digitální ekonomice) kromě implementace Aktu o digitálních službách (DSA) a částečně Aktu o správě dat (DGA), reviduje také současný zákon o některých službách informační společnosti, kdy z velké části přejímá implementaci sekundárních předpisů, zejména směrnici o soukromí a elektronických komunikacích (ePD), která je právě implementována v zákoně o některých službách informační společnosti.

Podmínky pro šíření obchodních sdělení elektronickými prostředky tak, jak jsou nyní upraveny v zákoně o některých službách informační společnosti, budou tedy nově revidovány a přizpůsobeny dosavadní praxi a vývoji právního řádu, zejména pak vstupu obecného nařízení v použitelnost. Dále je snahou Úřadu zavést i v oblasti šíření obchodních sdělení, institut nápravných opatření. V současnosti je možné za šíření nevyžádaných obchodních sdělení uložit pouze sankci. Smyslem správního řízení o protiprávním šíření obchodních sdělení však není jen trestat, ale taktéž napravit protiprávní stav. Zavedení tohoto institutu i pro oblast šíření obchodních sdělení by tak bylo velice vhodné a do budoucna prospěšné nejen pro samotné šiřitele obchodních sdělení, kterým by byly stanoveny jednoznačné povinnosti při zjednání nápravy, ale ve svém důsledku i pro jejich adresáty. ●

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.
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 2. ledna 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.

Ke dni 1. září 2022 a poté ke dni 1. ledna 2023 nabyly účinnosti dvě podstatné části novely zákona o svobodném přístupu k informacím provedené zákonem č. 241/2022 Sb. Tato novela rozšířila okruh povinných subjektů o nový typ, kterým je veřejný podnik. Definice veřejného podniku pro účely zákona o svobodném přístupu k informacím je obsažena v jeho § 2a. V důsledku této

změny se Úřad stal nadřízeným orgánem další poměrně velké skupiny povinných subjektů. Zmíněná novela dále omezila informační povinnost profesních samosprávných komor, a to pouze na informace vztahující se k výkonu veřejné správy, který byl těmto komorám svěřen zákonem. V procesní rovině byl v § 16 odst. 4 zákona o svobodném přístupu k informacím nově upraven tzv. „odvolací dialog" přenášející na odvolací orgán část povinností dosud příslušejících dotázanému povinnému subjektu. Smyslem této změny je nicméně především snadnější řešení formálních nedostatků, které nejsou samy o sobě předmětem sporu.

OBECNĚ K ROZHODOVÁNÍ ÚŘADU V OBLASTI SVOBODNÉHO PŘÍSTUPU K INFORMACÍM

Specifickým jevem, který přetrvával i v roce 2023, 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 subjekty a tato rozhodnutí je nucen 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 Úřad i v roce 2023 setkával 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, doručenky 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).

Na činnost Úřadu má vliv také skutečnost, že povinné subjekty, které jsou veřejnoprávními korporacemi nebo osobami soukromého práva, vystupují při vyřizování žádostí o informace ve dvojí roli – jednak jako správní orgány, jednak jako osoby nadané veřejnými subjektivními právy a povinnostmi poskytovat informace jen v mezích zákona o svobodném přístupu k informacím. Takové subjekty totiž reálně rozhodují o svých subjektivních právech, a proto mohou proti rozhodnutí Úřadu, kterým bylo rozhodnuto o odvolání proti rozhodnutí takového povinného subjektu, brojit žalobou dle § 65 odst. 1 soudního řádu správního. To s sebou přirozeně nese zvýšené nároky spojené se zastupováním Úřadu v soudních řízeních.

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

POZNATKY Z ROZHODOVACÍ PRAXE ÚŘADU A Z JUDIKATURY

Pro určení, zda je subjekt veřejnou institucí, postačuje převaha znaků

Městský soud v Praze se opakovaně zabýval otázkou, zda je dceřiná společnost akciové společnosti České dráhy veřejnou institucí (a tedy i povinným subjektem) ve smyslu § 2 odst. 1 zákona č. 106/1999 Sb. Jelikož je veřejná instituce neurčitým právním pojmem, je třeba při posuzování charakteru konkrétního subjektu vycházet z kritérií vymezených v nálezech Ústavního soudu ve věci Letiště Praha a ve věci ČEZ. Pro určení, zda je obchodní společnost veřejnou institucí, přitom vedle skutečnosti, že její akcie či podíly vlastní ze 100 % stát či územní samosprávný celek, postačuje převaha znaků vymezených v nálezu Ústavního soudu ve věci Letiště Praha. Městský soud v Praze vycházel z faktu, že akciová společnost České dráhy je veřejnou institucí,

přičemž jejím jediným akcionářem je Česká republika. Proto i její dceřiná společnost je zprostředkovaně ze 100 % vlastněna státem. Ačkoliv je tato dceřiná společnost soukromoprávním subjektem, zastává současně též společensky významnou veřejnou úlohu, která ve spojení s naplněním ostatních kritérií svědčí o tom, že je veřejnou institucí. Úřad tedy tuto otázku v předchozím správním řízení posoudil správně.

Městská obchodní společnost hospodaří s veřejnými prostředky

Krajský soud v Praze se ztotožnil se závěry Úřadu, podle nichž je obchodní společnost, jejímž stoprocentním vlastníkem je veřejnoprávní korporace (město), veřejnou institucí ve smyslu § 2 odst. 1 zákona o svobodném přístupu k informacím. Prostředky, s nimiž taková obchodní společnost hospodaří, sice formálně nejsou součástí veřejných rozpočtů, ale ve skutečnosti z nich pocházejí. Obchodní společnost, jejímž jediným vlastníkem je město, tak je příjemkyní veřejných prostředků. Skutečnost, že město pro výkon některých činností samosprávy zřídilo městskou společnost, neznamená, že se tím vymanilo z veřejné kontroly nad touto částí svého hospodaření.

Veřejná diskuse o výši odměny jednatele městské společnosti pak je ve veřejném zájmu, neboť jednak hospodaří s veřejnými prostředky, jednak jeho postavení je obdobné postavení radního města. Zveřejnění informace o odměně jednatele tak nelze považovat za nepřiměřený zásah do jeho soukromí.

Rozsah informační povinnosti veřejného podniku

Po nabytí účinnosti novely zákona o svobodném přístupu k informacím rozšiřující okruh povinných subjektů se Úřad v rámci své rozhodovací činnosti zabýval též otázkou, zda má veřejný podnik ve srovnání s veřejnou institucí omezenou informační povinnost či nikoliv. Dle Úřadu sice bylo záměrem evropské směrnice o otevřených datech a opakovaném použití informací veřejného sektoru z roku 2019 podrobit veřejné podniky informační povinnosti pouze v rozsahu nezbytném k zajištění veřejné kontroly vztahující se k činnostem, pro které jsou takové subjekty za veřejné podniky považovány, tj. ve vztahu k tzv. relevantní činnosti. Avšak úprava obsažená v zákoně o svobodném přístupu k informacím tento minimální standard informační povinnosti veřejného podniku dále doplnila, z čehož vyplývá, že veřejný podnik má stejný rozsah informační povinnosti jako veřejná instituce, která je obchodní společností nebo národním podnikem.

Poskytování informací v oblasti hospodářské soutěže a vymezení pojmu běžný obchodní styk

Úřad byl v rámci své rozhodovací činnosti rovněž opakovaně konfrontován s otázkou, jak pro účely zákona o svobodném přístupu k informacím vykládat výluku z práva na informace vymezenou v § 2b tohoto zákona. Smyslem § 2b odst. 1 zákona o svobodném přístupu k informacím je vyloučit z informační povinnosti takové informace, které se nedotýkají služeb obecného zájmu vymezených v § 2a odst. 1 písm. a) téhož zákona a které současně vypovídají o činnostech přímo vystavených hospodářské soutěži.

Naopak na informace týkající se poskytování služeb obecného zájmu (bez ohledu na to, zda se vztahují či nikoliv k činnostem přímo vystaveným hospodářské soutěži, respektive běžnému obchodnímu styku) a na informace, které se nevztahují k činnostem přímo vystaveným hospodářské soutěži, respektive běžnému obchodnímu styku, není možné aplikovat výluku z práva na informace vymezenou v § 2b odst. 1 zákona o svobodném přístupu k informacím.

Jelikož pojem „běžný obchodní styk“ užitý v § 2b odst. 1 písm. a) zákona o svobodném přístupu k informacím není v žádném právním předpise jednoznačně definovaný, je třeba jej vykládat tak, aby množina činností, které charakter běžného obchodního styku nemají, nezůstala vyprázdněná, neboť v takovém případě by vymezení podmínek ve zmíněném ustanovení postrádalo jakýkoliv smysl. Obchodní styk je tedy třeba chápat jako činnost spočívající ve výměně zboží či služeb za peníze či za jiné zboží či služby, který se děje mezi různými stranami, což z ní činí hospodářský, respektive ob-

chodní vztah. Obchodní styk tedy nelze naplnit tím, že jej povinný subjekt realizuje sám vůči sobě, neboť v takovém případě by absentoval znak transakce. Běžný obchodní styk pak značí činnost pro povinný subjekt obvyklou, standardní a nijak nevybočující.

Pokračující stírání rozdílů mezi tzv. fakultativními a obligatorními důvody pro neposkytnutí informace

Ústavní soud ve svém nálezu ze dne 17. 1. 2023, sp. zn. Pl. ÚS 25/21, dospěl k závěru, podle něhož kterýkoliv zákonný důvod pro neposkytnutí informace musí být při své aplikaci testován, zda skutečně v konkrétní věci chrání jiné základní právo nebo veřejný statek. V předmětné věci Ústavní soud podrobil přezkumu ustanovení § 73 odst. 7 zákona č. 372/2011 Sb., o zdravotních službách, podle kterého Ústav zdravotnických informací a statistiky poskytne na základě žádosti podle zákona o svobodném přístupu k informacím, pokud se jedná o údaje v Národním zdravotnickém informačním systému, pouze informace o struktuře dat. Doslovné znění tohoto ustanovení není dle Ústavního soudu ústavně souladné, neboť v rozhodném rozsahu nesplňuje kritérium nezbytnosti pro omezení základního práva. Současně však nebylo třeba napadené ustanovení rušit, neboť jej lze interpretovat i tak, že v rozhodném rozsahu informace poskytovat lze, a to na základě poměřování práv. Podle Ústavního soudu je povinnou součástí algoritmu rozhodování o žádosti úvaha, zda existuje důvod informace neposkytnout. K tomu je nutné položit si zásadní otázku, jaká ústavní hodnota, jaké základní právo či veřejný zájem by mohly být poskytnutím požadovaných informací dotčeny, či které z nich mají být konkrétním ustanovením vlastně ochráněny.

Při poskytování informací je třeba důsledně rozlišovat mezi anonymizací a pseudonymizací osobních údajů

Městský soud v Praze se v rámci přezkumu správního rozhodnutí Úřadu vydaného v odvolacím řízení zabýval otázkou, jaké údaje lze považovat za anonymizované a jaké pouze za pseudonymizované. Vycházel z premisy, že osobními údaji jsou jakékoliv informace, které se týkají identifikované nebo identifikovatelné žijící osoby. Údaje se přitom pokládají za skutečně anonymizované tehdy, je-li jejich anonymizace nezvratná a dotčenou osobu již nelze žádným způsobem identifikovat. Oproti tomu pseudonymizované údaje jsou osobní údaje, které sice byly zpracovány takovým způsobem, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně, avšak takové zpracování není nezvratné.

Zákon o svobodném přístupu k informacím je vystavěn na předpokladu, že informace lze od povinných subjektů požadovat i opakovaně, v různé míře granularity, v různé struktuře a analytické skladbě, přičemž předchozí vyhovění žádosti jednoho žadatele nesmí být na újmu posouzení žádosti jiného žadatele. Žadatelé tak mají právně neomezené možnosti žádat o různé kombinace strukturovaných dat se zjevnou možností získané osobní údaje kombinovat a tím překonávat či potlačovat zdánlivou izolovanost pseudonymizovaných osobních údajů. Pseudonymizované údaje tak může k identifikaci konkrétní osoby využít kdokoliv, nejen konkrétní žadatel o informace. Tuto skutečnost vyhodnotil Městský soud v Praze jako rozhodující pro závěr, podle něhož přidělení anonymního identifikátoru jednotlivým pojištěncům či pacientům (které ve své žádosti navrhnul žadatel o informace) nemá za následek anonymizaci údajů. Za situace, kdy pokročilé technologie umožňují propojování informací od různých zpracovatelů a kdy je velké množství informací veřejně dostupné, nelze vyloučit možnost identifikace jednotlivých osob ani tehdy, pokud by jim byl přidělen formálně bezvýznamový identifikátor propojující údaje v různých souborech dat.

Informace o spisové značce soudního řízení může být osobním údajem – objektivní pojetí ochrany osobních údajů

Nejvyšší správní soud se zabýval otázkou, zda může být osobním údajem také spisová značka trestního řízení. Dospěl přitom k závěru, že při posuzování, zda může být určitá informace osobním údajem ve smyslu čl. 4 odst. 1 obecného nařízení o ochraně osobních údajů, je třeba postupovat v souladu s tzv. objektivním poje-

tím osobních údajů. V tomto pojetí se naplnění definice osobního údaje neposuzuje ze subjektivního pohledu správce či zpracovatele, který údaji v daný moment disponuje, ale zjišťuje se, zda existuje další informace, která by ve spojení s původní informací mohla vést k identifikaci subjektu údajů. Informace je tedy osobním údajem, existují-li jakékoliv osoby nebo orgány, které by subjekt údajů dokázaly na základě dané informace (ve spojení s jim dostupnými doplňujícími údaji) identifikovat.

S přihlédnutím k objektivnímu pojetí osobních údajů dospěl Nejvyšší správní soud k závěru, že osobním údajem může být také spisová značka trestní věci projednávané určitým soudem, a to za předpokladu že existují další informace, které jiný subjekt má nebo by mohl mít k dispozici a s jejichž pomocí by mohl identifikovat konkrétního obžalovaného v řízení, k němuž se spisová značka vztahuje. Takovými dalšími informacemi mohou být například jiné údaje týkající se totožného řízení zveřejněné podle zákona o svobodném přístupu k informacím, rozhodnutí týkající se řízení zveřejněná na webových stránkách soudů, nedostatečná pseudonymizace obžalovaného, mediální zprávy apod. Není přitom rozhodné, zda konkrétní žadatel o informace je sám schopen subjekt údajů identifikovat.

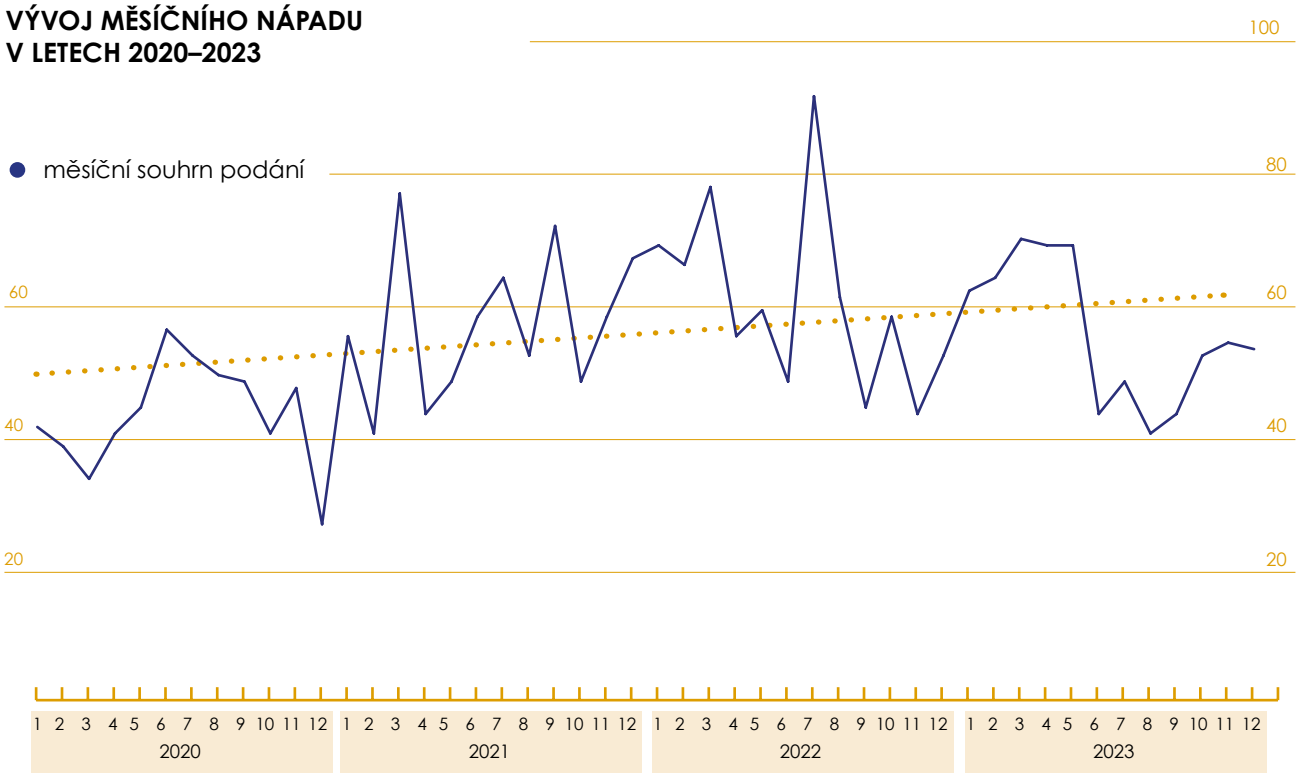
Nadřízeným orgánem Kanceláře Poslanecké sněmovny Parlamentu ČR je Úřad

Městský soud v Praze při posuzování otázky, kdo je nadřízeným orgánem Kanceláře Poslanecké sněmovny Parlamentu ČR, dospěl k závěru, že s účinností ode dne 2. ledna 2020 je orgánem věcně příslušným k rozhodnutí o odvolání proti rozhodnutí tohoto povinného subjektu Úřad a nikoliv osoba stojící v čele povinného subjektu, neboť nadřízený orgán nelze určit dle pravidel stanovených v § 178 správního řádu, a proto je třeba použít zvláštní pravidlo obsažené v § 20 odst. 5 zákona o svobodném přístupu k informacím. Obdobné závěry přirozeně platí též pro Kancelář Senátu Parlamentu ČR.

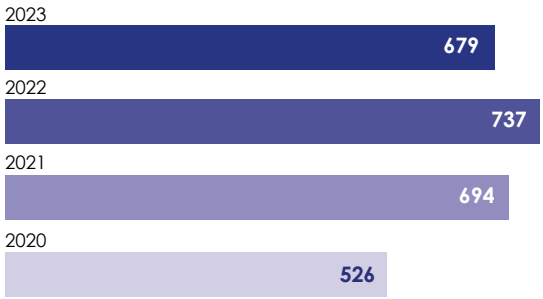
Rozhodnutí o odložení žádosti o informace je rozhodnutím v materiálním smyslu, proti němuž lze podat stížnost

Městský soud v Praze posuzoval otázku, zda je odložení žádosti o informace z důvodu vymezeného v § 14 odst. 5 písm. c) zákona o svobodném přístupu k informacím (požadované informace se nevztahují k působnosti povinného subjektu) rozhodnutím v materiálním smyslu. Dospěl přitom k závěru, že takové odložení žádosti rozhodnutím v materiálním smyslu je, což znamená, že proti němu lze podat stížnost na postup povinného subjektu při vyřizování žádosti o informace. Vydání rozhodnutí o tomto opravném prostředku je pak v souladu s judikaturou Nejvyššího správního soudu třeba považovat za rozhodnutí ve smyslu § 65 soudního řádu správního, jelikož povaha vyřízení stížnosti je odlišná v případech, kdy přezkoumávaný postup dotázaného povinného subjektu spočívá v nečinnosti a kdy spočívá ve věcném vyřízení žádosti. Věcným vyřízením žádosti o informace je právě i odložení žádosti podle § 14 odst. 5 písm. c) zákona o svobodném přístupu k informacím.

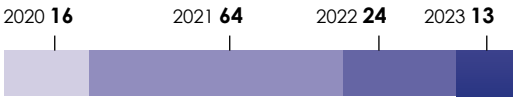
VÝVOJ MĚSÍČNÍHO NÁPADU V LETECH 2020–2023



SROVNÁNÍ VELIKOSTI NÁPADU V LETECH 2020–2023



POČET SOUDNÍCH ŘÍZENÍ S ÚČASTÍ ÚŘADU TÝKAJÍCÍCH SE ZÁKONA Č. 106/1999 SB. OZNÁMENÝCH ÚŘADU V JEDNOTLIVÝCH LETECH



Specifickým jevem 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 subjekty a tato rozhodnutí je nucen 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.

ORGANIZAČNÍ ZAJIŠTĚNÍ ROZHODOVÁNÍ ÚŘADU V OBLASTI SVOBODNÉHO PŘÍSTUPU K INFORMACÍM

Dnem 1. září 2022 nabyla účinnosti podstatná část novely zákona o svobodném přístupu k informacím provedená zákonem č. 241/2022 Sb., která mimo jiné vymezila nový typ povinného subjektu, kterým je veřejný podnik. S ohledem na pravidla pro určování nadřízeného orgánu v agendě svobodném přístupu k informacím se tak Úřad stal nadřízeným orgánem další rozsáhlé skupiny povinných subjektů, aniž by to bylo adekvátně reflektováno v personálním zajištění odboru práva na informace. S účinností od 1. ledna 2023 pak byly v řízení vedeném podle zákona o svobodném přístupu k informacím zavedeny některé nové procesní postupy, které rovněž objektivně přinesly další zatížení personálních kapacit Úřadu, které je o to markantnější v případě úřadu s takto široce vymezenou působností.

Zde lze připomenout apel obsažený v nálezu Ústavního soudu ze dne 17. ledna 2023, sp. zn. Pl. ÚS 25/21, podle něhož se požadavky kladené na výkon agendy poskytování informací podle zákona o svobodném přístupu k informacím, zejména pak úroveň správních rozhodnutí vydávaných povinnými subjekty a jejich nadřízenými orgány, od počátku účinnosti tohoto zákona nepoměrně zvýšily. Na její kvalitu přitom nelze rezignovat s poukazem, že se jedná pouze o okrajovou působnost povinných subjektů. Naopak, v současnosti již tvoří poskytování informací podle zákona o svobodném přístupu k informacím nedílnou součást jejich působnosti, a tomu je samozřejmě nutno přizpůsobit jejich personální vybavení. ●

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). Vyváření a transformace AIFO je právě úkolem informačního systému ORG (tento systém je také označován jako „převodník identifikátorů“).

ZIFO je Informačním systémem 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. Všechna ZIFO a AIFO jsou uložena v Informačním systému 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 předpisů ochrany 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.

Hlavními požadavky na IS ORG jsou:

- vysoká dostupnost – poskytování služby v režimu 7×24, 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 o kybernetické bezpečnosti byl ORG určen jako informační systém kritické infrastruktury a jako správce takového systému plní Úřad technická opatření stanovená ve vyhlášce o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

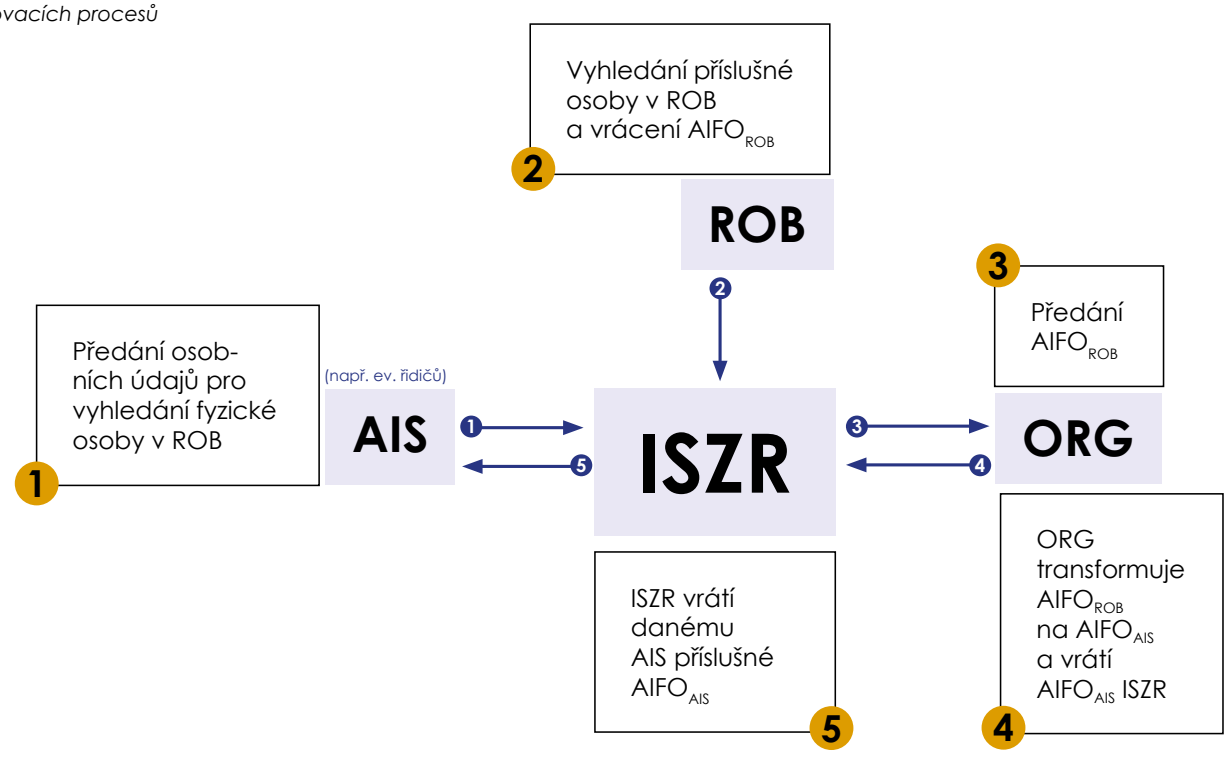
V roce 2023 uběhlo 11 let od začátku fungování základních registrů. Za dobu fungování základních registrů jejich význam i míra využívání velmi narostly. Jen počet provedených transakcí[33] v IS ORG vzrostl více než sedminásobně. Za minulý rok stoupl počet provedených transakcí o 13,09% proti roku 2022. Zároveň opět stoupl i maximální měsíční počet transakcí, konkrétně o 10,99%. Spolu s tím roste i význam a provozní zatížení IS ORG. V roce 2023 jsme zaznamenali vyšší využití základních registrů a tím i IS ORG v měsících únor a březen v souvislosti s hromadným zřizováním datových schránek pro podnikající fyzické osoby.

V roce 2023 proběhla další obnova HW, jemuž skončila podpora od výrobce. Systém IS ORG je

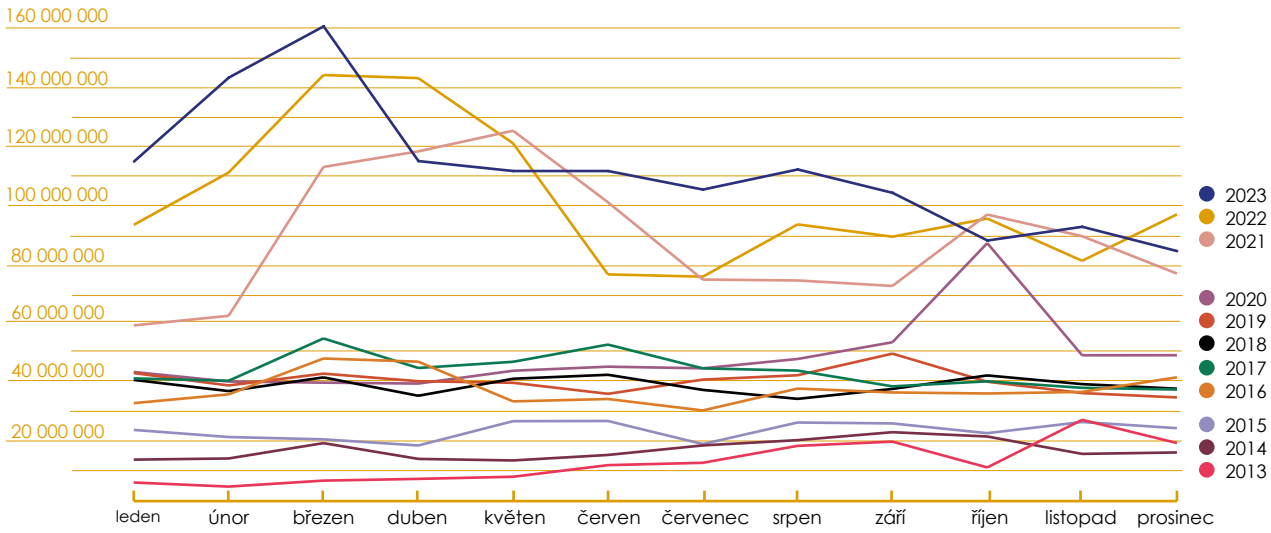
33 Transakcí se rozumí operace provádění v IS ORG – založení ZIFO, generování AIFO, překlad AIFO pro jinou agendu a další.

PRINCIP PŘIŘAZENÍ AIFO DANÉ AGENDĚ

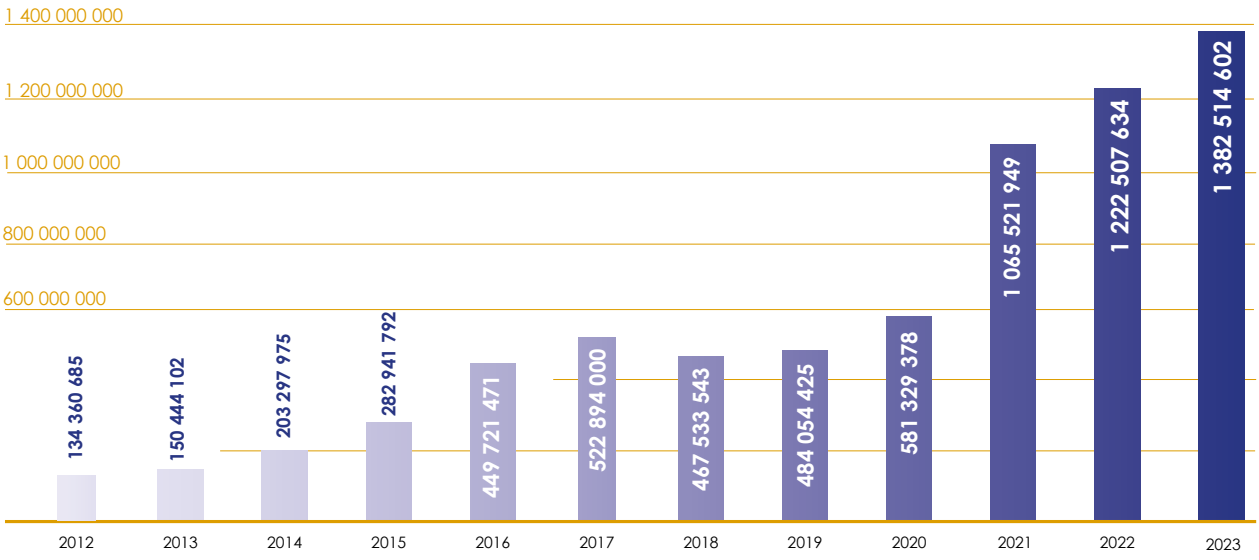
zjednodušené schéma bez ověřovacích a logovacích procesů



POČET TRANSAKCÍ V LETECH 2012–2023

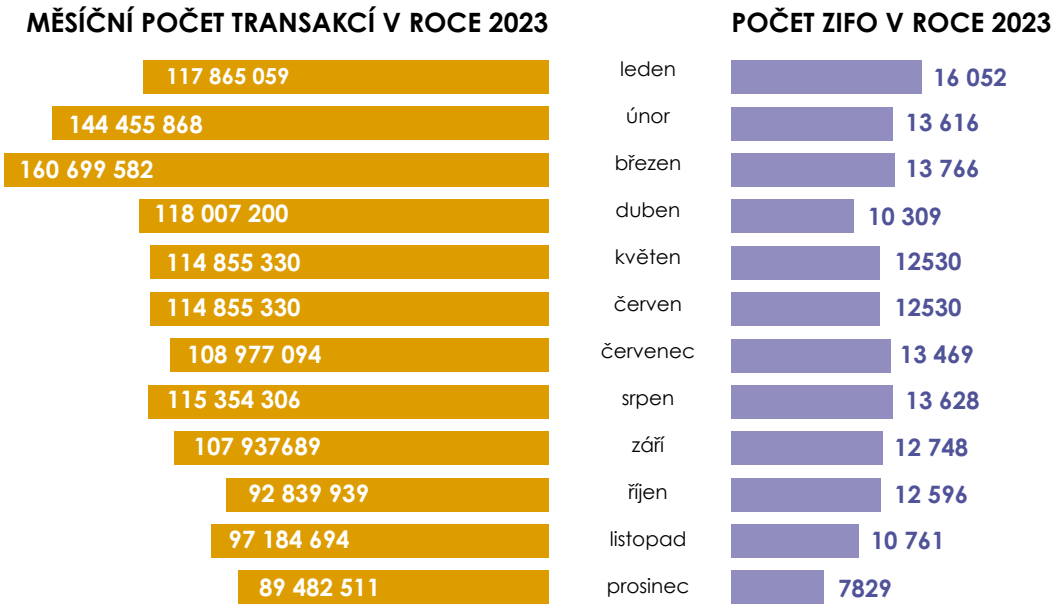


CELKOVÝ POČET TRANSAKCÍ V LETECH 2012–2023



v dobré kondici a v tuto chvíli mimo obnovy HW po konci podpory zvládá zvýšené nároky bez potíží s výkonem a výpadků.

V listopadu 2023 proběhl dozorový audit v rámci certifikace IS ORG podle ČSN EN ISO/IEC 27001:2014 bez nálezu neshody. V říjnu 2023 byla vydána česká verze ČSN EN ISO/IEC 27001:2022. Započali jsme úpravu dokumentace, tak aby byla v souladu s novou verzí normy. V roce 2025 bude IS ORG certifikován již podle normy ČSN EN ISO/IEC 27001:2022. Kyberbezpečnost je pro provoz IS ORG absolutní prioritou. IS ORG v roce 2023 nezaznamenal větší bezpečnostní incident.



Pokračuje trend růstu využívání základních registrů, důvodem je mimo jiné také obecný rozvoj propojeného datového fondu. V roce 2024 čeká IS ORG schválení nové strategie nana nadcházející období, 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, přípravy na splnění požadavků normy ČSN EN ISO/IEC 27001:2022 a hlavně na nové úkoly spojené s dalším rozvojem Základních registrů. Lze očekávat rovněž dynamický vývoj vzhledem k probíhajícím změnám ve správě základních registrů v souvislosti s projektem Základní registry nové generace. ●

Dozorová činnost a další odborné aktivity

CEF 2023

Úřad se i v roce 2023 zapojil do koordinované dozorové akce Sboru označené jako CEF 23 (Coordinated Enforcement Framework). Jejím tématem bylo prověření úlohy a postavení pověřenců pro ochranu osobních údajů. Úřad za tímto účelem oslovil všech 14 ministerstev prostřednictvím dotazníku zaměřeného na uvedené téma. Dotazník byl vypracován ve spolupráci se zapojenými evropskými dozorovými úřady.

Obdržené odpovědi Úřadu poskytly náhled na postavení pověřenců pro ochranu osobních údajů v rámci oslovených ministerstev. Na základě nich Úřad dospěl k závěru, že i v rámci takto homogenní skupiny správců osobních údajů lze pozorovat významné rozdíly v podmínkách, které vytváří pro možnost řádného plnění úkolů pověřence pro ochranu osobních údajů, jež mu vyplývají z příslušných ustanovení nařízení (EU) 2016/679.

Některé z odpovědí ministerstev podle Úřadu indikovaly podezření na porušení zejména čl. 38 nařízení (EU) 2016/679. Jednalo se například o možná pochybení ministerstev spočívající v tom, že nezapojují pověřence pro ochranu osobních údajů náležitě a včas do veškerých záležitostí souvisejících s ochranou osobních údajů, s čímž souvisí, že pověřenci pro ochranu osobních údajů podle dotazníků nemají vždy přístup k informacím souvisejícím se zpracováním osobních údajů. Z odpovědí rovněž vyplynulo, že některá ministerstva dávají pověřencům pro ochranu osobních údajů pokyny týkající se výkonu jejich úkolů, což nařízení (EU) 2016/679 výslovně zapovídá.

Na základě informací vyplývajících z tohoto dotazníkového šetření Úřad zejména v případech indikujících možné porušení nařízení (EU) 2016/679 hodlá přistoupit k využití svých vyšetřovacích a podle zjištěných skutečností případně i nápravných pravomocí ve vztahu k osloveným ministerstvům.

SCHENGENSKÁ SPOLUPRÁCE

Stejně jako v předchozích letech i v roce 2023 plnil Úřad roli vnitrostátního dozorového orgánu, kterému přísluší dohled nad zpracováním osobních údajů v rozsáhlých evropských infor-

mačních 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 (SIS, jehož nová, již třetí, generace byla spuštěna 7. března 2023), Vízový informační systém (VIS), Celní informační systém (CIS) a databázi otisků prstů Eurodac. Úřad je též příslušný k dohledu nad zpracováním osobních údajů národní jednotkou Europolu.

Úřad v této oblasti v roce 2023 ukončil dvě kontroly vedené u Policie ČR, a to kontrolu zpracování osobních údajů v národní části Schengenského informačního systému druhé generace a dále kontrolu národní jednotky Europolu, přičemž ani jednou z těchto kontrol nebylo konstatováno porušení povinností v oblasti ochrany osobních údajů.

Úřad dále v souladu s kontrolním plánem provedl kontrolu zpracování osobních údajů v systému Eurodac pro účely vymáhání práva, v rámci, které bylo shledáno, že kontrolovanou osobou (Ministerstvo vnitra) není postup porovnávání údajů o otiscích prstů s údaji systému Eurodac na interní úrovni upraven odpovídajícím způsobem, a to z hlediska nastavení úloh a odpovědností konkrétních útvarů. Zároveň však nebylo konstatováno porušení povinnosti při zpracování osobních údajů, neboť porovnání údajů o otiscích prstů s údaji systému Eurodac dosud nebylo realizováno. Bylo dále zjištěno, že kontrolovaná osoba pouze částečně splnila povinnost podle čl. 43 odst. 1 nařízení (EU) č. 603/2013, tj. povinnost nahlásit Evropské komisi útvary, jimž byly svěřeny stanovené konkrétní role, a bezodkladně oznámit jakoukoli jejich změnu. Tato povinnost musí být plněna i za situace, kdy porovnání údajů o otiscích prstů s údaji systému Eurodac nebylo realizováno tak, jak bylo v protokolu o kontrole konstatováno.

V souvislosti s Vízovým informačním systémem Úřad v roce 2023 prováděl dvě kontroly zpracování osobních údajů při vízovém procesu. Podrobnosti o těchto kontrolách jsou uvedeny v kapitole Závěry z kontrol.

Při své činnosti související se schengenskou agendou Úřad spolupracuje s dozorovými úřady ostatních členských států a též s Evropským inspektorem ochrany údajů (EDPS), s nimiž se pravidelně setkává v rámci tří koordinačních skupin a v rámci výboru pro koordinovaný dozor, přičemž zástupci Úřadu se v roce 2023 zúčastnili všech deseti uskutečněných jednání.

Jako další formu schengenské spolupráce lze považovat hodnotící a monitorovací mechanismus k ověření uplatňování schengenského acquis, tzv. schengenské evaluace, při kterých je v jednotlivých členských státech vyhodnocován soulad s evropským právem v oblastech jako jsou společná vízová politika, policejní spolupráce, problematika vnějších hranic nebo ochrana osobních údajů. Hodnotící týmy se skládají z expertů Evropské komise a členských států. Oba Úřadem nominovaní experti pro oblast ochrany osobních údajů byli Evropskou komisí zařazeni do skupiny expertů, a jeden z nich též vybrán pro konkrétní evaluaci. Zástupkyně Úřadu tak byla členem hodnotícího týmu pro evaluaci Litvy a osobně se účastnila šetření, které bylo v Litvě realizováno v květnu 2023.

Úřad je ze své pozice dále příslušný též k vyřizování podání souvisejících se zpracováním osobních údajů ve zmíněných informačních systémech. V roce 2023 Úřad obdržel a vyřídil celkem 19 podnětů týkajících se Schengenského informačního systému (stížnosti, žádosti o konzultaci či žádosti o přístup k osobním údajům, jejich opravu či výmaz) a též 3 podání vztahující se ke zpracování osobních údajů ve Vízovém informačním systému (stížnost a žádosti o konzultaci, resp. opravu a výmaz). Z hlediska ostatních systémů nebyla žádná podání učiněna. Úřadu však bylo v roce 2023 doručeno 14 dotazů týkajících se vízové problematiky. Tyto dotazy byly, stejně jako v předchozích letech, Úřadu adresovány i přesto, že vízová politika České republiky není v jeho působnosti. Ve všech případech však Úřad jednotlivým žadatelům objasnil své zákonné kompetence a poskytl relevantní informace a kontaktní údaje na příslušné orgány s cílem pomoci žadatelům s řešením jejich životní situace. I přesto, že jsou Úřadu výše uvedená podání často zasílána i v anglickém, ukrajinském či ruském jazyce, se Úřad vždy snaží žadatelům poskytnou všechny potřebné informace v pro ně srozumitelné podobě.

POČET VYŘÍZENÝCH PODNĚTŮ OHLEDNĚ ZPRACOVÁNÍ ÚDAJŮ V SCHENGENSKÉM PROSTORU
v letech 2013–2023

	SIS	VIS	Vízové dotazy
2023	19	3	14
2022	27	0	10
2021	40	1	6
2020	30	0	12
2019	58	0	13
2018	22	0	19
2017	10	0	26
2016	10	0	17
2015	11	0	48
2014	10	0	66
2013	9	0	63

PORADENSTVÍ A KONZULTACE

Úřad v rámci své konzultační agendy obdržel obdobně jako v minulých letech značné množství dotazů týkajících se kamerových systémů v nejrůznějších souvislostech (typicky ve věci tzv. kamery souseda umístěné na fasádě či plotu jeho rodinného domu nebo v rámci digitálního kukátka umístěném ve vchodových dveřích či kamer alokovaných v sídle či provozně široké škály soukromých či veřejných subjektů). Na setrvalý zájem o předmětné téma Úřad zareagoval koncipováním Metodiky k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů, jež byla předložena k veřejné konzultaci. Metodika byla přepracována a doplněna z původního dokumentu (vydaného v roce 2012) v souvislosti s přijetím obecného nařízení a dalšími dokumenty ke kamerovým systémům (Pokyny Evropského sboru pro ochranu osobních údajů č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky). V rámci přijetí těchto dokumentů došlo k určitým změnám (např. zrušení registrace zpracování osobních údajů, upřesnění výkladu práv subjektů údajů), kterými se povinnosti správců pozměnily nebo upravily. Metodika není dokumentem, jehož dodržování by bylo pro jakýkoliv subjekt povinné. Jejím cílem je přispět k jasnějšímu výkladu některých povinností v oblasti zpracování osobních údajů kamerovými systémy. Úřad pro ochranu osobních údajů publikoval metodiku koncem dubna 2023 na svém webu k veřejné diskusi. V rámci veřejné diskuse bylo zasláno celkem 119 připomínek od 18 subjektů. Po zpracování připomínek a jejich případném projednání s některými subjekty připravil Úřad novou verzi, která bude publikována začátkem roku 2024.

Dalšími frekventovanými tématy dotazů veřejnosti bylo nakládání s osobními údaji v rámci společenství vlastníků jednotek, pořizování záznamů ze zastupitelstva obce či možnosti a rozsahu výkonů práv subjektů údajů. Rovněž Úřad obdržel množství dotazů týkajících se občanskoprávních sporů, které však nejsou v působnosti Úřadu. Míra konkrétnosti odpovědí byla především ovlivněna úrovní popisu skutkového stavu (v mnoha případech omezeného pouze na obecné shrnutí situace, typicky bez bližší

specifikace účelu či dalších sektorových nebo technických specifik zpracování osobních údajů) a působností Úřadu (kdy např. Úřad není kompetentní k metodickému výkladu zvláštních právních předpisů, které jsou v gesci především jednotlivých ministerstev).

V roce 2023 byly primárně v budově Úřadu poskytnuty osobní konzultace např. společnosti Alza.cz a.s., a rovněž společnosti IRSnet CZ s.r.o. (provozovatel sítě Ticketportal.cz) ve věci zasílání obchodních sdělení. Tato problematika byla konzultována i se Sdružením agentur pro výzkum trhu a veřejného mínění (SIMAR) v kontextu specifik tohoto odvětví. S pověřenci pro ochranu osobních údajů několika vysokých škol a zástupkyní Centra pro studium vysokého školství (CSVŠ) byla projednána problematika zasílání dotazníků absolventům ze strany vysokých škol, které následně zpracovává CSVŠ v rámci projektu Eurograduate. S Ministerstvem obrany bylo prodiskutováno zpracování v rámci projektu Virtuálního náborového střediska. Prostřednictvím videokonference s Národním úřadem pro kybernetickou bezpečnost a informační bezpečnost (NÚKIB) byla debatována problematika koordinovaného zveřejňování zranitelnosti, které představuje formalizovaný proces dobrovolného objevování zranitelnosti v produktech informačních a komunikačních technologií třetími osobami tzv. objeviteli (etickými hackery), včetně notifikace objevené zranitelnosti vlastníkovi/správci ICT produktu (tzv. zodpovědné osoby) za účelem provedení bezpečnostní opravy.

V rámci podpory vzdělávání v ochraně osobních údajů uspořádal Úřad pro ochranu osobních údajů v roce 2023 několik pracovních seminářů určených pro správce, pověřence nebo odbornou veřejnost. Semináře byly zaměřeny na různá aktuální nebo žádaná témata. Částečně tak Úřad navázal na semináře pro pověřence, které proběhly v roce 2018, kdy nabylo účinnost obecné nařízení o ochraně osobních údajů.

První seminář byl zaměřen na výkon práv subjektů údajů v souvislosti s nově přijatými Pokyny Evropského sboru 1/2022 o právech subjektů údajů. Seminář probíhal pouze prezenční formou za účasti 34 externích účastníků. Na něj navázal seminář k problematice posouzení vlivu na ochranu osobních údajů. Seminář byl primárně určen pověřencům pro ochranu osobních údajů u správců provádějící vysoce rizikové zpracování, kde se předpokládá provedení posouzení vlivu na ochranu osobních údajů. Seminář proběhl rovněž pouze prezenční formou za účasti 33 externích účastníků. Dále Úřad uspořádal odborný seminář k tématu předávání osobních údajů do třetích zemí, který byl určen pověřencům pro ochranu osobních údajů u správců, kteří předávají nebo zamýšlejí předávat osobní údaje do třetích zemí. Tento seminář probíhal jak prezenčně (32 externích účastníků), tak souběžně i online formou (252 účastníků z řad pověřenců ze státní správy, samosprávy, průmyslu, zástupců školství, zdravotnictví, bank, pojišťoven apod.). Poslední seminář v roce 2023 nabídl příklady dobré praxe v ochraně osobních údajů v širších souvislostech se zaměřením na rozhodovací činnost Úřadu ve světle aktuální judikatury. Seminář proběhl rovněž prezenční i online formou a celkem se ho zúčastnilo 205 zájemců. Semináře se setkaly s velmi pozitivními ohlasy ze strany pověřenců a odborné veřejnosti. Úřad bude ve vzdělávacích akcích pro pověřence pokračovat.

Úřad v roce 2023 započal s vydáváním osvětových materiálů formou tištěných informačních letáků týkajících se např. podmínek poskytování konzultací, souborů cookies, Schengenského informačního systému, posouzení vlivu na ochranu osobních údajů (tzv. DPIA) a předávání údajů do třetích zemí. Konzultanti Úřadu se rovněž zúčastnili tradiční celostátní konference ISSS 2023 (Internet ve státní správě a samosprávě) v Hradci Králové a Výroční konference Spolku pro ochranu osobních údajů: GDPR 2023 v Praze.

Stejně jako v předchozích letech ani v roce 2023 neobdržel Úřad žádost, která by splňovala požadavky na poskytnutí konzultace podle čl. 36 obecného nařízení. V předmětném roce Úřad také neobdržel žádost o projednání ve věci vzniku nové evidence v rámci spravujícího orgánu podle § 38 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Poradenství a konzultace byly i v tomto roce poskytovány písemnou i telefonickou formou, mj. prostřednictvím informační linky.

EVROPSKÁ A ZAHRANIČNÍ SPOLUPRÁCE

Evropský sbor pro ochranu osobních údajů

Úřad je součástí Evropského sboru pro ochranu osobních údajů (EDPB) zřízeného podle článku 68 GDPR. Podílí se na činnosti Sboru, především při přípravě odborných dokumentů (pokyny, doporučení, stanoviska, rozhodnutí) převážně určených odborné nebo laické veřejnosti. Sbor rovněž v některých případech vydává stanoviska nebo písemná vyjádření na vyžádání institucí, například Evropské komise nebo členů Evropského parlamentu.

Zástupce Úřadu se účastnil všech patnácti plenárních zasedání EDPB, z nichž šest bylo s osobní účastí v Bruselu a zbývající proběhly vzdálenou formou. Vedle pléna, které je vrcholným orgánem, pracují v rámci EDPB tematicky specializované odborné skupiny (expert subgroups) složené z odborníků členských úřadů. Z celkového počtu dvanácti odborných skupin má Úřad svého zástupce v osmi z nich, konkrétně je to:

- Skupina pro strategické poradenství (Strategic Advisory),
- Skupina pro spolupráci (Cooperation),
- Skupina pro technologii (Technology),
- Skupina pro hranice, cestování a prosazování práva (Borders, Travel and Law Enforcement),
- Skupina pro mezinárodní předávání (International Transfers),
- Skupina pro klíčová ustanovení (Key Provisions),
- Skupina pro prosazování práva (Enforcement),
- Skupina uživatelů IT (IT Users).

Delegáti v těchto odborných skupinách se účastnili celkem 71 pracovních schůzí, konaných ve valné většině distančně, což představuje účast téměř 81 % ze všech schůzí uskutečněných v těchto podskupinách v referenčním roce. V případě jednoho dokumentu (Pokyny 01/2022 k právům subjektů údajů) byl úřad spolupracujícím zpravodajem, přičemž tato aktivita byla ukončena vypořádáním připomínek obdržených v rámci veřejné konzultace. Dále se Úřad podílí na přípravě jednotné metodiky pro vykazování souměřitelných statistických údajů vypovídajících o činnosti členů EDPB. Koncem roku se Úřad přihlásil jako spolupracující zpravodaj k nově chystaným dvěma stanoviskům ohledně závazných podnikových pravidel pro předávání osobních údajů do zahraničí. Ve dvou případech pracoval delegát Úřadu jako člen týmu pro hodnocení sboru předložených závazných podnikových pravidel.

V roce 2023 vydal EDPB řadu pokynů, které jsou podrobněji pojednány v části „Přehled oblastí upravených pokyny EDPB".

Rada Evropy

Zástupci úřadu se ve francouzském Štrasburku zúčastnili obou (v červnu a listopadu) plenárních zasedání Konzultačního výboru pro Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat T-PD).

Výbor mimo jiné schválil a publikoval Pokyny k ochraně údajů při zpracování osobních údajů pro účely boje proti praní špinavých peněz/proti financování terorismu (AML/CFT). Účelem těchto pokynů je poskytnout orientaci v tom, jak začlenit požadavky Úmluvy 108+ v oblasti AML/CFT, aby byla zajištěna odpovídající úroveň ochrany údajů a zároveň usnadněny přeshraniční toky údajů. Dalšími dokumenty schválenými a uveřejněnými Výborem jsou Vzorové smluvní doložky pro přeshraniční toky osobních údajů pro předávání údajů mezi správci (Module 1) a mezi správcem a zpracovatelem (Module 2). Zároveň se připravují další vzorové smluvní doložky pro předávání osobních údajů mezi zpracovateli (Module 3).

Světové shromáždění pro ochranu soukromí (GPA)

Ve dnech 15.–20. října 2023 se na Bermudách konala 45. výroční konference Světového shromáždění pro ochranu soukromí (Global Privacy Assembly). Delegáti přijali Strategický plán na léta 2023–2025 a také následující usnesení:

- Usnesení o umělé inteligenci a zaměstnávání,
- Usnesení o zdravotních datech a vědeckém výzkumu,
- Usnesení o dosahování globálních standardů ochrany dat,
- Usnesení o knihovně GPA,
- Usnesení o systémech generativní umělé inteligence,
- Usnesení o zřízení pracovní skupiny pro mezisektorovou genderovou perspektivu v ochraně dat,
- Usnesení o ocenění za ochranu soukromí a lidská práva.

Konference evropských dozorových úřadů

Konference evropských dozorových úřadů (tzv. jarní konference) se tentokrát konala ve dnech 10.–12. května 2023 v Budapešti. Úřad na ni vyslal tři pracovníky. Konference přijala tři dokumenty, a to:

- Usnesení akreditaci dozorového úřadu San Marina za člena konference,
- Usnesení o potřebě rozšíření spolupráce v oblasti ochrany osobních údajů a soutěžního práva,
- Usnesení o revizi jednacího řádu konference.

Delegáti Úřadu získali poznatky zejména o aktuální judikatuře SDEU a ESLP, spolupráci při prosazování práva mezi členy a nečleny Evropského hospodářského prostoru, o postavení pověřenců pro ochranu osobních údajů a v neposlední řadě z oblasti týkající se vztahu mezi právem na ochranu osobních údajů a právem v oblasti hospodářské soutěže. Některé konferenční příspěvky se zabývaly vlivem moderních informačních technologií na ochranu osobních údajů a soukromí.

European Case Handling Workshop – Bern

Pořadatelství letošního ročníku evropského semináře k dozorové praxi se ujal švýcarský federální dozorový úřad (FDPIC). Účastnila se ho ve dnech 8.–9. listopadu 2023 v Bernu také expertka českého úřadu. Celkem se na akci sjelo 80 účastníků z 29 zemí. Každoročně pořádaný workshop je příležitostí pro setkání zástupců dozorových úřadů při rozhovorech nad konkrétními otázkami ochrany osobních údajů. Z celkem třinácti témat, které pořadatel účastníkům nabídl, lze jmenovat např. diskusi o diskreční pravomoci dozorového orgánu při vyřizování stížností, o dopadech a újmách plynoucích z nedostatečné ochrany osobních údajů či o technologiích detekce tváře a rozpoznání tváře z pohledu ochrany osobních údajů.

Stáž v polském dozorovém úřadě

Úřad se v uplynulém roce zapojil do společného projektu EDPB a EDPS Secondment Programme, v rámci, kterého byl v květnu 2023 jeden ze zaměstnanců Úřadu vyslán na třítýdenní odbornou stáž u polského dozorového úřadu – Urząd Ochrony Danych Osobowych (UODO). Jednalo se přitom o pilotní ročník celého programu, prostřednictvím kterého EDPB naplňuje svůj úkol podporovat společné školící programy a usnadňovat výměny pracovníků mezi dozorovými úřady, jak mu ukládá čl. 70 odst. 1 písm. v) GDPR.

Odborné stáže se u polského úřadu současně účastnil též německý zástupce z Úřadu komisaře pro ochranu osobních údajů a svobodu informací spolkové země Porýní-Falc. V rámci programu tak mohlo dojít k výměně informací a zkušeností rovnou mezi třemi státy, přičemž vedle poznatků o organizaci dozorových orgánů a specifikách nastavení ochrany osobních údajů v jednotlivých státech, měli zástupci možnost prodiskutovat též aktuální výzvy kterým ve svých úřadech aktuálně čelí. Jednou z představovaných oblastí hodných zmínky jsou vzdělávací a osvětové aktivity, kterými se UODO právem pyšní. Příkladem budiž projekt Twoje dane – Twoja sprawa (Tvoje údaje – Tvoje záležitost), zaměřený primárně na učitele, a prostřednictvím ně pak též na žáky základních a středních škol, zástupci českého i německého úřadu měli možnost se v rámci probíhajícího, toho času již třináctého, ročníku zúčastnit webináře na téma biometrie.

Program stáží nadto pomohl mezi všemi zúčastněnými stranami otevřít další komunikační kanál a umožnil tak do budoucna bližší spolupráci pro prosazování ochrany osobních údajů napříč členskými státy.

Praktické školení k auditům webových stránek

Zástupce Úřadu se ve dnech 12.–13. června 2023 účastnil v Bruselu praktického školení organizátory zvaný „bootcamp". Akce byla věnována nástrojům pro provádění kontrol webových stránek ohledně používání souborů cookies. V rámci tohoto školení se probíraly metody a postupy související s evidencí stavu a posuzováním souladu kontrolovaných internetových stránek s legislativou, s důrazem na cookies, jejich klasifikaci a související softwarové nástroje. Zastoupeni byli odborníci jednotlivých dozorových úřadů, kteří mají danou problematiku v gesci, sdíleli zkušenosti a konzultovali postupy, které jednotlivé úřady v dané oblasti aplikují. Vzhledem ke kladné odezvě účastníků bylo dohodnuto obdobnou specificky zaměřenou akci uspořádat i v roce 2024.

Bilaterální aktivity

Dne 16. května 2023 navštívila Úřad pětičlenná delegace odborníků na kybernetickou bezpečnost ze Senegalu, kterou vedla místopředsedkyně senegalské Komise pro ochranu osobních údajů. Návštěvu zprostředkovalo Ministerstvo zahraničních věcí. Zájmem senegalské delegace bylo poznat zkušenosti úřadu z oblasti dozoru a také se zkušenostmi v oblasti kyberbezpečnosti. Úřad měl příležitost představit svoji činnost také na poli mezinárodní spolupráce, především v Evropském sboru pro ochranu osobních údajů.

Ve dnech 25.–27. září 2023 se na pozvání slovenské strany uskutečnilo v Trenčíně setkání vedoucích pracovníků českého a slovenského úřadu. Účelem setkání byla výměna zkušeností získaných během pěti let uplatňování a prosazování obecného nařízení o ochraně osobních údajů. Jednání bylo rozčleněno do dvanácti tematicky specializovaných bloků (např. dozorová činnost, kamerové systémy, oznamování porušení zabezpečení, legislativa EU, a také ekonomické a technické aspekty činnosti úřadů).

Dne 1. listopadu 2023 přivítali předseda a místopředseda úřadu pana Vencislava Karadžova, předsedu bulharské Komise pro ochranu osobních údajů, který je současně členem výkonného výboru Světového shromáždění pro ochranu soukromí (GPA). Vedle tématu vzájemné spolupráci mezi dozorovými úřady hovořili o návrhu připravovaného evropského nařízení o procesních pravidlech při prosazování obecného nařízení.

Mechanismus spolupráce

Formy spolupráce mezi dozorovými úřady upravuje obecné nařízení pro ochranu osobních údajů. K jejímu usnadnění úřady využívají elektronický nástroj Systém pro výměnu informací o vnitřním trhu (Internal Market Information – IMI). V praxi je nejvyužívanější formou spolupráce postup podle článku 61 GDPR, který je méně formální a spolupráce není striktně povinná, a který je využíván pro vzájemné konzultace, předávání informací o konkrétních případech a probíhajících šetřeních nebo k nabízení informací, u nichž je předpoklad, že by mohly být přínosné a využitelné v dozorové praxi ostatních úřadů. Během roku 2023 bylo do IMI vloženo celkem 222 žádostí o dobrovolnou spolupráci podle článku 61 GDPR, jejichž adresátem byl kromě jiných dozorových úřadů také český úřad, sám pak do systému vložil 20 žádostí.

Druhou nejpoužívanější formou spolupráce je tzv. mechanismus jediného kontaktního místa (one-stop-shop). Uplatňuje se při šetření přeshraničních případů, charakteristických tím, že zpracování osobních údajů probíhá ve více členských zemích EU anebo zpracovatelskou operací mohou být dotčeni jednotlivci sídlící ve více členských státech. V takových situacích je nejprve postupem podle článku 56 GDPR určen vedoucí dozorový úřad, který pak funguje jako jediné kontaktní místo a vede šetření daného konkrétního případu, přičemž spolupracuje s dotčenými dozorovými úřady podle článku 60 GDPR. Úřad na základě obdržených 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 25 případech, při-

čemž doposud přijal 11 z nich. Ve zbývajících případech nebylo o vedoucím dozorovém úřadu zatím rozhodnuto nebo role vedoucího dozorového úřadu nebyla přijata.

Zapojení Úřadu do činnosti EDPB v oblasti předávání a certifikací

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

Zvláštní kapitolu činnosti podskupiny v konkrétních případech představuje hodnocení jednotlivých návrhů závazných podnikových pravidel vypracovaných konkrétními skupinami podniků. Hodnocení, komentáře a doporučení podskupiny v rámci koordinační procedury (WP263) mají zajistit, aby do procedury podle čl. 64 odst. 1 písm. f) obecného nařízení byly přijímány pouze již dobře propracované návrhy. Úřad v roce 2023 ve dvou případech vykonával roli spoluhodnotitele (Accenture BCR-P, Servier BCR-C). Ve dvou případech se jako spolu reportér podílel na formulaci vlastního stanoviska Sboru k návrhu BCR (Accenture BCR-P, MAPFRE BCR-C).

V rámci podskupiny CEH zástupci Úřadu spolupracovali na hodnocení stanovisek EDPB k návrhům certifikačních kritérií pro certifikaci shody s GDPR podle čl. 42 odst. 1 obecného nařízení a nadnárodních kodexů chování podle čl. 40 odst. 2 obecného nařízení.

POSKYTOVÁNÍ INFORMACÍ ÚŘADEM PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM, JAKO POVINNÝM SUBJEKTEM

Úřad poskytoval i v roce 2023 informace o své činnosti v rozsahu, který ukládá orgánům veřejné moci jako povinným subjektům zákon o svobodném přístupu k informacím. Základní informace podle zákona o svobodném přístupu k informacím zpřístupňuje Úřad několika způsoby v souladu se zákonem č. 106/1999 Sb., a to jak na svých webových stránkách uoou.gov.cz, tak 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 na webových stránkách Úřadu zveřejňovány v souladu s § 18 zákona o svobodném přístupu k informacím.[34]

Úřad za rok 2023 eviduje 145 písemných žádostí podaných podle zákona o svobodném přístupu k informacím, což představuje 45% nárůst počtu oproti roku 2022. Lze konstatovat, že častěji bylo požadováno v jedné žádosti poskytnutí značného množství různorodých informací vzájemně nesouvisejících, případně vyšší množství rozhodnutí Úřadu, jež byly v žádostech o poskytnutí informace vymezeny typem řízení, případně předmětem řízení a rozsah byl stanoven za určité období, nejčastěji od účinnosti GDPR.

Žadatelé tradičně pocházeli nejen z řad laické veřejnosti, ale i veřejnosti odborné, kdy lze, stejně jako v předchozích letech, v roce 2023 opětovně sledovat nárust žádostí o poskytnutí informace podaných osobami vykonávajícími právnické povolání, kde lze předpokládat, že účelem žádostí o poskytnutí informace bylo využití těchto informací pro výkon této činnosti. Předmětem žádostí o poskytnutí informace byla zejména činnost Úřadu jako dozorového úřadu v oblasti ochrany osobních údajů, a to převážně ve formě jednotlivých rozhodnutí, případně dalších dokumentů týkajících se podaných podnětů/stížností kontrolních a správních řízení, včetně informací o počtu kontrol a správních řízení či

34 Zde není zohledněno specifické postavení Úřadu podle zákona č. 111/2019 Sb., tedy ustanovení § 16b a § 20 zákona č. 106/1999 Sb.

výši sankce, kterou Úřad v těchto řízení vyměřil. Žadatelé se dále zajímali obecně o fungování Úřadu, případně o činnosti svěřené Úřadu zákonem o svobodném přístupu k informacím jako povinnému subjektu i § 16b a § 20 odst. 5 zákona o svobodném přístupu k informacím

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 GDPR, případně vydaných na základě § 16b zákona o svobodném přístupu k informacím (přezkumná řízení, opatření proti nečinnosti) či protokolů z kontrol provedených Úřadem. Ve vztahu 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, případně bližší informace k dosud nejvyšší uloženým pokutám. 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. 4 zákona o svobodném přístupu k informacím na webových stránkách Úřadu.

Naprostou většinu požadovaných informací poskytl Úřad v roce 2023 bezplatně. V souladu se zákonem o svobodném přístupu k informacím Úřad na svých webových stránkách zveřejňuje sazebník úhrad za poskytování informací, nově přijatou směrnicí č. 4/2023. V roce 2023 došlo k vyměření úhrady za mimořádně rozsáhlé vyhledání informací ve dvou případech. Výše stanovených úhrad činila celkem 16 101 Kč. Vyměřená úhrada byla v obou případech nakonec zaplacena, a to přesto, že ve druhém případě byla žadatelem podána stížnost na výši požadované náhrady nákladů, která byla shledána předsedou Úřadu jako neopodstatněná. V obou případech se jednalo o žádost o poskytnutí velkého množství rozhodnutí, která musela být Úřadem vyhledána, shromážděna a zejména anonymizovanána.

Část žádostí o poskytnutí informace Úřad odložil, neboť se nevztahovala k jeho působnosti (takové byly v roce 2023 čtyři).

V roce 2023 bylo vydáno 22 rozhodnutí o odmítnutí žádosti o poskytnutí informace, případně její části. V převážné většině případů bylo odmítnuto poskytnutí pouze části informace, případně jednoho či více dotazů zaslaných v žádosti o poskytnutí informace. Převažujícím důvodem, pro který byly žádosti o poskytnutí informace zcela či alespoň částečně odmítány, byla zákonná výluka podle § 2 odst. 4 zákona č. 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 podle § 2 odst. 4 a § 3 odst. 3 zákona o svobodném přístupu k informacím, které informační povinnosti nepodléhají či jako informaci neexistující podle nového § 11b zákona o svobodném přístupu k informacím 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 GDPR nebo zákona č. 110/2019 Sb. 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 2023 podány pouze tři rozklady. Podle organizačního řádu vydává rozhodnutí v prvním stupni ředitel odboru legislativy a metodiky. O rozkladu proti prvostupňovému rozhodnutí Úřadu rozhoduje předseda Úřadu. Ve všech případech předseda Úřadu jako nadřízený orgán rozklad svým rozhodnutím zamítl a napadené rozhodnutí potvrdil.

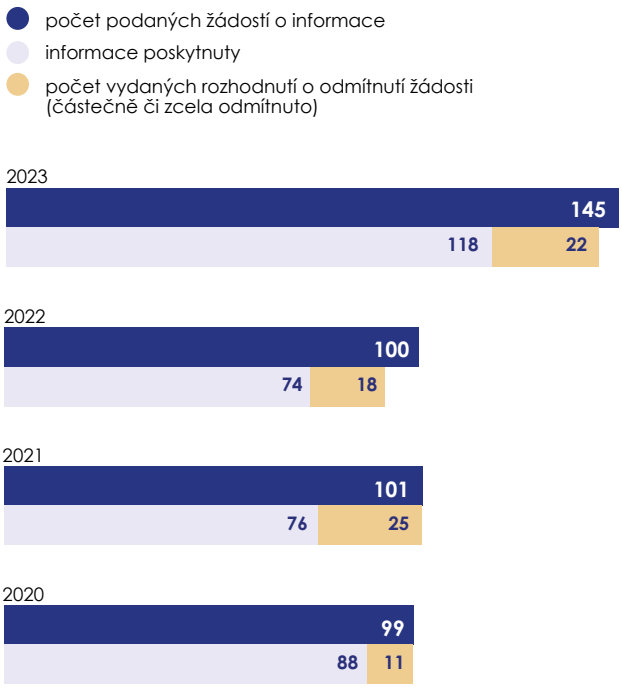
V roce 2023 nebyly Úřadem poskytnuty žádné výhradní licence.

V roce 2023 obdržel Úřad sedm stížností podle § 16a zákona o svobodném přístupu k informa-

cím. Tři z těchto stížností byly podány jedním žadatelem, který tvrdil, že mu nebyla poskytnuta úplná informace a na základě těchto stížností bylo Úřadu přikázáno požadované informace poskytnout. Jedna stížnost byla podána proti odložení žádosti o poskytnutí informace pro nedostatek působnosti a byla předsedou Úřadu shledána nedůvodnou a předchozí postup Úřadu byl potvrzen. Jedna ze stížností nebyla podána v souladu se zákonem č. 500/2004 Sb., správní řád, a proto se jí nadřízený orgán nezabýval. Další stížnost podal žadatel, který nesouhlasil s výší sdělené úhrady, předseda Úřadu výši sdělené úhrady potvrdil. Poslední stížnost, ve které žadatel tvrdil, že mu nebyla poskytnuta úplná informace, byla shledána předsedou Úřadu nedůvodnou a předchozí postup Úřadu byl potvrzen.

V roce 2023 neeviduje Úřad v případech, kdy byl povinným subjektem, podání žádné žaloby ve věci přezkoumání zákonnosti rozhodnutí povinného subjektu o odmítnutí žádosti o poskytnutí informace.

ŽÁDOSTI PODLE ZÁKONA O SVOBODNÉM PŘÍSTUPU K INFORMACÍM V LETECH 2020–2023*

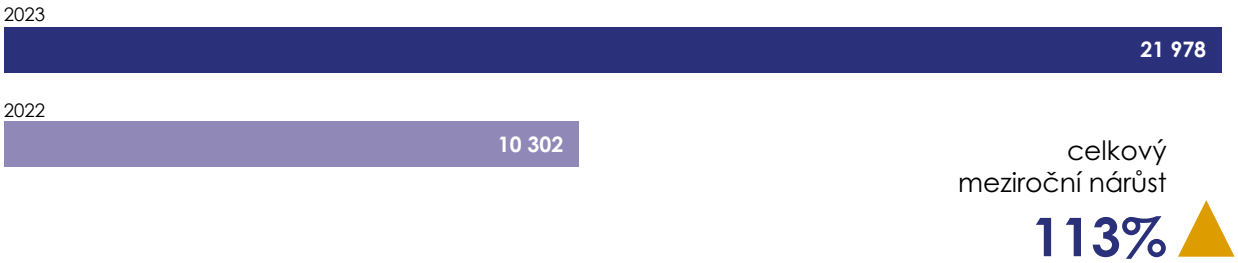


* Nejsou zahrnuty ty případy, ve kterých došlo k odložení žádosti v souladu se zákonem č. 106/1999 Sb.

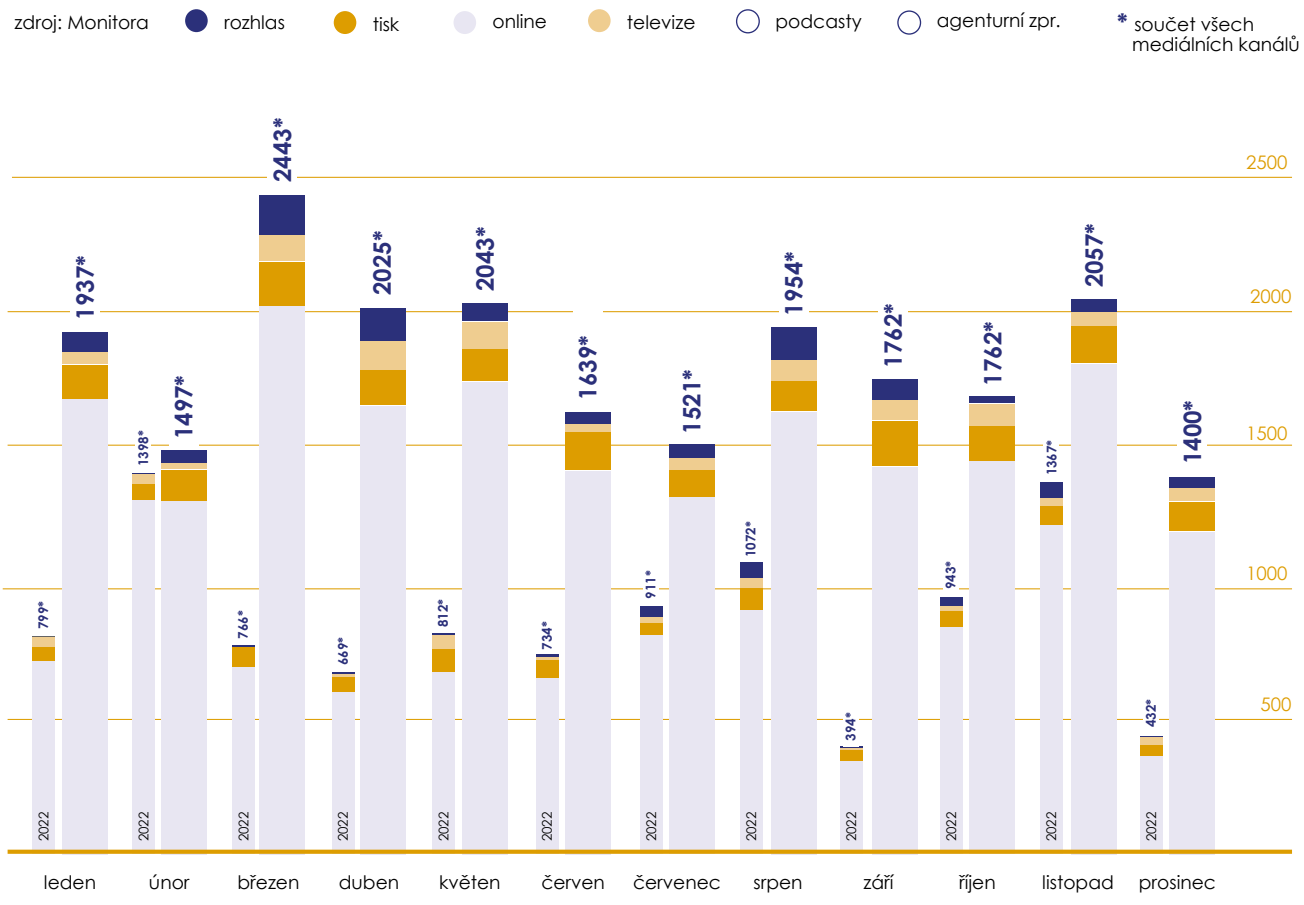
MEDIÁLNÍ KOMUNIKACE

Komunikační podpora Úřadu pro ochranu osobních údajů byla v roce 2023 cílena jak na širokou, tak i na odbornou veřejnost. V oblasti mediální komunikace došlo k výraznému posílení mediálního zásahu pro téma ochrany osobních údajů, a to v celkovém hodnocení (+) 113procentních bodů. Stejně tak tomu bylo i v případě významného zvýšení četnosti Úřadem mediálně publikovaných informací.

OCHRANA OSOBNÍCH ÚDAJŮ – MEDIÁLNÍ ZÁSAH OCHRANA OSOBNÍCH ÚDAJŮ – MĚSÍČNÍ NÁRŮST MEDIÁLNÍHO ZÁSAHU (GRP) V ROCE 2023 OPROTI ROKU 2022 (GRP) CELKEM 2022 A 2023



OCHRANA OSOBNÍCH ÚDAJŮ – SROVNÁNÍ MEDIÁLNÍHO ZÁSAHU (GRP) V LETECH 2022 A 2023



Hlavními tématy v oblasti mediální komunikace Úřadu pro ochranu osobních údajů byla témata, která navazovala na činnost a rozhodování partnerských dozorových úřadů, vlastní témata Úřadu pro ochranu osobních údajů a také témata, která reflektovala společenské dění a mediální zájem v České republice.

Mediálně nejvýznamnější témata, která byla ÚOOÚ komunikována ve vazbě na činnost partnerských dozorových autorit sdružených v evropském Sboru pro ochranu osobních údajů, patří rozhodnutí italského dozorového úřadu o zákazu provozu aplikace Chat GPT a sociální platformy TikTok na území Itálie nebo vysoká pokuta pro společnost META Ireland za behaviorální reklamu a předávání a zpracovávání údajů uživatelů platforem Facebook a Instagram.

Z hlediska mediálního zájmu byla během roku 2023 Úřadem nejčastěji komunikována témata (kromě už zmíněných), která vykazovala vysokou míru mediální atraktivity. V této souvislosti je nezbytné zmínit témata, která měla přímou vazbu na zpracování a ochranu osobních údajů a soukromí. Těmito tématy byly zejména Virtuální náborové středisko AČR, aplikace Karanténa a pokuta udělená ÚOOÚ Ministerstvu vnitra[35] ve výši 975 000 Kč, plošné zveřejnění osobních údajů majitelů datových schránek na internetu, únik osobních údajů uživatelů služby SIPO České pošty a v neposlední řadě biometrické kamerové systémy a jejich používání, například v souvislosti s provozem informačního systému Policie ČR Digitální podoba osob.

Celý rok 2023 se pak média velmi aktivně zajímala např. o případ bývalého poslance, a to jak ve vztahu k jeho údajnému vyzrazení totožnosti některých klíčových svědků, tak následně i ve vazbě na přímý přenos soudního přelíčení na TV Nova, kde byly zveřejněny osobní údaje účastníků řízení. Zájem byl také o rozhodnutí Úřadu ve věci podnětu bývalého prezidenta ČR Miloše Zemana na neoprávněné nakládání s osobními údaji ze strany ÚVN Praha, dále pak o rozhodnutí ÚOOÚ v případě publikovaného videozáznamu MP Praha z incidentu s moderátorem České televize.

V oblasti prezentace Úřad pro ochranu osobních údajů v roce 2023 pokračoval v implementaci nového jednotného vizuálního stylu, realizoval kompletní redesign struktury, obsahu a vizuálního stylu svých internetových stránek (u české jazykové mutace), a to včetně převedení na novou státní doménu gov.cz. Úřad také v rámci své osvětové a vzdělávací role pořádal odborné tematické semináře. Ty byly určeny zejména pro pověřence pro ochranu osobních údajů. Publikována byla také řada informačních osvětových materiálů určených jak pro odbornou, tak i pro širokou veřejnost.

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 2023 obdržel celkem 15 nových podání podle § 175 správního řádu, a to 13 stížností a dvě žádosti o přešetření vyřízení stížnosti. V naprosté většině 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.

Ve stejném období Úřad vyřídil celkem 13 podání podle § 175 správního řádu, a to 11 stížností a dvě žádosti o přešetření vyřízení stížnosti. Z tohoto počtu byly tři stížnosti vyhodnoceny jako důvodné nebo částečně důvodné a osm nedůvodných. Obě žádosti o přešetření byly vyhodnoceny jako nedůvodné. Typickým opatřením v případě důvodné stížnosti je podle povahy věci v takových případech následné nové posouzení původního podnětu a uplatnění dozorových postupů. Zbývajícími dvěma stížnostmi z roku 2023 se bude Úřad zabývat v roce 2024.

35 Pokuta byla udělena Ministerstvu vnitra ČR, protože Policie ČR nemá právní subjektivitu

STATISTIKA STÍŽNOSTÍ PODLE § 175 SPRÁVNÍHO ŘÁDU V ROCE 2023

Nápad v roce 2023	**15**	
Z toho stížností podle § 175 odst. 1	13	
Z toho žádostí podle § 175 odst. 7	2	
Nevyřízené z roku 2022	0	
Z toho stížností podle § 175 odst. 1	0	
Z toho žádostí podle § 175 odst. 7	0	
Vyřízení v roce 2023	13	
Z toho stížností podle § 175 odst. 1	11	
Z toho žádostí podle § 175 odst. 7	2	
Podle druhu	§ 175 odst. 1	§ 175 odst. 7
Stížnost na chování	1	0
Stížnost na postup	10	2
Podle způsobu vyřízení	§ 175 odst. 1	§ 175 odst. 7
Stížnost nedůvodná	8	2
Stížnost částečně důvodná	2	0
Stížnost důvodná	1	0
Nevyřízeno	2	
Z toho stížností podle § 175 odst. 1	2	
Z toho žádostí podle § 175 odst. 7	0	

V jednom případě směřoval podnět, který Úřad obdržel od stěžovatele, proti údajnému nevhodnému chování úřední osoby, ve zbytku proti postupu úřední osoby.

Výrazný pokles počtu evidovaných stížností byl v roce 2023 způsoben akceptací výkladu, že v řízeních podle zákona o svobodném přístupu k informacím se ustanovení § 175 správního řádu neuplatní, neboť to vylučuje § 20 odst. 4 zákona o svobodném přístupu k informacím, v němž zjevně absentuje odkaz na uvedené procesní ustanovení, naopak je obsažen pokyn zákonodárce „v ostatním se správní řád nepoužije“. Podání takto označená tedy Úřad vyhodnocuje podle jejich obsahu a jejich věcné vyřízení podřizuje aplikovatelnému právnímu rámci. Zároveň do výkazu nejsou zahrnovány stížnosti, které nesplňovaly náležitosti podání podle § 37 právního řádu. Z výše uvedených důvodů tak do statistiky není započteno dalších celkem 24 věcí *stížnostního* charakteru, v nichž se fyzické a právnické osoby obracely na Úřad, a tento reagoval zpravidla jiným druhem sdělení. ●

Organizační, technické a finanční zajištění činnosti 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. lednu 2023 byl celkový počet systemizovaných služebních a pracovních míst v Úřadu 113, přičemž k 31. prosinci 2023 byl počet systemizovaných míst o jedno systemizované místo vyšší v důsledku zániku systemizovaného místa inspektora k 1. srpnu 2023 a vytvoření dvou systemizovaných míst náhradou za rušené místo. K 31. prosince 2023 byl tedy celkový počet systemizovaných míst 114.

I v roce 2023 plynule pokračoval chod jednotlivých procesů personální správy Úřadu, a to v návaznosti na vývoj legislativy v oblasti státní služby a pracovněprávních vztahů. V této souvislosti byla významná převážně novela zákoníku práce účinná od 1. října 2023, která přinesla v důsledku transpozice evropské legislativy nové administrativní povinnosti související s výkonem personální práce, zejména v oblasti dohod o pracích konaných mimo pracovní poměr.

Do služebního poměru bylo v roce 2023 nově přijato 14 státních zaměstnanců a 15 státních zaměstnanců služební poměr ukončilo nebo došlo k jejich zařazení do jiného služebního úřadu. Do pracovního poměru pak bylo přijato šest zaměstnanců, přičemž osm zaměstnanců pracovní poměr ukončilo.

V rámci Úřadem zajišťované zvláštní části úřednické zkoušky pro obor služby „Ochrana osobních údajů“ absolvovalo tuto zkoušku celkem 10 žadatelů, přičemž 10 žadatelů složilo zkoušku úspěšně v prvním řádném termínu.

K 1. lednu 2023 bylo v Úřadu v evidenčním stavu 105 zaměstnanců, k 31. prosinci 2023 byl pak jejich počet 106.

Průměrný přepočtený evidenční počet zaměstnanců za rok 2023 činil 103,66.

Dalších 50 osob vykonávalo v Úřadu činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr, přičemž 20 externích spolupracovníků vykonávalo činnosti spojené s rozhodováním rozkladové komise, sedm externích spolupracovníků zajišťovalo úklid objektu Úřadu a zbylý počet s Úřadem spolupraco-

val 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 41–60 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 tří čtvrtin funkčních míst v Úřadu, na zbývající čtvrtinu je předpokládáno dosažení úplného středoškolského vzdělání.

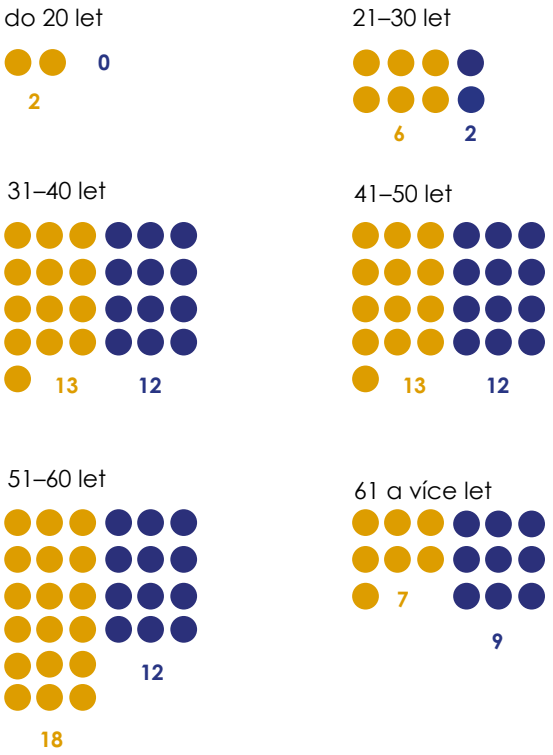
Úřad umožňuje a zabezpečuje odborný rozvoj svých zaměstnanců. Zajišťuje jim prohlubování odborné kvalifikace a v případě potřeby i její zvýšení. Studentům vysokých škol Úřad poskytuje možnost absolvovat odbornou praxi. Tímto způsobem tak podporuje jejich zájem o problematiku ochrany osobních údajů a zároveň tak vyhledává nové potenciální zaměstnance.

ČLENĚNÍ ZAMĚSTNANCŮ ÚŘADU PODLE VZDĚLÁNÍ A POHLAVÍ
stav k 31. prosinci 2023

Celý soubor	Muži	Ženy	Celkem
Základní	0	0	0
Střední odborné +VL	1	0	1
Střední odborné	0	0	0
Úplné střední všeobecné	1	4	5
Úplné střední odborné + VL	1	2	3
Úplné střední odborné	3	12	15
Vyšší odborné vzdělání	0	0	0
Vysokoškolské – bakalářské	1	3	4
Vysokoškolské – magisterské a vyšší	40	38	78
Celkem	**47**	**59**	**106**

ČLENĚNÍ ZAMĚSTNANCŮ ÚŘADU PODLE VĚKU A POHLAVÍ
stav k 31. prosinci 2023

celkem
59 ŽEN
47 MUŽŮ



Identifikované personální potřeby Úřadu

Úřad v průběhu roku 2023 identifikoval a v rámci různých fází procesů přípravy státního rozpočtu na rok 2024, střednědobého výhledu na léta 2025–2026 a systemizace opakovaně uplatňoval níže uvedené potřeby formou požadavků, které však nebyly ze strany Ministerstva financí pro rok 2024 zohledněny. Z hlediska významu těchto potřeb bude nezbytnost jejich zabezpečení nabývat v průběhu času stále vyšší intenzity, neboť přestože bude Úřad i v roce 2024 hospodařit se stejným počtem systemizovaných míst jako v roce 2023, objem finančních prostředků na platy bude o 2% zkrácený. V této souvislosti bude i možnost odměnit stávající zaměstnance za plnění úkolů ve vztahu k personálně nezabezpečeným agendám velmi omezená.

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Rozšíření působnosti Úřadu o agendy zákona o svobodném přístupu k informacím bylo nezbytné reflektovat rovněž v rovině personálního zabezpečení tak, aby bylo zajištěno plnění této

nové působnosti v zákonných mezích. Agenda svobodného přístupu k informacím byla svěřena Úřadu paradoxně v době, kdy výrazně vzrostla zátěž v souvislosti s účinností obecného nařízení o ochraně osobních údajů, což by samo o sobě odůvodňovalo personální posílení. Úřad je jednak nadřízeným orgánem mnoha set povinných subjektů (rozhodování o odvoláních a o stížnostech na postup těchto povinných subjektů při vyřizování žádostí o informace), jednak přezkumným orgánem pro cca 15 000 povinných subjektů. Množství podřízených povinných subjektů se navíc oproti původním předpokladům průběžně rozšiřuje na základě judikatury správních soudů. Zde lze zmínit například rozsudek Nejvyššího správního soudu č. j. Komp 3/2021-26 ze dne 16. února 2022, v jehož důsledku narostl počet podřízených povinných subjektů o dalších zhruba 1000.

Odbor práva na informace se v roce 2023 podobně jako v roce předchozím potýkal s potížemi způsobenými jeho nedostatečným personálním zajištěním. V odboru práva na informace je systemizováno 10 míst státních zaměstnanců, z čehož pouze pět míst bylo pro tuto agendu nově vytvořeno za účelem výkonu působnosti v oblasti svobodného přístupu k informacím. Zbylých pět míst bylo bez náhrady vyčleněno z jiných útvarů Úřadu. To zjevně neodpovídá potřebné kapacitě de facto ústředního orgánu, který rozhoduje ve třech funkčních stupních správního řízení, nemluvě o právní analytické a metodické činnosti a přípravě závěrů Úřadu k publikaci. Úřad rovněž vystupoval či vystupuje v desítkách soudních řízení, do nichž většinou nastoupil bez vlastního přičinění namísto původního žalovaného toliko v důsledku změny zákona. Na služební místa v odboru práva na informace jsou současně kladeny vysoké odborné nároky, což je společně se značným pracovním vytížením jednotlivých zaměstnanců vyplývajícím z neustále narůstajícího nápadu vyřizovaných věcí a jejich zvyšující se komplexnosti důvodem nesnadného obsazování uvolněných míst.

Pro úplnost lze doplnit, že Petiční výbor Poslanecké sněmovny Parlamentu ČR doporučil již v roce 2020 svým usnesením č. 175/2020 zřídit tři místa pro rozhodování podle zákona o svobodném přístupu k informacím. Zřízení systemizovaných míst v tomto rozsahu nicméně dosud realizováno nebylo. Doposud bylo ve vztahu k agendě zákona o svobodném přístupu k informacím zohledněno pouze navýšení o jedno nové systemizované služební místo od 1. srpna 2023, jehož finanční krytí jde na vrub části zůstatku rušeného místa inspektora ochrany osobních údajů k 31. červenci 2023.

S ohledem na vývoj v průběžném vyřizování agend se jeví jako nezbytné, aby došlo ke zřízení dalšího systemizovaného služebního místa v návaznosti na výše uvedenou soudem přiznanou působnost Úřadu podle zákona o svobodném přístupu k informacím v oddělení právním, odboru právního a koordinačního, které připravuje podklady pro rozhodnutí předsedy Úřadu o rozkladech. V blízké době lze rozumně očekávat značný nárůst právě rozkladů, jejichž vyřízení bude připravovat oddělení právní. K tomu nutno dále přičíst narůstající činnost Evropského sboru pro ochranu osobních údajů, zejména v oblasti rozhodování sporných právních aplikačních otázek podle čl. 65 obecného nařízení, na čemž se Úřad podílí.

Hlava IV. zákona o zpracování osobních údajů

Za účelem obnovení výkonu dozorových pravomocí Úřadu a k naplnění všech závazků, které pro Českou republiku vyplývají z ratifikace Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108 (dále jen „Úmluva č. 108“) vyhlášené pod č. 115/2001 Sb. m. s. včetně dodatku,[36] který ČR ratifikovala 24. září 2003 ve vztahu ke zpracování osobních údajů spadajících pod hlavu IV zákona č. 110/2019 Sb., o zpracování osobních údajů, požaduje Úřad zřízení dvou nových systemizovaných míst.

Ustanovení hlavy IV zákona č. 110/2019 Sb. se použijí při zpracování osobních údajů k zajišťování obranných a bezpečnostních zájmů České republiky, pokud jiný právní předpis nestanoví jinak. Jedná se tedy o zpracování osobních údajů, na které se nevztahuje obecné na-

36 Česká republika přijala závazek zřídit dozorový orgán podle dodatkového protokolu k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice.

řízení o ochraně osobních údajů[37] (upraveno v hlavě II zákona č. 110/2019 Sb.) ani trestně právní směrnice[38] (upraveno v hlavě III zákona č. 110/2019 Sb.).

Okruh správců, jejichž činnost spadá pod hlavu IV zákona č. 110/2019 Sb.:

a) Národní bezpečnostní úřad,
b) Národní úřad pro kybernetickou a informační bezpečnost,
c) ostatní úřady, pokud zpracovávají osobní údaje v rámci národní bezpečnosti (obrany státu), včetně řešení krizových situací za nouzového nebo jiného krizového stavu (do této kategorie spadá předmětný návrh zákona),
d) ostatní úřady, pokud zpracovávají osobní údaje v rámci společné zahraniční a bezpečnostní politiky Evropské unie.

Při ratifikaci Úmluvy č. 108 bylo v souladu s čl. 13 této úmluvy učiněno oznámení České republiky, že pověřeným úřadem je Úřad pro ochranu osobních údajů. Podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, plnil Úřad působnost spadající i pod Úmluvu č. 108.

Od přijetí zákona č. 110/2019 Sb., o zpracování osobních údajů, tedy od 24. dubna 2019 však zákonodárcem byla zvolena konstrukce působnosti Úřadu vymezená v § 54 zákona, ve kterém však není explicitně zmíněna působnost Úřadu ve vztahu ke zpracování osobních údajů spadající pod hlavu IV zákona č. 110/2019 Sb., což je však v rozporu se závazky, které pro Českou republiky vyplývají z ratifikace Úmluvy č. 108.

Potřeba explicitního obnovení dozorových pravomocí Úřadu plyne tedy primárně z konstrukce § 54 zákona č. 110/2019 Sb., která mj. zdůrazňuje vyprázdněnost působnosti Úřadu k naplnění všech závazků, které pro Českou republiku vyplývají z ratifikace Úmluvy č. 108. Dá se tedy říci, že Úřad má dozorovou pravomoc vyplývající z mezinárodního práva i v tomto případě, pouze podle vnitrostátního práva nemá organizační a hmotněprávní normu, která by umožňovala ji řádně naplnit, proto byla navržena změna zákona č. 110/2019 Sb.[39], která sice nyní společně s návrhem zákona, kterým se mění některé zákony v oblasti obrany, předložena nebude, což však nic nemění na nutnosti plnění mezinárodních závazků České republiky.

Zákonem, kterým se mění některé zákony v oblasti obrany,[40] se totiž podstatně rozšiřuje zpracovávání osobních údajů v hlavě IV a tím i potřeba dozoru, přičemž současně je potřeba nadále plnit veškeré další úkoly, které Úřadu byly svěřeny. Je tedy nezbytné vytvoření dvou služebních míst zařazených ve 13. platové třídě podle nařízení vlády č. 304/2014 Sb., o platových poměrech státních zaměstnanců. Výkon státní služby na těchto služebních místech se bude zabývat primárně agendou podle hlavy IV zákona č. 110/2019 Sb.

Zřízení těchto dvou služebních míst bylo předmětem jednání mezi Úřadem, Ministerstvem obrany a Ministerstvem financí v rámci připomínkového řízení k předmětnému návrhu zákona již v prosinci 2022.

Nové evropské systémy

Od roku 2024 se předpokládá postupné spuštění čtyř nových evropských systémů. Konkrétně se jedná o Entry/Exit System (EES), Evropský systém pro cestovní informace a povolení (ETIAS), Evropský informační systém rejstříků trestů – státní příslušníci třetích zemí (ECRIS-TCN) a dále tzv. rámec pro interoperabilitu mezi informačními systémy EU v oblasti hranic a víz (dále jen „Interoperabilita“). V případě všech těchto systémů vždy příslušná evropská právní norma ukládá

37 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.

38 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

39 V § 54 zákona č. 110/2019 Sb., o zpracování osobních údajů, se za odstavec 2 vkládá nový odstavec 3, který zní: „(3) Zpracování osobních údajů podle hlavy IV tohoto zákona, s výjimkou zpravodajských služeb, dozoruje Úřad.“ Dosavadní odstavce 3 a 4 se označují jako odstavce 4 a 5.

40 Zákon byl vyhlášen 23. 6. 2023 ve Sbírce zákonů v částce 89 pod číslem 178/2023 Sb., kterým se mění některé zákony v oblasti obrany.

národním dozorovým orgánům nové povinnosti, a to zejména výkon nezávislého dohledu nad zákonností zpracování osobních údajů, přičemž je stanovena povinnost periodických kontrol prováděných minimálně jednou za tři roky v případě EES, ETIAS a ECRIS TCN a jednou za čtyři roky v případě Interoperability. Nadto vzniknou dozorovým úřadům ve vztahu ke všem systémům další povinnosti, a to vyřizování stížností subjektů údajů, pravidelné provádění informačních kampaní spolu s Evropským inspektorem ochrany údajů (EDPS) a Evropskou komisí, pomoc a poradenství subjektům údajů při uplatňování jejich práv, povinnost pravidelného zveřejňování statistických dat a aktivní spolupráce s EDPS a dozorovými úřady jiných členských států, včetně pravidelných setkání nejméně dvakrát ročně. V rámci (všech) nařízení (EU), kterými jsou výše uvedené systémy zaváděny, je stanovena povinnost členských států zajistit, aby jejich dozorový úřad měl dostatek zdrojů k plnění úkolů, které členským státům dané nařízení ukládá.

Národní Schengenský implementační plán 2021, který slouží k naplňování cílů Koncepce schengenské spolupráce 2021-2027, též stanovil úkol 5/1 „V souvislosti se spuštěním nových informačních systémů zajistit dostatečné personální kapacity ÚOOÚ“ s indikátorem plnění „personální posílení příslušného pracoviště ÚOOÚ.“ U tohoto úkolu bylo uveden termín dokončení 2023 s tím, že jako způsob financování bylo stanoveno: „Náklady opatření budou řešeny z rozpočtových prostředků odpovědných a spolupracujících subjektů.“ V rámci připomínek Schengenského implementačního plánu 2023 byla navržena změna pro tento úkol, přičemž bylo navrženo, aby indikátor plnění zněl: „vytvoření 3 nových systemizovaných služebních míst v rámci příslušného pracoviště ÚOOÚ“ a způsob financování: „navýšení rozpočtu ÚOOÚ.“

DGA

Věcný záměr zákona o správě dat veřejného sektoru spadá do oblasti veřejnoprávní regulace a má za cíl postihnout dvě oblasti, jejichž absence úpravy se dlouhodobě ukazuje jako problematická. Jsou jimi principy správy dat veřejného sektoru a úprava regulace řízeného přístupu k datům veřejného sektoru a jejich opětovné užití. Obecně předpokládané hospodářské dopady budou spočívat zejména v nutných nákladech, kterými jsou:

- náklady nutné na provádění datových auditů – půjde zejména o náklady vynaložené na přijetí nových, případně vyškolení stávajících pracovníků orgánů veřejné správy tak, aby odborně tuto činnost mohli zastat, případně náklady na zaplacení služeb externího dodavatele, který audity provede,
- náklady nutné na zřízení infrastruktury, která umožní řízený přístup k datům,
- náklady nutné na vytvoření centrálního informačního místa, ať už v podobě zřízení nové instituce, nebo rozšíření kompetencí některé ze stávajících institucí.

Z dlouhodobého náhledu je možné očekávat celkovou úsporu na provozu ISVS a dalších registrů provozovaných při výkonu veřejné správy, protože systematický přístup k datům a jejich uspořádání umožní efektivnější výkon veřejné správy.

V souvislosti s projednáváním návrhu věcného záměru zákona o správě dat veřejného sektoru byl Úřadem do návrhu usnesení vlády, kterým se schvaluje uvedený návrh věcného záměru, vložen požadavek na schválení „rozšíření počtu systemizovaných míst na Úřadu o tři místa z důvodů zajištění efektivního výkonu dozoru a vymáhání povinností vyplývajících z rámce ochrany osobních údajů při aplikaci řízeného přístupu.“ Současně byl do návrhu usnesení vlády vložen úkol pro ministra vnitra „předložit před nabytím účinnosti zákona o správě dat veřejného sektoru podle bodu III tohoto usnesení změnu systemizace Úřadu pro ochranu osobních údajů podle bodu II tohoto usnesení a ministru financí navýšit objem prostředků na platy a příslušenství formou navýšení celkových výdajů kapitoly 343 – Úřad pro ochranu osobních údajů.“ Přestože uvedené předkladatel, tedy Ministerstvo vnitra akceptovalo, ve schváleném usnesení vlády č. 576 ze dne 16. srpna 2023 se tento požadavek neobjevil. To však nic nemění na potřebnosti zřízení těchto nových systemizovaných míst.

DSA

Podle čl. 13 odst. 1 nařízení (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (dále jen DGA) určí členské státy jeden či více orgánů příslušných pro plnění úkolů souvisejících s postupem pro oznamování týkajícím se služeb zprostředkování dat. Podle čl. 23 odst. 1 DGA určí členské státy jeden či více příslušných orgánů odpovědných za veřejný vnitrostátní rejstřík uznaných organizací pro datový altruismus. Podle čl. 49 odst. 1 nařízení (EU) 2022/2065 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (dále jen „DSA") mají členské státy určit jeden či více příslušných orgánů, které odpovídají za dohled nad poskytovateli zprostředkovatelských služeb a za vymáhání tohoto nařízení. Čl. 50 a 51 DSA dále specifikují požadavky a pravomoci příslušných orgánů. Podle čl. 50 odst. 1 DSA mají členské státy mj. zajistit, aby jejich koordinátoři digitálních služeb (tj. hlavní dozorové orgány) měli pro plnění svých úkolů k dispozici veškeré nezbytné zdroje, včetně dostatečných technických, finančních a lidských zdrojů, a mohli tak náležitě dohlížet na všechny poskytovatele zprostředkovatelských služeb spadajících do jejich pravomoci.

Návrh zákona o digitální ekonomice a změně některých souvisejících zákonů (dále jen „návrh zákona") určuje jako příslušné orgány podle čl. 49 odst. 1 DSA Český telekomunikační úřad a Úřad pro ochranu osobních údajů. K návrhu zákona probíhalo od 10. října do 7. listopadu 2023 mezirezortní připomínkové řízení a v současné době probíhá vypořádání obdržených připomínek.

Návrh zákona zavádí dvě zcela nové unijní agendy (DSA a DGA) a obnovuje jednu stávající (šíření obchodních sdělení). K tomu, aby mohl ÚOOÚ řádně plnit dozor nad zpracováním osobních údajů a současně nadále plnit veškeré další úkoly, které mu byly svěřeny, je nezbytné k zabezpečení agend DSA vytvoření nových systemizovaných služebních míst.

Shrnutí identifikovaných personálních potřeb

Celkově se jedná ve smyslu shora uvedeného o identifikaci potřeby vzniku nových 12 systemizovaných služebních míst.

K zabezpečení identifikovaných potřeb je nutné navýšit objem prostředků na platy na RP 5013 v celoročním vyjádření o 7 443 216 Kč s trvalým vlivem.

V rámci úpravy rozpočtu kapitoly bude nezbytné v této souvislosti zajistit i související příslušenství, které činí v celoročním vyjádření:

- navýšení sociálního pojištění za zaměstnavatele na RP 5031: 1 845 918 Kč,
- navýšení zdravotního pojištění za zaměstnavatele na RP 5032: 669 890 Kč,
- navýšení přídělu do FKSP na RP 5342: 74 433 Kč,
- příslušenství celkem: 2 590 241 Kč.

Celkem se tedy jedná o legitimní potřebu navýšení výdajů rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů o 10 033 457 Kč, a to s trvalým vlivem.

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ ÚŘADU

Úřad pro ochranu osobních údajů 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. Pověřenec Úřadu především poskytuje informace a poradenství zaměstnancům, kteří se na zpracování osobních údajů podílejí, a zodpovídá dotazy subjektů údajů, jejichž osobní údaje zpracovává sám Úřad.

V roce 2023 v činnosti pověřence převažovala konzultační činnost uvnitř Úřadu spojená především s problematikou aktualizace záznamů o činnostech zpracování, cookies souborech a kamerového systému se záznamem. 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 osobních údajů. V roce 2023 se jednalo o posouzení žádostí o přístup k dokumentu „Twitter Assesment", který vypracovala síť pověřenců v roce 2020.

HOSPODAŘENÍ ÚŘADU

Odbor provozně ekonomický v oblasti hospodaření Úřadu zodpovídá za řízení jeho rozpočtu jako samostatné kapitoly státního rozpočtu, tj. sestavuje rozpočet a sleduje jeho čerpání. Nedílnou součástí řízení rozpočtu je i spravování investičních programů Úřadu.

Schválený rozpočet na rok 2023

ROZPOČET ÚŘADU BYL SCHVÁLEN ZÁKONEM Č. 449/2022 SB., O STÁTNÍM ROZPOČTU ČESKÉ REPUBLIKY NA ROK 2023

Ukazatele kapitoly 343 – Úřad pro ochranu osobních údajů

Souhrnné ukazatele	v Kč
Příjmy celkem	1 000 000
Výdaje celkem	189 695 700
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	1 000 000
v tom: příjmy z rozpočtu Evropské unie bez společné zemědělské politiky celkem	0
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	1 000 000
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	189 695 700
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	74 850 575
Povinné pojistné placené zaměstnavatelem*)	25 299 495
Základní příděl fondu kulturních a sociálních potřeb	1 459 193
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	11 479 825
Platy zaměstnanců na služebních místech dle zákona o státní službě	54 169 938
Platy zaměstnanců v pracovním poměru odvozované od platů ústavních činitelů	7 309 900
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	13 479 488

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

Čerpání rozpočtu v roce 2023

Příjmy

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částkou 10 457,39 tis. Kč

Jednalo se především o:

- sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti,
- sankce uložené podle zákona č. 101/2000 Sb., o ochraně osobních údajů, resp. podle zákona č. 110/2019 Sb., o zpracování osobních údajů, zákona o kontrole č. 255/2012 a dalších zákonů,
- náhrady nákladů řízení,
- vrácené přeplatky za energie z minulého roku.

Výdaje

Čerpání výdajů ve výši 173 747,90 tis. Kč zahrnuje:

- veškeré náklady na platy a související výdaje,
- kapitálové výdaje spojené s objektem Úřadu a obnovou informačních systémů, jak samotného Úřadu, tak i informačního systému ORG v systému základních registrů,
- další běžné výdaje spojené s chodem Úřadu, tj. zejména položky spojené s nákupem drobného hmotného majetku, materiálu, IT služeb, služeb spojených s provozem budovy a ostatních služeb, cestovného, vzdělávání a údržby,
- výdaje související s neinvestičními nákupy.

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 **100 910,91 tisíc Kč** je dáno kvalifikační strukturou a plněním plánu počtu pracovníků.

Stav k 31. prosinci 2023 byl **114 systemizovaných míst**.

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

V souladu se schválenou dokumentací programu 034V01„Rozvoj a obnova materiálně technické základny Úřadu pro ochranu osobních údajů od r. 2017“ a programu 343V02 „Rozvoj a obnova materiálně technické základny Úřadu pro ochranu osobních údajů od r. 2022“ bylo celkem vyčerpáno **10 876,36 tis. Kč.**

PŘEHLED ČERPÁNÍ ROZPOČTU V ROCE 2023

Položka	Název položky	Schválený rozpočet v Kč	Konečný rozpočet v Kč	Skutečnost v Kč
		190 695 700,00	194 887 375,78	184 205 287,53
Příjmy		1 000 000,00	0	10 457 386,98
1	Daňové příjmy			400,00
2	Nedaňové příjmy	1 000 000,00	0	10 453 517,94
3	Přijaté tranfery			3 469,04
Výdaje		189 695 700,00	194 887 375,78	173 747 900,55
5	Běžné výdaje	176 216 212,00	175 349 195,68	162 871 538,65
50	Plata a obdobné a související výdaje	100 150 070,00	99 048 557,24	98 033 044,00
501	Platy	72 959 663,00	71 866 351,00	71 853 651,00
5011	Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	11 479 825,00	10 372 885,00	10 372 885,00
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	54 169 938,00	54 182 989,00	54 182 989,00
5014	Platy zaměstnanců v pracovním poměru odvoz. od platů úst. Činitelů	7 309 900,00	7 310 477,00	7 297 777,00
502	Ostatní platby za provedenou práci	1 890 912,00	2 077 547,00	1 774 970,00
5021	Ostatní osobní výdaje	1 890 912,00	2 077 547,00	1 774 970,00
503	Povinné pojistné placené zaměstnavatelem	25 299 495,00	25 104 659,24	24 404 423,00
5031	Povin. pojist. na sociál. zabezp.	18 562 943,00	18 449 709,37	17 837 223,00
5032	Povin. pojist. na veřej. zdravotní pojištění	6 736 552,00	6 654 949,87	6 567 200,00
51	Výdaje na neinv. nákupy a souvis. výdaje	73 881 949,00	74 209 058,64	62 768 126,49
513	Výdaje na nákup materiálu	1 967 000,00	2 075 851,00	1 049 754,95
514	Úroky a ostatní finanční výdaje	10 000,00	45 371,96	38 922,88
515	Výdaje na nákup vody, paliv a energie	5 542 979,00	4 699 448,16	2 369 862,27
516	Výdaje na nákup služeb	59 678 970,00	60 935 577,52	55 893 199,14
517	Výdaje na ostatní nákupy	3 903 000,00	3 832 500,00	1 678 150,25
518	Výdaje na netransferové převody uvnitř rozpočtové jednotky	0,00	0,00	0,00
519	Výdaje související s neinv. nákupy, příspěvky, náhrady a věcné dary	2 780 000,00	2 620 310,00	1 738 237,00
53	Neinv. transfery veřejnoprávním osobám a platby daní	1 484 193,00	1 476 183,80	1 454 972,16
534	Neinv. převody vlastním fondům a ve vztahu k útvarům bez plné právní subjektivity	1 459 193,00	1 451 183,80	1 449 092,16
5342	Základní příděl fondu kulturních a sociálních potřeb	1 459 193,00	1 451 183,80	1 449 092,16
536	Ostatní neinv. transfery jiným veřejným rozpočtům, platby daní a další povinné platby	25 000,00	25 000,00	5 880,00
54	Neinv. transfery a některé náhrady fyz. osobám	700 000,00	615 396,00	615 396,00
6	Kapitálové výdaje	13 479 488,00	19 538 180,10	10 876 361,90
61	Investiční nákupy a související výdaje	13 479 488,00	19 538 180,10	10 876 361,90
611	Pořízení dlouhodobého nehmot. majetku	0,00	2 017 070,00	1 578 203,00
6111	Programové vybavení	0,00	2 017 070,00	1 578 203,00
612	Pořízení dlouhodobého hmot. majetku	13 479 488,00	17 521 110,10	9 298 158,90
6121	Stavby	3 000 000,00	5 818 500,00	283 140,00
6122	Stroje, přístroje a zařízení	0,00	421 080,00	197 714,00
6125	Informační a komunikační technologie	10 479 488,00	11 281 530,10	8 817 304,90

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. prosince 2023.

ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2023 a informace o jejím předání proběhne v řádném termínu do 31. července 2024 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 sdělením Ministerstva financí k aplikaci některých ustanovení zákona č. 221/2015 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, a v návaznosti na zákon č. 110/2019 Sb., o zpracování osobních údajů, nemá Úřad povinnost schvalovat účetní závěrku auditorem.

ZPRÁVA INTERNÍHO AUDITORA

Služební místo interního auditora bylo v roce 2023 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:

- 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 2023

- 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 2023 vycházela především ze střednědobého plánu auditů, z výsledků předchozích auditů a z požadavků vedoucích zaměstnanců Úřadu, přičemž byla zaměřena i na konzultační činnost v souvislosti s veřejnosprávní kontrolou ze strany Ministerstva financí, která v Úřadu proběhla v roce 2022. Následně v roce 2023 probíhala daňová kontrola vedená Finančním úřadem pro Kraj Vysočina a zahájená v prosinci 2022, při které Úřad poskytoval součinnost.

Provedená kontrola Ministerstvem financí, jejímž předmětem bylo hospodaření Úřadu s veřejnými prostředky v letech 2020–2021, se zabývala celou řadou oblastí od ekonomicko-provozních činností včetně realizace veřejných zakázek přes oblast účetnictví až po personální správu. V protokolu o výsledku veřejnosprávní kontroly Ministerstvo financí konstatovalo určité nedostatky vnitřního kontrolního systému Úřadu, které však, jak Úřad dokládal 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 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 zamezující 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 2024. ●

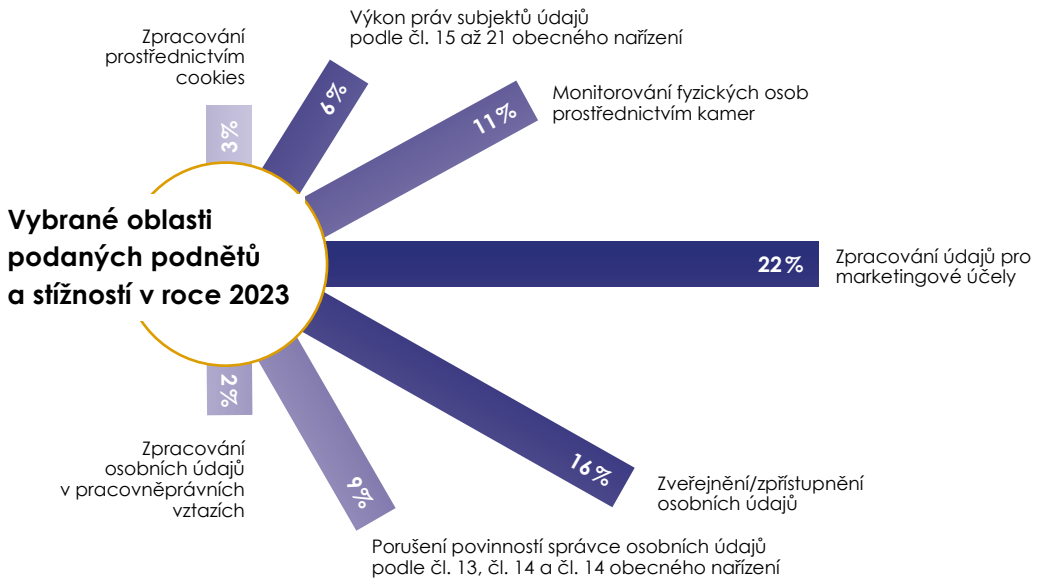
Úřad v číslech

Počet stížností a podnětů

	2020	2021	2022	2023
Celkový počet přijatých podnětů a stížností	**1855**	**2430**	**2192**	**2322**
z toho stížností	1697	1720	1528	1373
z toho podnětů	158	710	664	949
Doplnění stížností/podnětů	neevidováno	827	714	571
Vyřízeno odpovědí podateli	**1278**	**1774**	**1264**	**1582**
Vyřízeno upozorněním správce na možné porušení obecného nařízení	452	491	785	936
Reakce správců na upozornění	neevidováno	neevidováno	550	232
Předáno ke kontrole nebo jinému řízení	125	165	141	165
Poskytnutí součinnosti policii/ žádost OČTŘ o součinnost	14	25	23	11

OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ PODLE ČL. 33 GDPR (DATA BREACH)

	2020	2021	2022	2023
Počet ohlášení porušení zabezpečení osobních údajů	**292**	**294**	**313**	**383**
Doplnění ohlášení porušení zabezpečení osobních údajů	neevidováno	94	151	265



Dozorová činnost Úřadu

DOZOROVÁ ČINNOST V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ

Počet zahájených kontrol	35
Počet ukončených kontrol	25
Počet vydaných protokolů o kontrole	27
Počet kontrolních protokolů napadených námitkami	9
Počet pravomocně uložených nápravných opatření	9
Počet uložených pravomocných trestů	23
Součet výše uložených pravomocných pokut za porušení předpisů na ochranu osobních údajů	3 653 000 Kč
Počet pravomocně uložených trestů za nesoučinnost podle kontrolního řádu	3
Vyřízeno jinak (tj. předně odloženo podle § 76 zákona č. 250/2016 Sb., podle § 65 zákona č. 110/2019 Sb., podle § 43 správního řádu)	25

Počet obdržených námitek proti kontrolním zjištěním v rámci kontrolních protokolů		9
Počet vyřízených námitek (včetně z předchozího období)		12
z toho vyhověno	0	
z toho vráceno k došetření	2	
z toho částečně vyhověno	4	
z toho nedůvodné	6	
Zvolen postup podle § 14 odst. 3 kontrolního řádu		1

DOZOROVÁ ČINNOST V OBLASTI OBCHODNÍCH SDĚLENÍ

Upozorňující dopisy jednotlivým subjektům		359
Zahájených kontrol		13
Ukončených kontrol		15*
Napadeno námitkami		3
z toho vyhověno	0	
z toho vráceno k došetření	0	
z toho částečně vyhověno	0	
z toho nedůvodné	3	
Pokuty za neposkytnutí součinnosti v kontrole		2
Řízení o sankci		29
Celková výše pravomocně uložených sankcí		8 623 000 Kč

*z toho 7 z předchozích let

Rozhodovací činnost Úřadu

ROZHODOVACÍ ČINNOST ÚŘADU V OBLASTI SVOBODNÉHO PŘÍSTUPU K INFORMACÍM

Nadřízený orgán (§ 20 odst. 5 InfZ)	
1) odvolání	
– informační příkaz	17
– v části vydán informační příkaz, v části rozhodnutí povinného subjektu zrušeno a věc vrácena k novému projednání	3
– rozhodnutí povinného subjektu potvrzeno	38
– rozhodnutí povinného subjektu zrušeno, věc vrácena k novému projednání	119
– rozhodnutí povinného subjektu částečně potvrzeno, v části rozhodnutí povinného subjektu zrušeno a věc vrácena k novému projednání	8
– ostatní způsoby vyřízení	4
2) stížnost na postup povinného subjektu	
– informační příkaz	1
– postup potvrzen	38
– příkaz povinnému subjektu vyřídit žádost	39
– v části postup potvrzen, v části příkaz povinnému subjektu vyřídit žádost	8
– výše úhrady požadované povinným subjektem snížena	12
– ostatní způsoby vyřízení	3
3) opravný prostředek postoupen jinému subjektu z důvodu nepříslušnosti Úřadu	45
Přezkum (§ 16b odst. 1 a 2 InfZ)	
– přezkumné řízení nezahájeno	78
– rozhodnutí nadřízeného orgánu zrušeno, věc vrácena	9
– rozhodnutí nadřízeného orgánu zrušeno pro nicotnost	2
Ochrana před nečinností § 16b odst. 3 InfZ)	
– nedůvodný podnět	94
– opatření proti nečinnosti	69

Rozhodování předsedy Úřadu

SPRÁVNÍ ŘÍZENÍ

Podané rozklady proti rozhodnutím Úřadu	8
Vyřízené rozklady	5*
– rozklad zamítnut	4
– rozhodnutí změněno	1
– rozhodnutí zrušeno	0

*z toho 2 z předchozích let

SOUDNÍ PŘEZKUM ROZHODNUTÍ (PŘEDSEDY) ÚŘADU

Městský soud v Praze:	
podané žaloby	4
žaloba se zamítá	2
rozhodnutí se ruší a věc se vrací	1
Nejvyšší správní soud:	
podané kasační stížnosti	1
kasační stížnost se zamítá	1

Celkem podaných žalob od roku 2001	176
z toho ukončených soudních řízení	170
neukončených soudních řízení	6

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

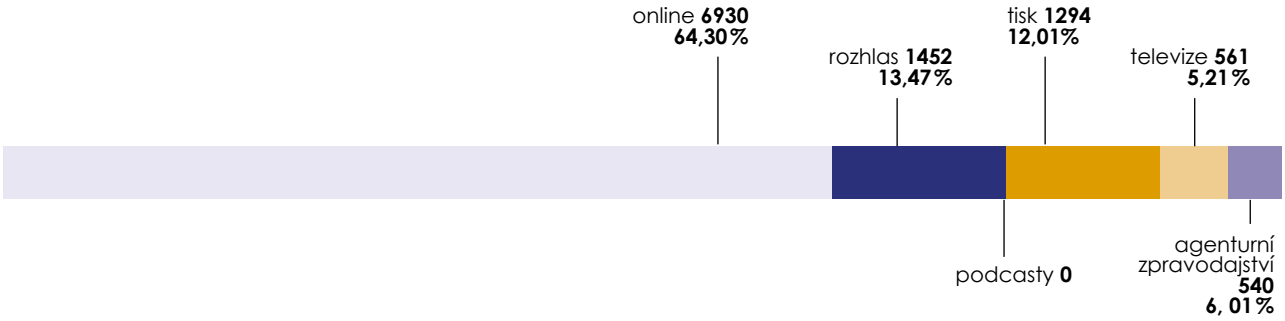
ŽÁDOSTI PODLE ZÁKONA Č. 106/1999 SB. V ROCE 2023

Počet podaných žádostí o informace	145
informace poskytnuty	118
počet vydaných rozhodnutí o odmítnutí žádosti (částečně či zcela odmítnuto)	22
počet odložených žádostí	4
počet podaných rozkladů proti rozhodnutí	3
počet stížností podaných podle § 16a	**7**
požadavek na úhradu nákladů za mimořádně rozsáhlé vyhledávání informací	**2**
uhrazené náklady za mimořádné vyhledávání informací	**2**

Mediální komunikace

MEDIATYP 2023

celkový počet článků



zdroj: Mediaboard

Seznam použitých zkratek

Afs	Řízení o kasační stížnosti ve finanční věci
AIFO	Agendový identifikátor fyzické osoby
AIS	Agendové informační systémy
BCR	Binding Corporate Rules (Závazná vnitropodniková pravidla)
BSI	Bezvýznamový směrový identifikátor
CEF	Coordinated Enforcement Framework (Společná dozorová akce EDPB)
CEH	EDPB Compliance, E-government and Health Expert Subgroup (Podskupina EDPB pro dodržování předpisů, elektronickou veřejnou správu a zdravotnictví)
CIS	Celní informační systém
CSA	Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu
ČR	Česká republika
ČÚZK	Český úřad zeměměřický a katastrální
DGA	European Data Governance Act (Evropský akt o správě dat)
DPIA	Posouzení vlivu na ochranu osobních údajů
DPPR	Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679
DSA	Digital Service Act (Akt o digitálních službách)
EDPB / Sbor	European Data Protection Board (Evropský sbor pro ochranu osobních údajů)
EDPS	European Data Protection Supervisor (Evropský inspektor ochrany údajů)
EHP	Evropský hospodářský prostor
ePD	ePrivacy Directive – nařízení 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)
EU	Evropská unie

EURODAC	European Asylum Dactyloscopy Database (Evropská databáze pro srovnání otisků prstů žadatelů o azyl a některých kategorií ilegálních přistěhovalců)
GPA	Global Privacy Assembly (Světové shromáždění pro ochranu soukromí)
GDPR / obecné nařízení / / Nařízení (EU) 2016/679	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)
IS ORG	Informační systém ORG (Informační systém pro převod identifikátorů)
ISZR	Informační systém základních registrů
KIFO	Klientský identifikátor fyzické osoby
Nařízení EU o ochraně spotřebitelů	Nařízení Evropského parlamentu a Rady (EU) 2017/2394 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování právních předpisů na ochranu zájmů spotřebitelů a o zrušení nařízení (ES) č. 2006/2004
Nařízení (EU) č. 603/2013	Nařízení Evropského parlamentu a Rady (EU) č. 603/2013 ze dne 26. června 2013 o zřízení systému „Eurodac" pro porovnávání otisků prstů za účelem účinného uplatňování nařízení (EU) č. 604/2013, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států, a pro podávání žádostí orgánů pro vymáhání práva členských států a Europolu o porovnání údajů s údaji systému Eurodac pro účely vymáhání práva a o změně nařízení (EU) č. 1077/2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (přepracované znění)
NSS	Nejvyšší správní soud
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OP	Občanský průkaz
Pl.	Plénum
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)
sp. zn.	Spisová značka

Trestněprávní směrnice	Směrnice Evropského parlamentu a Rady (EU) č. 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady č. 2008/977/SVV
ÚOOÚ / Úřad	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud
VIS	Vízový informační systém
Vízový kodex	Nařízení Evropského parlamentu a Rady (ES) č. 810/2009 ze dne 13. července 2009 o kodexu Společenství o vízech
ZIFO	Zdrojový identifikátor fyzické osoby
ZR	Základní registry

Seznam odkazovaných zákonů

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
Zákon č. 99/1963 Sb., občanský soudní řád
Zákon č. 553/1991 Sb., o obecní policii
Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)
Zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů
Zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů
Zákon č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů
Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole)
Zákon č. 150/2002 Sb., soudní řád správní
Zákon č. 235/2004 Sb., o dani z přidané hodnoty
Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)
Zákon č. 500/2004 Sb., správní řád
Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
Zákon č. 262/2006 Sb., zákoník práce
Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
Zákon č. 273/2008 Sb., o Policii České republiky
Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
Zákon č. 111/2009 Sb., o základních registrech
Zákon č. 100/2010 Sb., kterým se mění zákon č. 111/2009 Sb., o základních registrech
Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)
Zákon č. 67/2013 Sb., kterým se upravují některé otázky související s poskytováním plnění spojených s užíváním bytů a nebytových prostorů v domě s byty
Zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon)
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
Zákon č. 234/2014 Sb., o státní službě
Zákon č. 110/2019 Sb., o zpracování osobních údajů
Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci
Zákon č. 269/2021 Sb., o občanských průkazech
Zákon č. 283/2021 Sb., stavební zákon
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
Zákon č. 241/2022 Sb., kterým se mění zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů, a zákon č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu, experimentálního vývoje a inovací), ve znění pozdějších předpisů
Zákon č. 424/2022 Sb., kterým se mění zákon č. 67/2013 Sb., kterým se upravují některé otázky související s poskytováním plnění spojených s užíváním bytů a nebytových prostorů v domě s byty, ve znění pozdějších předpisů
Zákon č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony
Zákon č. 171/2023 Sb., o ochraně oznamovatelů
Zákon č. 430/2023 Sb., kterým se mění zákon č. 269/2021 Sb., o občanských průkazech, ve znění zákona č. 471/2022 Sb., a zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů
Vyhláška č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění zákona č. 309/2002 Sb., zákona č. 320/2002 Sb. a zákona č. 123/2003 Sb.
Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci

Úřad pro ochranu osobních údajů

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2023
Úřad pro ochranu osobních údajů
Pplk. Sochora 27, 170 00 Praha 7
E-mail: posta@uoou.gov.cz
Internetová adresa: uoou.gov.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 Batková
Stylistická a jazyková korektura: Mgr. Lenka Brabencová, Aneta Vaňková
Tisk: Expresta

Úřad pro ochranu
osobních údajů