SENÁT

PARLAMENTU ČESKÉ REPUBLIKY

15. funkční období

75

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2024

2025

Výroční zpráva
2024

Úřad pro ochranu
osobních údajů

Slovo předsedy

Vážené dámy, vážení pánové,

v úvodu výroční zprávy Úřadu pro ochranu osobních údajů za rok 2024 se s Vámi chci podělit o klíčové události, které formovaly naši činnost v uplynulém roce. Výroční zpráva, kterou máte před sebou, je přehledem usilovné práce, výsledků a výzev, jimž jsme čelili v rámci zajištění ochrany osobních údajů nejen v České republice.

Mgr. Jiří Kaucký
předseda Úřadu pro ochranu osobních údajů

Rok 2024 byl pro Úřad významným obdobím. Pokračovali jsme v plnění tradičních úkolů v oblasti ochrany osobních údajů, ochrany soukromí obecně a v oblasti svobodného přístupu k informacím. Také jsme však čelili novým výzvám, způsobeným rychlým až překotným technologickým pokrokem, změnami v národní a zejména evropské legislativě a dynamickým, leckdy překvapivým vývojem judikatury. Svou roli hrálo také rostoucí povědomí veřejnosti o otázkách ochrany osobních údajů a s tím související pozornost, kterou lidé ochraně svého soukromí stále více věnují.

Právě zpětná vazba ze strany veřejnosti nás utvrzuje v přesvědčení, že ochrana osobních údajů, která vede k partnerské spolupráci i ke střetům dozorového úřadu s veřejnou mocí a správci osobních údajů, má stále větší význam. Je třeba nepolevovat, výkon činnosti v oblasti ochrany osobních údajů nadále prohlubovat a rozšiřovat co do rozsahu i kvality.

Ochrana soukromí v digitálním věku

Ochrana osobních údajů je v dnešní době víc než jen právní otázkou: stala se klíčovým tématem moderní společnosti, v níž neustále přibývají nové oblasti digitálního zpracování dat (zejména v posledních letech masivně nasazované prvky umělé inteligence), což logicky vyžaduje vyšší míru regulace digitální ekonomiky. Strmě rostoucí množství osobních údajů, shromažďované a zpracovávané v různých sektorech, vyžaduje nejen sofistikovanou legislativní reakci, ale rovněž dokonce předvídání dalšího vývoje. Samozřejmostí je přitom aktivní a zodpovědný přístup všech správců a zpracovatelů, kteří s osobními údaji nakládají.

Kromě zvyšování objemu zpracovávaných osobních údajů vyvolaného používáním nových technologií nelze pominout ani skutečnost, že na jedné straně neustále vzrůstá zájem o osobní data uživatelů internetu a datových služeb s cílem zpeněžení těchto údajů či pří-

mo za účelem jejich zneužití, na straně druhé si uživatelé digitálních služeb stále více uvědomují, že jejich osobní údaje jsou využívány a často i zneužívány, a dle možností uplatňují jejich ochranu (například odmítáním marketingových cookies sloužících k sledování a profilování potenciálních klientů za účelem cílené reklamy), což pak zejména odborníky na reklamu vede k hledání nových způsobů přístupu k datům uživatelů; lze zmínit např. zavádění *cookie wall* a *consent or pay* modelů znemožňujících přístup na webovou stránku, pokud klient neumožní zpracování osobních údajů za účelem behaviorální reklamy, nebo pokud za vstup na stránku nezaplatí.

Potřeba Úřadu držet krok s vývojem společnosti a nastolit preventivní přístup je zvláště významná. V současném globalizovaném digitálním prostředí totiž bude v případě úniku či zneužití osobních údajů velmi obtížné, nebo dokonce nemožné je dohledat a zabránit jejich dalšímu zneužívání, a to se všemi negativními důsledky pro subjekty těchto údajů. Uložení pokuty viníka sice odradí od případného dalšího protiprávního jednání, potenciální škody vzniklé únikem dat však neeliminuje. To samé platí u nápravných opatření, jejichž účinek je přirozeně nejsilnější, jsou-li uložena co nejdříve, tedy při včasném zachycení systémových nedostatků a ještě předtím, než se tyto nedostatky projeví právě únikem či zneužitím osobních údajů.

Preventivní zaměření Úřadu je přínosem nejen pro subjekty osobních údajů, ale i pro jejich správce a zpracovatele. Dynamicky se rozvíjející digitální ekonomika potřebuje přiměřenou míru předvídatelnosti vývoje státní regulace, nikoliv „mlčení“ po čase následované stanovením pravidel cestou legislativy či dokonce aplikační praxe se zásadními dopady na již zavedené (a často finančně nákladné) postupy a technologie. Tomuto efektu se zřejmě nepodaří zcela se vyhnout, je však třeba zdůraznit, že se nejedná o projev svévole veřejné moci. Může jít o objektivně novou oblast činnosti, resp. o zcela novou technologii, kterou lze efektivně regulovat, až když poznání nových vztahů a zákonitostí a jejich reálných dopadů do soukromí osob dosáhne úrovně potřebné pro tvorbu smysluplných pravidel. Může nastat i případ, kdy takové poznání sice v rámci světa existuje, avšak není sdíleno se státními orgány ČR, které tak nemohou včas reagovat. Bohužel však může jít i o případy, kdy státní orgány nemají vybudovanou dostatečnou personální nebo technickou kapacitu, aby na vývoj digitální ekonomiky mohly adekvátně reagovat v reálném čase. Potřeba reflektovat neustále se zvyšující nároky v oblasti ochrany osobních údajů zabezpečením potřebné personální a odborné kapacity Úřadu se jeví jako naprosto nezbytná nejen pro výkon dozoru, ale i pro prevenci a odborný dialog, které jsou jeho nedílnou součástí.

Nyní stojíme před novým a významným milníkem. Evropský zákonodárce již přijal řadu zásadních evropských aktů, které budou následně implementovány do českého právního řádu a uvedeny do praxe. Jedná se například o akt o digitálních službách, akt o datech, akt o správě dat, akt o digitálních trzích či akt o umělé inteligenci. Bude nezbytná úzká spolupráce státní správy s představiteli průmyslu a obchodu, rozličnými odbornými asociacemi, neziskovým sektorem a občany. Evropská komise tyto akty předložila a prosadila s cílem, aby digitální transformace sledovala prospěch všech. Pro úspěch tohoto záměru je klíčové, aby byl fakticky a právně uskutečnitelný a aby uložené povinnosti byly splnitelné a vymahatelné. S vymahatelností je nutně spojena dostatečná kapacita orgánů státní správy, jinak právo jako takové, a v tomto případě i základní lidské právo na soukromí a ochranu osobních údajů, pozbude své autority.

Procesní stránka ochrany osobních údajů

Nezanedbatelným prvkem v oblasti uplatňování ochrany osobních údajů je nastavení procesních pravidel dozorových úřadů. V současné době je připravován legislativní návrh nařízení o procesních pravidlech při prosazování GDPR [*Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679*], jenž však dosud zůstával spíše stranou mediálního zájmu. Úřad tomuto návrhu již delší dobu věnuje zvýšenou pozornost, protože jeho přijetí si pravděpodobně vyžádá významnou revizi procesních postupů Úřadu spojenou s odpovídajícími legislativními kroky v rámci České republiky. Připravované nařízení má upravovat podrobné postupy dozorových úřadů při řešení přeshraničních případů. Aktuálně návrh nařízení na přelomu roku vstoupil do tzv. trialogů a nutno uvést, že mezi Radou EU a Evropským parlamentem je patrné principiálně odlišné uchopení zásad správního řízení.

Je jisté, že česká pravidla pro řízení před Úřadem budou muset projít podstatnou novelizací týkající se nejen přeshraničních, ale i vnitrostátních řízení. Budoucí nařízení, ve snaze navýšit standard procesních práv subjektů údajů domáhajících se zásahu dozorových orgánů v případech přeshraničního zpracování osobních údajů (typicky v případech, kdy se zpracování osobních údajů dotýká subjektů údajů z více zemí EU), totiž zatíží proces řadou nových administrativních kroků, které dosud nebyly jeho součástí. Doplnění procesních postupů o nové prvky vyžadované připravovaným nařízením tak správní řízení před Úřadem administrativně výrazně zatíží. Ostatně procesní nároky plynoucí ze samotného GDPR postupně zvyšuje i judikatura Soudního dvora EU. Zkomplikování správního procesu tak nesměřuje k faktickému posílení práv subjektů údajů, ale absurdně spíše ke zhoršení jejich situace, protože bez dostatečných personálních, technických a administrativních kapacit Úřad nebude schopen poskytnout ochranu práv subjektům údajů v reálném čase. Navíc již nyní je Úřad pod náporem četných podání individuálních stěžovatelů s často omezeným obecným přesahem pod tlakem judikatorní činnosti správních soudů nucen věnovat velkou část kapacit v podstatě administrativní činnosti, spočívající ve vyřizování dalších a dalších procesních úkonů.

V případě zavedení všech procesních postupů tak, jak jsou aktuálně v návrhu nařízení koncipovány (a jejich následného nezbytného promítnutí i do správního řízení týkajícího se vnitrostátních zpracování), hrozí mnohonásobně vyšší administrativní zátěž v nově zahajovaných správních řízeních. Pokud by ke schválení procesního nařízení došlo bez zásadní změny vnitrostátní právní úpravy a bez významného zvýšení personální kapacity Úřadu, tedy bez institucionálního a organizačního zajištění implementace nařízení, Úřad by byl vzápětí zcela paralyzován množstvím formálních procesních úkonů a nemohl by poskytovat ochranu práv subjektům údajů dostatečně operativně. Zamýšlené posílení práv subjektů osobních údajů by tak zůstalo jen „na papíře“.

Význam prevence a kontrolní činnosti

Jednou z hlavních oblastí činnosti Úřadu v roce 2024 byla prevence porušování právních předpisů o ochraně osobních údajů a posílení kontrolních mechanismů Úřadu. Věnovali jsme se kontrolám veřejného a soukromého sektoru i monitorování nových technologických trendů, které mohou mít dopad na ochranu osobních údajů. Provedli jsme řadu významných kroků, které v důsledku příznivě ovlivnily praxi v oblasti ochrany dat. Zejména lze uvést vydání pravomocného rozhodnutí ve věci společnosti Avast Software s.r.o., které jsme uložili za neoprávněné zpracování osobních údajů uživatelů

jejího antivirového programu Avast a jeho rozšíření internetových prohlížečů (Browser Extensions) pokutu 351 miliónů korun.

Úřad se intenzivně zabýval též jednáním společností, které lidem rozesílají vystavené faktury vyzývající k zaplacení údajně objednaných služeb prostřednictvím e-mailových zpráv. Proti těmto společnostem Úřad důrazně zakročil v rámci svých pravomocí a uložil pokuty za více než 5 milionů korun.

Významným aktuálním tématem na poli ochrany osobních údajů je trend online platforem uplatňovat ve vztahu ke svým uživatelům model získávání souhlasu se zpracováním osobních údajů, zvaný *consent or pay*. Uživateli konkrétních webových stránek je znemožněna interakce s nimi, pokud nepřistoupí k udělení souhlasu se zpracováním osobních údajů (typicky za účelem cílené či behaviorální reklamy, k čemuž jsou využity například údaje o prohlížení webu a IP adresa uživatele), či k zaplacení poplatku. Z pohledu GDPR vyvstává předně otázka, zda je takový souhlas se zpracováním osobních údajů svobodný a zda je dostatečně informovaný. Uživatel totiž musí mít k dispozici informace o tom, jak bude s jeho údaji nakládáno, a to v dostatečně srozumitelné a detailní podobě. Při posuzování tohoto modelu Úřad vycházel i ze stanoviska EDPB, podle něhož osobní údaje nelze považovat za obchodovatelné komodity. Velké online platformy by měly mít na paměti, že je třeba zabránit tomu, aby se základní právo na ochranu údajů přeměnilo na prvek, který musí subjekty údajů zaplatit, s tím, že ve většině případů nebude možné, aby velké online platformy splňovaly požadavky na platný souhlas, pokud konfrontují uživatele pouze s binární volbou mezi udělením souhlasu se zpracováním osobních údajů pro účely behaviorální reklamy a zaplacením poplatku, bez možnosti dalších alternativ volby.

Intenzivně jsme začali řešit také případné nadužívání osobních údajů ze státních registrů soukromým sektorem, především ze základního registru obyvatel, do kterého mají přístup v zákonem stanoveném rozsahu například banky či pojišťovny. Této oblasti budeme i nadále věnovat zvýšenou pozornost.

Vzdělávání a osvěta

Ve velké míře jsme se věnovali vzdělávání a osvětě v oblasti ochrany osobních údajů a v oblasti svobodného přístupu k informacím. Kultivace obecného povědomí o těchto tématech je totiž klíčovou podmínkou pro nalezení rovnováhy mezi nezpochybnitelným právem veřejnosti na informace a účinnou ochranou soukromí. Proto v rámci našich pravidelných aktivit pokračujeme v pořádání seminářů nejen pro pověřence, jejichž cílem je posílit povědomí odborné i laické veřejnosti o právech jednotlivců a povinnostech organizací při zpracování osobních údajů i při poskytování informací podle zákona o svobodném přístupu k informacím. I v tomto roce bylo možné se těchto seminářů zúčastnit nejen prezenčně, ale i formou vzdáleného přístupu, takže jsme byli schopni uspokojit všechny zájemce o účast na seminářích, jichž bylo v průměru kolem 450 na jeden seminář, přičemž nejvyšší zájem vyvolal seminář prezentující naši metodiku ke kamerovým systémům, který sledovalo 613 účastníků.

K šíření povědomí o GDPR nadále provozujeme stálou GDPR informační linku pro veřejnost. Se správci údajů řešíme jejich problémy formou písemné i ústní konzultace. Současně vydáváme metodiky, metodické pokyny, informační letáky a doporučení, které pomáhají odborné i laické veřejnosti správně interpretovat a aplikovat právní normy.

Prosazování práva na informace

V oblasti práva na informace dochází k neustálému rozšiřování okruhu povinných subjektů, a to jak v důsledku změn zákona o svobodném přístupu k informacím, tak s ohledem na stále se zpřesňující výklad tohoto zákona představovaný judikaturou správních soudů. Tento vývoj současně Úřad staví před zcela nové výzvy, kterých je nucen se chopit s využitím stávajících ne zcela dostatečných personálních kapacit a v rámci nejednoznačně určených kompetencí. Mnohé povinné subjekty také aktivně hájí, na rozdíl od správních orgánů v tradičním slova smyslu, svá veřejná subjektivní práva před soudy, což dále zvyšuje nároky kladené na zaměstnance Úřadu, kteří se problematice svobodného přístupu k informacím věnují. Zvyšující se počet soudních řízení v této oblasti je rovněž důsledkem faktu, že Úřad ve své rozhodovací praxi řeší dosud nezodpovězené právní otázky, což přirozeně vybízí k jejich následnému podrobení soudnímu přezkumu. Zmíněný vývoj na druhé straně představuje potvrzení role Úřadu při kultivaci a prosazování práva na informace v České republice, k nimž v posledních letech dochází.

Pohled do budoucnosti

Výhled do roku 2025 a dalších nejbližších let ukazuje, že význam práva na ochranu soukromí má stále stoupající tendenci. Je totiž čím dál víc zřejmé, že ochrana tohoto základního lidského práva se musí vyvíjet souběžně s vývojem digitálních technologií, aby technologický pokrok ve spojení s jeho masovým využíváním nebyl vykoupen absolutní ztrátou soukromí uživatelů. Úřad pro ochranu osobních údajů je připraven pokračovat v plnění svého poslání a reagovat na aktuální potřeby a problémy. Také v nadcházejících letech se zaměříme na to, abychom zůstali inovativní, proaktivní a vysoce profesionální institucí, která bude nadále důsledně chránit práva jednotlivců a všemožně podporovat zodpovědné nakládání s osobními údaji.

Závěrem chci vyjádřit poděkování všem zaměstnancům a spolupracovníkům Úřadu za jejich vysoké pracovní nasazení, odbornost a každodenní úsilí, které vynakládají při plnění našich úkolů. Děkuji také všem ostatním, kteří se na ochraně osobních údajů nejrůznějším způsobem podílejí. Společně budujeme prostředí, v němž je ochrana soukromí základem důvěry a bezpečnosti v digitálním světě.

Vážené dámy a pánové, ve výroční zprávě Úřadu pro ochranu osobních údajů za rok 2024 najdete podrobné informace o naší činnosti v oblasti ochrany osobních údajů, realizace práva na informace a plnění dalších zákonných povinností. Věřím, že vám zpráva poskytne cenné poznatky a přispěje k hlubšímu pochopení významu ochrany osobních údajů a soukromí jednotlivce.

S úctou,

Mgr. Jiří Kaucký,

předseda Úřadu pro ochranu osobních údajů

Obsah

I. Ochrana osobních údajů (GDPR)

V oblasti ochrany osobních údajů zastává Úřad pro ochranu osobních údajů (ÚOOÚ) roli dozorového ústředního správního úřadu. Jak samotné obecné nařízení o ochraně osobních údajů (GDPR), tak české národní právo skýtá Úřadu širokou škálu nástrojů, které využívá při své činnosti. Tyto nástroje či pravomoci jsou podle své povahy **vyšetřovací** (čl. 58 odst. 1 GDPR) a **nápravné** (čl. 58 odst. 2 GDPR). Vyšetřovací pravomoci jsou užívány ke zjištění skutkového stavu věci, nápravné pravomoci jsou aplikovány v případech porušení ochrany osobních údajů za účelem dosažení stavu souladného s GDPR.

K vyšetřovacím nástrojům náleží zejména pravomoc provádět audity (v českém právním řádu se jedná o výkon kontroly dle kontrolního řádu) či pravomoc nařídit správci a zpracovateli poskytnutí potřebných informací. Mezi pravomoci nápravné patří pravomoc nařídit správci či zpracovateli uvést operace zpracování do souladu s GDPR, pravomoc uložit správní pokutu nebo napomenutí či pravomoc uložit dočasné omezení zpracování osobních údajů (v kontextu českého právního řádu se jedná o vydání předběžného opatření). Co se týče praktického uplatnění některé z pravomocí, kterými Úřad disponuje, je zcela na jeho rozhodnutí, který z nástrojů vyhodnotí jako nejvhodnější.

Dozor nad zpracováním osobních údajů je prováděn jednak na základě stížností subjektů údajů, jednak na základě vlastních poznatků Úřadu. Každá stížnost je Úřadem ve vhodné míře šetřena [čl. 57 odst. 1 písm. f) GDPR]. Stížnost na zpracování osobních údajů však musí splňovat jisté náležitosti. Předně musí subjekt údajů tvrdit, že jsou konkrétním způsobem dotčena jeho práva ve smyslu GDPR. Jedná se většinou o situace, kdy si subjekt údajů stěžuje na neoprávněnost zpracování osobních údajů správcem, na nedostatečné informování správce o zpracování osobních údajů či na nedostatečnou reakci správce na žádost o přístup k osobním údajům subjektu. Ze stížnosti musí být zároveň patrné, že ji činí dotčený subjekt údajů, proto stížnost musí naplňovat definici podání dle § 37 správního řádu.

Pokud stížnost tyto náležitosti neobsahuje, Úřad ji považuje za podnět. Podnětem je sdělení podatele poukazující na konkrétní zpracování osobních údajů, jež není v souladu s GDPR, aniž by však takovým zpracováním byla dotčena jeho práva z GDPR vyplývající. Důsledkem toho podatel nemá postavení stěžovatele ve smyslu čl. 77 GDPR.

Úřadu jsou postupovány rovněž stížnosti týkající se tzv. přeshraničního zpracování osobních údajů (čl. 4 bod 23 GDPR). Jedná se o případy, kdy se subjekt údajů nacházející se v jiném členském státě EU cítí dotčen na svých právech zaručených GDPR zpracováním osobních údajů prováděným správcem, jenž má hlavní provozovnu na území ČR. Stížnosti týkající se přeshraničního zpracování osobních údajů jsou pak předávány příslušnému zahraničnímu dozorovému úřadu. Většinou se jedná o globální technologické společnosti provozující sociální sítě zpravidla se sídlem v Irsku.

Konkrétně Úřad na základě obdržených stížností inicioval celkem 11 procedur podle čl. 56 GDPR, tedy navrhl příslušnost některého ze zahraničních dozorových úřadů, aby se věcí zabýval z pozice vedoucího dozorového úřadu. Naopak Úřad byl do této role navržen celkem v 15 případech a ve všech úlohu vedoucího dozorového úřadu přijal.

K řešení stížností mnohdy postačuje dopis Úřadu správci [v režimu čl. 58 odst. 1 písm. d) či čl. 58 odst. 2 písm. a) GDPR], jímž je upozorněn na případný problém. Správce pak často sám zjedná nápravu, čímž je předmět stížnosti vyřešen.

Z vlastní iniciativy Úřad zahajuje šetření v návaznosti na kontrolní plán, na základě vlastního monitoringu veřejného prostoru či v důsledku obdržených podnětů. Kontrolní plán je roční a Úřad zveřejňuje jeho rámcové zaměření.

I.1. KONTROLNÍ ČINNOST

Kontrolní činnost vykonává Úřad dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád). Smyslem kontroly je zjištění skutkového stavu věci, přičemž prakticky se jedná o zjištění, jak probíhá předmětné zpracování osobních údajů, jaká jsou jeho organizační a technická nastavení a jaké je zabezpečení osobních údajů. Ke kontrole Úřad přistupuje v případech, kdy existuje podezření na rozsáhlé systémové pochybení.

Výsledkem kontroly je kontrolní protokol, který zachycuje zjištěný stav věci s uvedením nedostatků a označením porušených právních předpisů (kontrolní zjištění). Kontrolní protokol není rozhodnutím a nelze jím uložit žádnou povinnost kontrolované osobě spočívající například v uložení nápravného opatření nebo sankce, to lze učinit pouze ve správním řízení.

Kontrolní plán Úřadu na rok 2024 byl zaměřen na využívání dat z registru obyvatel orgány veřejné moci, nahrávání telefonických hovorů, zpracování osobních údajů v informačních systémech v rámci Schengenského prostoru, zpracování osobních údajů Policií ČR a rozesílání nevyžádaných obchodních sdělení. Spolu s dalšími evropskými dozorovými úřady se Úřad zapojil do koordinované dozorové akce (*Coordinated Enforcement Framework 2024*), sledující implementaci práva na přístup ze strany správců osobních údajů. Ke konci roku 2024 nebyly všechny kontrolní akce dokončeny, a to i s ohledem na to, že byly zahajovány v průběhu celého roku. O výsledcích těchto akcí bude Úřad informovat.

Digitální podoba osob

Úřad v roce 2024 provedl kontrolu Policie ČR ohledně zpracování osobních údajů v souvislosti s využíváním informačního systému Digitálních podob osob (IS DPO). Tento systém je Policií ČR využíván v rámci trestního řízení ke ztotožnění neznámých osob na základě digitálních fotografií.

Kontrolou bylo zjištěno, že IS DPO pracuje na základě *facial recognition,* technologie automatického rozpoznávání tváří. IS DPO porovnává vektorové zobrazení obličeje z fotografie zájmové osoby s vektorovými zobrazeními obličejů z fotografií v referenční databázi. Referenční databázi tvoří fotografie z informačních systémů evidence občanských průkazů a evidence cestovních dokladů a k nim přiřazené jedinečné identifikátory.

Možnost získat a dále zpracovávat digitální fotografie a agendové identifikátory z uvedených databází a využívat je pro identifikaci konkrétní osoby za obecně formulovanými účely souvisejícími s trestnou činností či zajišťováním veřejného pořádku a bezpečnosti ČR vyplývá z § 66a zákona č. 273/2008 Sb. ve spojení s ustanovením § 79 odst. 1 téhož zákona.

Digitální fotografie obličeje zpracovávaná zvláštními technickými prostředky, které umožňují identifikaci osoby, představuje biometrický údaj. V IS DPO tak dochází ke zpracování zvláštní kategorie osobních údajů. Právní základ pro povolení zpracování zvláštních kategorií údajů by měl být podle čl. 10 písm. a) směrnice (EU) 2016/680 definován obecně závazným právním předpisem, ze kterého musí jasně a přesně vyplývat jeho účel, rozsah a podmínky, kdy může k takovému zpracování dojít. Zmíněný požadavek však úprava IS DPO v jediném ustanovení § 66a zákona č. 273/2008 Sb. (a v příloze rozkazu policejního prezidenta) nesplňuje.

Kontrolou bylo rovněž konstatováno, že Policie ČR nesplnila povinnost toto zpracování předem projednat s Úřadem (resp. podat Úřadu žádost o projednání připravovaného zpracování), jež jí vyplývá z § 38 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť vytvořila novou evidenci velkého rozsahu a s využitím nových technologií zpracovává mimo jiné biometrické údaje, což představuje vysoké riziko zásahu do práv a svobod subjektů údajů.

Docházkové systémy využívající biometrické osobní údaje

Úřad dokončil některé z kontrol zahájených v závěru roku 2023, jejichž předmětem byly zaměstnanecké docházkové systémy využívající otisky prstů. Otisky prstů jsou biometrické údaje v daném kontextu využívané k identifikaci, čímž na základě čl. 9 GDPR podléhají zvýšené ochraně. Ta spočívá zejména v tom, že GDPR obecně zakazuje zpracování osobních údajů vyjmenovaných v čl. 9 odst. 1 GDPR, přičemž v čl. 9 odst. 2 GDPR vypočítává výjimky, na jejichž základě lze takové údaje zpracovávat.

Z povahy věci je fungování docházkových systémů založeno na jedinečné identifikaci fyzické osoby (jedině tak může docházkový systém zaznamenávat příchody a odchody konkrétních pracovníků), a to na rozdíl od systémů umožňujících pouze vstup do určitých prostor bez další identifikace. V druhém případě se ve většině případů nebude jednat o zpracování biometrických údajů za účelem jedinečné identifikace.

V kontrolovaných případech zaměstnavatelé v pozici správců osobních údajů založili zpracování na základě souhlasu ve smyslu čl. 9 odst. 2 písm. a) GDPR. Navíc však umožňovali zaměstnancům jinou alternativu evidence docházky, konkrétně s využitím RFID čipu, jenž zároveň sloužil pro vstup.

Kontrola ÚOOÚ shledala, že zaměstnavatel porušil tzv. zásadu minimalizace údajů danou čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679, neboť v období od měsíce dubna roku 2022 do data vydání protokolu o kontrole zpracovával v elektronickém docházkovém systému *hashe* otisků prstů svých zaměstnanců v celkovém počtu nejméně 57 subjektů údajů, přestože tyto údaje nebyly nezbytné ve vztahu k účelu evidence docházky zaměstnanců.

Pochopitelně nelze vyloučit existenci zaměstnavatelů v pozici správců údajů, v jejichž případě bude užití docházkového systému zpracovávajícího biometrické údaje náležitě zdůvodnitelné. Je však zřejmé, že půjde o zcela výjimečné situace, které vždy budou muset zohlednit požadavky čl. 9 GDPR.

V této souvislosti Úřad zdůrazňuje, že zásadní nebezpečí týkající se biometrických údajů spočívá v jejich nezaměnitelnosti (jedná se o jedinečné fyzické znaky osob). Pokud tedy dojde jednou k úniku takovýchto údajů, jedná se o nevratný problém. Riziko úniku je pak

jen zvýšeno v situacích, kdy správce ke zpracování osobních údajů využívá zpracovatele a biometrické údaje jsou uloženy mimo dispozici správce.

Zneužití údajů z platebních karet

Během roku 2024 Úřad prověřoval porušení povinností spojených se zpracováním osobních údajů na platebních kartách. Toho se měla dopustit společnost zabývající se online objednávkami a doručováním jídla. Důvodem pro provedení kontroly bylo několik stížností na zneužití osobních údajů uvedených na platebních kartách, které měli stěžovatelé uložené v systému společnosti. Údaje zneužil útočník, který jejich prostřednictvím prováděl objednávky.

ÚOOÚ shledal, že společnost nejméně v období, kdy mělo dojít k incidentům, nedisponovala dostatečnými technickými a organizačními opatřeními pro zabezpečení osobních údajů uživatelů. Konkrétně po zadání správné kombinace přístupových údajů (e-mailové adresy a hesla, u něhož nebyly kladeny nároky na obtížnost, navíc bez dvoufaktorového ověření) bylo možné získat některé osobní údaje a objednávat potraviny. Zjištěné nedostatky Úřad vyhodnotil jako porušení čl. 32 odst. 1 GDPR.

Popsaný případ ilustruje vysokou důležitost spolehlivých technických opatření ve vztahu ke klientům, která mohou zabránit zneužití osobních údajů, ale i majetkové škodě.

Zpracování údajů z rozesílaných SMS

Úřad se zabýval porušením povinností při zpracování osobních údajů klientů v souvislosti s rozesíláním SMS mobilním operátorem. Operátor považoval za nezbytné zasílat klientům informace o vystaveném vyúčtování a proběhlých platbách několika způsoby, a to na osobní účet zákazníka na webových stránkách, adresným e-mailem či v listinné podobě poštou. Současně toto informování probíhalo prostřednictvím SMS zpráv, přičemž nebylo umožněno zasílání SMS zrušit.

Úřad zjistil, že toto zpracování osobních údajů se týkalo části klientů bez přihlédnutí k tomu, zda konkrétní osoby měly v minulosti u tohoto operátora problém s úhradou vyúčtování, a bez zohlednění faktu, že klienti stejnou informaci dostávali i jiným způsobem. Takové nastavení zpracování osobních údajů Úřad vyhodnotil jako rozporné se standardní ochranou osobních údajů a konstatoval, že mobilní operátor nezavedl vhodná technická a organizační opatření k zajištění toho, aby došlo ke zpracování pouze těch osobních údajů, jež jsou pro každý konkrétní účel nezbytné, jak vyplývá z ustanovení čl. 25 odst. 2 GDPR.

V návaznosti na tuto skutečnost ÚOOÚ vyhodnotil v konkrétních případech klientů nadměrné informování o vystaveném vyúčtování a jeho uhrazení prostřednictvím SMS jako zpracování bez právního důvodu dle čl. 6 odst. 1 GDPR. Úřad shledal, že kontrolovaná osoba nesplnila ani svou informační povinnost vůči subjektům údajů, když v této souvislosti neinformovala o účelech zpracování osobních údajů, jak ukládá čl. 13 odst. 1 písm. c) obecného nařízení.

Jednou z klíčových podmínek GDPR je nezbytnost zpracování osobních údajů. Praktickým důsledkem této podmínky je, že správce by měl provádět pouze takové zpracování osobních údajů, které je zcela nezbytné pro naplnění účelu zpracování. V daném případě

však správce osobních údajů prováděl rozesílku SMS, aniž by to bylo nezbytné, neboť zároveň využíval jiných způsobů ke sdělení totožných informací.

Vedení databáze náboženskou společností

ÚOOÚ prověřoval možné porušení povinností při zpracování osobních údajů vedených v databázích náboženské společnosti. Správce měl údajně o stěžovatelích – bývalých členech náboženské společnosti – uchovávat řadu informací i poté, co již nebyli členy. Po ukončení členství náboženská společnost část osobních údajů stěžovatelů vymazala a na jejich žádost jim zpřístupnila seznam nadále zpracovávaných osobních údajů. Po žádosti o výmaz těchto údajů však bylo stěžovatelům sděleno, že tak nelze učinit, neboť se jedná o údaje nezbytné pro oprávněné náboženské účely.

Úřad přezkoumal postup náboženské společnosti a porušení GDPR nezjistil. Bylo shledáno, že údaje, které náboženská společnost nevymazala, je nadále možné uchovávat v souladu s legitimními účely náboženské společnosti. Zjištěno bylo pouze bagatelní porušení, kdy kontrolovaná osoba nedohledala osobní údaje bývalého člena náboženské společnosti, přestože je měla dle vnitřních předpisů nadále vést. Uvedený nedostatek byl vyhodnocen jako porušení čl. 5 odst. 1 písm. f) GDPR, tedy nedostatečné zabezpečení osobních údajů před jejich náhodnou ztrátou či zničením.

Správce může i po skončení vztahu se subjektem údajů o něm vést údaje v nezbytném rozsahu, pokud k tomu má důvod. Zároveň by však měl předcházet náhodné ztrátě či zničení osobních údajů. To lze zajistit vhodným nastavením procesů uvnitř organizace, proškolením personálu či prováděním vlastních auditů, které odhalí případné problémy nastavení systému.

Využívání osobních údajů ze základního registru obyvatel

Při provádění kontrol v bankovním sektoru ÚOOÚ zjistil potenciálně velmi problematickou praxi některých bank týkající se využívání osobních údajů ze základního registru obyvatel.

Obecně zákon č. 21/1992 Sb., o bankách, dovoluje ve svém § 38af odst. 1 k plnění svých povinností stanovených právním předpisem využívat údaje mimo jiné i ze základního registru obyvatel. Praktické naplnění zákonné možnosti využívat údaje shromažďované primárně státem dle poznatků Úřadu spočívá v tom, že údaje jsou využívány v takové míře, že reálně dochází k vytváření kopií částí základního registru obyvatel, a to ve vztahu ke klientům banky.

Úřad v této souvislosti v roce 2024 vydal kontrolní protokol a záležitostí se nadále intenzivně zabývá napříč bankovním sektorem.

Zpracovatelské smlouvy krajů

ÚOOÚ se zaměřil na posuzování náležitostí smluv o zpracování osobních údajů podle čl. 28 odst. 3 GDPR (zpracovatelské smlouvy) uzavíraných mezi kraji jakožto správci osobních údajů a jejich jednotlivými zpracovateli. Kontrolní akce se týkala 13 krajů ČR.

Ze zjištěných skutečností vyplynulo, že přinejmenším některé z kontrolovaných osob si nejsou vědomy celkového rozsahu situací, při nichž je nutné zpracovatelskou smlouvu

uzavřít. Tato skutečnost byla patrná zejména ve vztahu ke zpracování osobních údajů prováděnému v souvislosti s provozem webových stránek. Vyvstala proto pochybnost, zda správci mají dostatečný přehled o jimi prováděném zpracování osobních údajů.

V případech posuzovaných smluv bylo možno identifikovat častou praxi smluvních stran spočívající v téměř doslovném opisování jednotlivých ustanovení GDPR, upravujících požadavky na obsah zpracovatelské smlouvy. Takový schematický postup však nemůže naplnit smysl a účel zpracovatelských smluv. Ty stranám naopak poskytují prostor pro tolik potřebnou konkretizaci v čl. 28 odst. 3 GDPR relativně abstraktně stanovených povinností, dopadajících zejména na zpracovatele osobních údajů.

Typickým příkladem nedostatečného přístupu ke sjednávání požadovaného obsahu zpracovatelské smlouvy je přepisování ustanovení čl. 28 odst. 3 písm. c) GDPR, případně jeho čl. 32 bez jakékoli konkretizace, či pouze s minimální konkretizací technických a organizačních opatření přijatých k zabezpečení zpracování osobních údajů. Uvedený problém se často vyskytoval také ve vztahu k závazku zpracovatele napomoci splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů, napomoci správci při zajišťování souladu s povinnostmi podle čl. 32 až čl. 36 GDPR, jakož i dalších. Úprava některých obsahových náležitostí spíše popisného charakteru pak ve zpracovatelských smlouvách scházela zcela, jako například v případě povahy zpracování osobních údajů.

ÚOOÚ v roce 2025 plánuje vydat souhrnnou zprávu z této kontrolní akce, která bude obsahovat i závěry aplikovatelné v praxi správců osobních údajů.

Coordinated Enforcement Framework 2024

Stejně jako v předchozích letech, také v roce 2024 se Úřad zapojil do koordinované dozorové akce Evropského sboru pro ochranu osobních údajů zvané *Coordinated Enforcement Framework (CEF)*. Tentokrát se společná akce zaměřila na postupy správců při uplatňování práva subjektu údajů na přístup k osobním údajům, zakotveného v čl. 8 Listiny základních práv EU a čl. 15 GDPR.

ÚOOÚ se zapojil primárně formou dotazníkového šetření. Dotazník byl vypracován ve spolupráci se zapojenými dozorovými úřady a jako okruh adresátů určil 22 bankovních institucí se sídlem v České republice.

Vyhodnocením dotazníků Úřad odhalil potenciální výskyt některých negativních jevů spojených s procesem vyřizování žádostí o přístup k osobním údajům, jež indikovaly možné porušení GDPR. Konkrétně v některých případech banky deklarovaly dobu uchovávání obdržených žádostí o přístup k osobním údajům, která zjevně přesahovala lhůty vyplývající z právních předpisů, v krajním případě se dokonce jednalo o několik desítek let. Při ověřování totožnosti subjektu údajů v souvislosti s žádostí o přístup k jeho osobním údajům, zejména při komunikaci na dálku, pak banky nezřídka uváděly, že požadují sdělení relativně běžných identifikátorů jako rodné číslo. Riziko neoprávněného přístupu k osobním údajům některé banky alespoň zmírňovaly zasíláním vyřízení žádosti o přístup k osobním údajům prostřednictvím předem sjednaného komunikačního kanálu. Mezi bankami se však vyskytly i takové, které v souvislosti s podáním žádosti o přístup k osobním údajům preferovaly dvoufaktorové ověření, či alespoň používaly méně běžné identifikátory (např. číslo smlouvy).

Na základě informací získaných šetřením ÚOOÚ v případech indikujících možné porušení GDPR v dohledné době využije svých pravomocí ve vztahu ke konkrétním bankám za účelem sjednání nápravy.

I.2. SPRÁVNÍ ŘÍZENÍ

Úřad vede správní řízení, a to buď řízení o nápravném opatření (v procesním režimu správního řádu), anebo řízení o přestupcích (v procesním režimu zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, a subsidiárně správního řádu). Jakkoliv je pro Úřad primární dosažení nápravy závadného stavu, v mnohých případech tak učinit nelze, neboť závadný stav již netrvá. Úřad při stanovování sankcí vždy přihlíží ke všem okolnostem případu a není výjimkou, že v případě bagatelních porušení udělí pouze napomenutí. V případě závažných, úmyslných a systémových pochybení však Úřad sahá i k udělení sankcí, které mohou v odůvodněných případech dosahovat hranice stovek miliónů korun.

Úřad zahajuje řízení v případech, kdy je skutkový stav dostatečně jasný (např. vyplývá ze stížnosti), nebo řízení předcházelo provedení kontroly, která dostatečně objasnila skutkové okolnosti zpracování osobních údajů.

Nedostatečně chráněné osobní údaje

V průběhu roku 2024 se Úřad ve zvýšené míře zabýval případy nálezů dokumentů s osobními údaji, například v kontejnerech komunálního odpadu. Jednalo se o typické příklady absolutně nedostatečného způsobu zabezpečení osobních údajů. Nálezy dokumentů byly mnohdy ohlášeny Policii ČR, čímž bylo zabráněno jejich případnému zneužití.

Zveřejnění registračních značek na sociálních sítích

V roce 2024 ÚOOÚ řešil neobvyklý případ zveřejnění 32 vybraných registračních značek automobilů. Úřad se běžně nezabývá zpracováním osobních údajů v příspěvcích běžných uživatelů na sociálních sítích, neboť většinou jde o osobní činnosti vyjmuté z věcné působnosti GDPR. Zde však byla působnost Úřadu dána, neboť zveřejnění registračních značek mělo poukázat na možný problém ve veřejném prostoru.

Osobní údaje odcizené ze systémů carsharingové společnosti

Závažný byl případ společnosti zabývající se *carsharingem*, sdílením osobních automobilů. Pro využití této služby bylo nutné nahrát do aplikace konkrétní dokumenty. Došlo však k průniku do IT systémů správce a následně k úniku některých dokumentů s osobními údaji. Dokumenty nebyly nijak chráněny, například ani vodoznakem, jenž by snížil hrozbu jejich zneužití. Správce se tak provinil jejich nedostatečným zabezpečením. Při výpočtu sankce ÚOOÚ přihlédl k faktu, že správce s Úřadem spolupracoval a sám byl obětí útoku, přičemž nebyla zjištěna žádná škoda, která by dotčeným subjektům údajů vznikla. Správce posléze přijal dodatečná zabezpečení dokumentů, včetně umístění vodoznaku.

Odmítnutí spolupráce kontrolované osoby

Relativně neobvyklý případ řešil Úřad v rámci kontroly zpracování osobních údajů. Kontrolovaná osoba zásadním způsobem odmítala spolupracovat, a to i přes opakované výzvy.

Úřad tak byl nucen udělit pokutu za nesoučinnost dle kontrolního řádu. Pokuta sice byla uhrazena, kontrolovaná osoba však nadále nespolupracovala, což vedlo k uložení další pokuty za nesoučinnost. Jak poté vyšlo najevo, kontrolovaná osoba se domnívala, že zaplacením pokuty za nesoučinnost je zproštěna povinnosti s Úřadem spolupracovat. Uhrazení pokuty však nemá žádný vliv na povinnost spolupráce kontrolovaných osob s ÚOOÚ, ostatně pokuty za nesoučinnost lze udělovat opakovaně, neboť jejich smyslem je zajištění řádného průběhu kontroly.

Zpracování osobních údajů v rámci souborů cookies a modelů *consent or pay*

Jako v předchozích obdobích, tak i v roce 2024 se věnoval Úřad problematice souborů cookies. V roce 2024 vedl 5 řízení, a to se středně velkými a velkými správci osobních údajů, v rámci kterých hrozí v případě shledání porušení GDPR pokuty v řádech miliónů korun. Těžiště problematiky se však v roce 2024 přesunulo od nastavení cookies lišt k využívání modelu *consent or pay* (souhlas, nebo zaplať). Během roku 2024 Úřad obdržel rekordní počet stížností na model *consent or pay*, provozovaný některými online platformami.

Nejvyšší pokuta za neoprávněné zpracování osobních údajů

V roce 2024 Úřad uložil dosud nejvyšší pokutu ve výši 351 milionů Kč. Pokuta byla uložena společnosti poskytující antivirový software (dále jen společnost A) za neoprávněné zpracování osobních údajů uživatelů jejího antivirového programu a jeho rozšíření internetových prohlížečů (*Browser Extensions*).

V rámci poskytování služeb antivirového softwaru zpracovávala společnost A osobní údaje uživatelů. V prokázaném období části roku 2019 předávala část těchto údajů týkajících se přibližně 100 milionů uživatelů společnosti B (dále jen společnost B), a to zejména pseudonymizovanou historii prohlížení internetu navázanou na jedinečný identifikátor.

Úřad shledal společnost A vinnou ze spáchání přestupků podle § 62 odst. 1 písm. a) a b) zákona č. 110/2019 Sb. Těchto přestupků se společnost A dopustila tím, že jako správce osobních údajů předávala osobní údaje uživatelů antivirového programu své sesterské společnosti B za účelem, který deklarovala jako tvorbu statistické analýzy trendů, přestože k tomuto zpracování jí nesvědčil právní titul ve smyslu čl. 6 odst. 1 nařízení (EU) 2016/679, a dále tím, že v souvislosti s předáváním osobních údajů společnosti B jako správce osobních údajů nedostatečně informovala subjekty údajů o účelech zpracování a o právním základu pro zpracování.

Společnost A se v rámci správního řízení hájila tím, že používala robustní anonymizační techniky, a předávané údaje proto byly anonymní. Anonymizací se rozumí proces, při kterém jsou zpracovány osobní údaje tak, aby bylo dosaženo nevratného znemožnění identifikace subjektu údajů. Na zpracování anonymních údajů se nařízení (EU) 2016/679 nevztahuje. Pokud jsou osobní údaje pouze pseudonymizovány, mohou být na základě dodatečných informací přiřazeny fyzické osobě, a jedná se tak o osobní údaje, které mají být zpracovávány v souladu s uvedeným nařízením. Společnost A předávala historii prohlížení internetových stránek, ze které před předáním odstranila přímé identifikátory (např. jméno, příjmení, e-mailovou adresu apod.) a další informace (např. unikátní kombinace určitých parametrů v URL adrese), přičemž některé URL nebyly předávány vůbec.

Současně byl předáván i údaj o čase, tudíž předávané URL adresy tvořily určitý řetězec, který byl prostřednictvím jedinečného identifikátoru instalace předmětného antivirového softwaru vázán na jedno zařízení, případně jednoho uživatele (uvedený identifikátor následně společnost B nahradila jiným jedinečným identifikátorem, díky kterému bylo možné vytvořit, resp. zachovat, řetězce pseudonymizovaných URL adres, které byly společnosti B předávány postupně). Přestože nebyl předáván kompletní řetězec URL adres, Úřad dospěl k závěru, že tento řetězec byl unikátní (neboť se liší internetové stránky, které uživatelé navštívili, jejich pořadí, počet i doba, kterou na nich strávili), a bylo tak možné sledovat (jedinečný) pohyb uživatele na internetu, jaké stránky navštívil, jaká videa shlédl, jaké články si přečetl, co vyhledával či koupil. Společnost B mohla obdržené údaje spojit s dalšími údaji z jiných zdrojů, včetně veřejně dostupných (např. sociálních sítí), a tím minimálně část subjektů údajů opětovně identifikovat a zjistit informace o jejich zájmech, chování, preferencích, bydlišti, majetkových poměrech, profesi apod. Mohlo tak dojít k citelnému zásahu do soukromí subjektů údajů.

Uživatelé byli společností A mylně informováni, že předává anonymní údaje, přestože předávala pseudonymizované osobní údaje. Společnost A přitom uživatelům slibovala, že bude respektovat jejich soukromí a nebude nikdy sdílet žádné osobní údaje. Uživatelé byli rovněž informováni o tom, že účelem předávání údajů je tvorba analýzy trendů, tedy že údaje byly zpracovávány pro statistické účely. Úřad však dospěl k závěru, že výsledkem zpracování údajů společností B nebyly pouze statistické údaje, tedy souhrnné údaje, které nelze vztáhnout k jednotlivci. Společnost B se mimo jiné prezentovala jako společnost zpřístupňující data „*marketérům*“, jimž poskytovala „*vhled do on-line chování spotřebitelů*“ a nabízela „*sledování cesty uživatelů na atomární úrovni*“.

Úřad v rozhodnutí zdůraznil, že společnost A je jedním z předních odborníků na kybernetickou bezpečnost, který nabízí veřejnosti nástroje k ochraně dat a soukromí. Její zákazníci tak nemohli očekávat, že právě tato společnost bude předávat jejich osobní údaje, respektive údaje, na jejichž základě by mohla být zjištěna nejen jejich totožnost, ale i další údaje týkající se jejich soukromí. Protože se jednalo o případ přeshraničního zpracování osobních údajů klientů v zemích EU, věc byla řešena zároveň s ostatními dotčenými dozorovými úřady v EU v rámci stanoveného mechanismu spolupráce. Rozhodnutí předsedy Úřadu bylo napadeno správní žalobou, o které dosud nebylo rozhodnuto.

I.3. SOUDNÍ ROZHODNUTÍ

Aplikace Karanténa a nezákonné shromažďování osobních údajů

Městský soud v Praze pravomocným rozsudkem z 20. června 2024 potvrdil předchozí rozhodnutí ÚOOÚ vydaná ve věci sp. zn. UOOU-02569/22 (viz výroční zpráva Úřadu za rok 2023). Tímto rozsudkem byla Policie ČR jako spravující orgán podle § 24 odst. 3 zákona č. 110/2019 Sb. (respektive Ministerstvo vnitra vystupující v odpovědnostním právním vztahu za Policii ČR) uznána vinnou tím, že v souvislosti s provozem aplikace Karanténa využívané při namátkových kontrolách osob v období od 1. dubna 2021 do 8. března 2022 nezákonně shromáždila osobní údaje 2 110 084 osob, jimž byla v rámci opatření proti šíření onemocnění COVID-19 nařízena izolace, za což jí byla vyměřena pokuta ve výši 975 000 Kč.

Soud v souladu s názorem ÚOOÚ zejména shledal, že se jednalo o zpracování osobních údajů prováděné v režimu Hlavy III zákona č. 110/2019 Sb., tedy o jednání v dozorové působnosti Úřadu, a to i s možností jej sankcionovat podle § 63 zákona č. 110/2019 Sb. Dále soud konstatoval, že ze samotného počtu zpracovávaných osobních údajů vyplývá, že se jednalo o jejich plošné shromažďování. Nemohlo se tedy jednat o jejich využití k šetření trestného činu či přestupku, což podporuje i skutečnost, že Policie ČR osobní údaje využívala při namátkových standardních kontrolách, které ze své povahy nesměřují k šetření konkrétního závadového jednání.

Úřad při svém rozhodování vzal v úvahu mimořádné okolnosti způsobené tehdejší pandemií COVID-19. Nicméně, jak potvrdil i soud, tyto okolnosti nemohou nikoho opravňovat k arbitrárnímu jednání porušujícímu právní řád, a překračujícímu dokonce i opatření tehdejšího Ústředního krizového štábu, a to v rozporu s veřejným zájmem na přiměřenou ochranu soukromí, resp. osobních údajů. Přitom bylo možné nalézt řešení, které by bylo v souladu s právním řádem a zároveň by umožnilo řádné plnění úkolů zúčastněných státních orgánů včetně Policie ČR.

Zveřejňování trestních rozsudků

Po složitém několikaletém řízení Městský soud v Praze svým rozsudkem čj. 9 A 87/2022-40 ze dne 30. května 2024 potvrdil poslední z rozhodnutí Úřadu vydaných ve věci sp. zn. UOOU-05284/19. Jím byl spolek, jehož účelem je ochrana občanských a lidských práv, uznán vinným ze spáchání přestupku podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., za což mu byla uložena pokuta ve výši 5 000 Kč.

Přestupku se spolek dopustil zveřejněním nedostatečně anonymizovaného trestního příkazu na svém profilu na sociální síti Facebook. Přitom byly publikovány údaje o jménu, příjmení, místu narození a místu bydliště odsouzené osoby, spolu s odkazem na facebookový profil s fotografií odsouzené osoby. Jak uvedl Úřad, a následně potvrdil i soud, tyto údaje umožnily identifikaci příslušné osoby, a představují tedy osobní údaj.

Dále soud potvrdil názor Úřadu, podle něhož předmětnému zveřejnění nesvědčil žádný z právních důvodů podle GDPR nebo zákona č. 110/2019 Sb. Navíc byl předmětný dokument zveřejněn na facebookovém profilu, který neměl zpravodajský charakter. Stejně tak Úřad ani soud neshledal žádný veřejný zájem na tom, aby byly publikovány osobní údaje odsouzené osoby. Postup, který příslušný spolek zvolil, svědčí o nepřípustném motivu, konkrétně o snaze dalšího veřejného potrestání odsouzené osoby.

Kasační stížnost spolku podanou v této věci pak Nejvyšší správní soud usnesením čj. 6 As 200/2024-31 ze dne 28. srpna 2024 odmítl, a to z důvodů nedoložení buď plné moci udělené advokátovi k zastupování v předmětném řízení anebo náležitého vzdělání zastupujícího zaměstnance, resp. člena stěžovatele, nicméně uvedené usnesení bylo nálezem Ústavního soudu čj. III. ÚS 2512/24 ze dne 29. ledna 2025 zrušeno. Ve věci tudíž bude rozhodováno znovu.

Ohlašovací a oznamovací povinnost v případě porušení zabezpečení osobních údajů

Městský soud v Praze svým rozsudkem čj. 17 A 109/2023-54 ze dne 31. května 2024 potvrdil předchozí rozhodnutí Úřadu vydaná ve věci sp. zn. UOOU-00414/23, jimiž byla zdravotnickému zařízení jako správci uložena pokuta ve výši 309 000 Kč.

Zdravotnické zařízení neoznámilo ÚOOÚ kybernetický útok na servery, na nichž byly uloženy databáze tohoto zdravotnického zařízení, a nedoložilo, že by informovalo dotčené subjekty údajů (přibližně 247 000 pacientů) o porušení zabezpečení jejich osobních údajů. Navíc se dokumentace zdravotnického zařízení k porušení zabezpečení nezabývala dopady narušení bezpečnosti, které jsou povinným údajem této dokumentace podle čl. 33 odst. 5 GDPR.

Rozsudek Městského soudu v Praze napadlo zdravotnické zařízení kasační stížností, o níž NSS dosud nerozhodl.

Náhrada nemajetkové újmy pohledem Soudního dvora EU

Během roku 2024 vydal Soudní dvůr EU celkem šest rozsudků zabývajících se právem na náhradu nemajetkové újmy a odpovědností správce podle čl. 82 nařízení (EU) 2016/679. Konkrétně se jedná o rozsudky ve věcech: C-687/21 (*MediaMarktSaturn*); C-741/21 (*juris GmbH*); C-182/22 a C-189/22 (*Scalable Capital*); C-590/22 (*PS Adresse erronée*); C-507/23 (*Patērētāju tiesību aizsardzības centrs*) a C-200/23 (*Agentsia po vpisvaniyata*). Rozsudky určují linii, jakým způsobem Soudní dvůr EU přistupuje k rozsahu náhrady nemajetkové újmy a otázkám jejího posouzení. Dva z rozsudků podrobněji rozebíráme.

V prvním rozsudku ze dne 25. ledna 2024 ve věci C-687/21, *MediaMarktSaturn*, se Soudní dvůr zabýval případem, ve kterém žalobce zakoupil elektroniku v obchodě provozovaném žalovanou stranou, přičemž platbu za tento nákup realizoval prostřednictvím úvěru poskytnutého třetí stranou. Za tímto účelem vyplnil několik dokumentů obsahujících jeho osobní údaje, například bankovní údaje a údaje o svých příjmech. Tyto dokumenty však zaměstnanci žalované strany omylem předali jinému zákazníkovi, který je odnesl z prodejny. Tento zákazník dokumenty přibližně po půl hodině vrátil, přičemž nebylo zjištěno žádné zneužití obsažených osobních údajů. Spor se týkal toho, zda má žalobce podle nařízení (EU) 2016/679 právo na odškodnění za nemajetkovou újmu způsobenou tímto pochybením žalované strany.

Soudní dvůr zejména potvrdil, že nemajetková újma podle čl. 82 nařízení (EU) 2016/679 vyžaduje, aby dotčený subjekt prokázal odůvodněné obavy a reálné riziko zneužití osobních údajů. Obava z možného zneužití osobních údajů třetími stranami, kterou pociťuje subjekt údajů v důsledku porušení tohoto nařízení, může sama o sobě představovat „nehmotnou újmu“. Dotčený subjekt nicméně musí prokázat důvodnost obavy z nebezpečí zneužití jeho osobních údajů. Je pak na vnitrostátním soudu, aby ověřil, zda je tato obava opodstatněná. Subjekt navíc musí prokázat, že toto riziko je skutečné, a ne hypotetické (např. když se žádná třetí strana s dotyčnými osobními údaji prokazatelně neseznámila). Soudní dvůr tak dospěl k závěru, že v situaci, kdy dokument obsahující osobní údaje byl neoprávněně předán třetí straně, která se s těmito údaji prokazatelně neseznámila, „nehmotnou újmu“ ve smyslu nařízení (EU) 2016/679 nepředstavuje pouhá obava subjektu údajů, že by si třetí strana mohla pořídit kopii, a tak v budoucnu jeho údaje šířit, nebo je dokonce zneužít. Soudní dvůr také rozhodl, že ke konstatování nevhodnosti technických a organizačních opatření zavedených dotyčným správcem nepostačuje sama o sobě okolnost, že zaměstnanci správce předali omylem neoprávněné třetí straně dokument obsahující osobní údaje zákazníka. Soudní dvůr nadto zopakoval své závěry z prejudikatury, a sice že čl. 82 nařízení (EU) 2016/679 nevyžaduje, aby byl pro účely náhrady újmy na základě tohoto ustanovení zohledněn stupeň závažnosti poru-

šení správcem. Kromě toho Soudní dvůr zrekapituloval, že právo na náhradu újmy stanovené v čl. 82 nařízení (EU) 2016/679 plní, zejména v případě nehmotné újmy, kompenzační funkci v tom smyslu, že peněžitá náhrada na základě uvedeného ustanovení musí umožnit plnou náhradu újmy, která konkrétně vznikla v důsledku porušení tohoto nařízení, a nikoli funkci sankční.

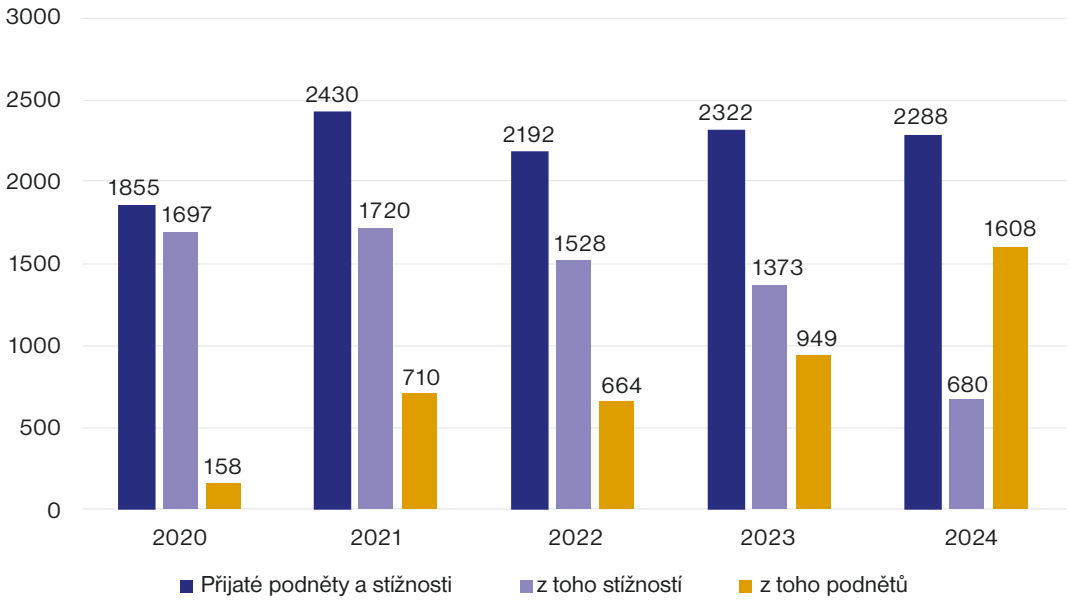
Ve druhém rozsudku Soudního dvora EU ze dne 4. října 2024 ve věci C-507/23, *Patērētāju tiesību aizsardzības centrs*, bylo řešeno, že Středisko pro ochranu práv spotřebitelů šířilo na několika internetových stránkách video, v němž mimo jiné vystupovala postava napodobující známého lotyšského novináře (žalobce), aniž by k tomu žalobce udělil souhlas. Stalo se tak v rámci kampaně za účelem informovanosti spotřebitelů o rizicích při nákupu ojetého vozidla. Ve sporném videu byl napodoben hlas žalobce, zobrazen seznam jeho oblíbených vět a použita čepice podobná té jeho. Objevil se v něm dokonce i záběr z jeho pořadu. Navzdory nesouhlasu, který žalobce vyjádřil v souvislosti s výrobou a šířením tohoto videa, zůstalo video dostupné na internetu. Středisko pro ochranu práv spotřebitelů také odmítlo jeho výslovné výzvy k zastavení tohoto šíření a náhradě újmy vzniklé poškozením jeho pověsti. Žalobce se po Středisku pro ochranu práv spotřebitelů domáhal náhrady nemajetkové újmy ve formě omluvy, jakož i odškodnění ve výši 2 000 eur. Sporný byl zejména výklad čl. 82 nařízení (EU) 2016/679.

Soudní dvůr v první řadě opět potvrdil závěry vyplývající z prejudikatury, jejímž prostřednictvím opakovaně vyložil, že porušení ustanovení nařízení (EU) 2016/679 nestačí samo o sobě k tomu, aby zakládalo „újmu“ ve smyslu čl. 82 odst. 1 tohoto nařízení. Existence „újmy“, ať již hmotné či nehmotné povahy, je totiž jednou z podmínek práva na náhradu újmy stanoveného v tomto ustanovení, stejně jako existence porušení ustanovení uvedeného nařízení a příčinné souvislosti mezi touto újmou a tímto porušením, přičemž tyto tři podmínky jsou kumulativní. Soudní dvůr se kromě toho zabýval i tím, zda omluva může představovat přiměřenou náhradu nehmotné újmy na základě tohoto ustanovení, zejména v případě, kdy nelze obnovit stav předcházející vzniku této újmy. V tomto případě potvrdil, že omluva může skutečně představovat přiměřenou náhradu nehmotné újmy, za předpokladu, že tato forma náhrady může plně nahradit újmu vzniklou subjektu údajů. V rámci třetí předběžné otázky pak Soudní dvůr rozhodl, že postoj a motivace správce se nezohledňují za účelem případného přiznání nižší náhrady újmy subjektu údajů, než je újma, kterou konkrétně utrpěl. V této souvislosti Soudní dvůr zdůraznil, že čl. 82 nařízení (EU) 2016/679 plní výlučně kompenzační funkci, na rozdíl od jiných ustanovení, jako jsou čl. 83 a 84 nařízení (EU) 2016/679, které mají v zásadě sankční účel.

I.4. PODNĚTY A STÍŽNOSTI

Ani v roce 2024 neklesal celkový počet stížností a podnětů, jichž bylo zaznamenáno stejně jako v předcházejících letech více než 2000. Takový počet podání vede v určitém počtu případů k tomu, že šetření mohou trvat delší dobu, než podatelé či stěžovatelé očekávají. Pro urychlení šetření je klíčová také kvalita jednotlivých stížností, neboť pokud z nich není zřejmý problém či to, čeho se stěžovatel domáhá, Úřad se zpravidla obrací na stěžovatele, aby tyto skutečnosti objasnil.

Vývoj počtu stížností a podnětů v letech 2020–2024



Zároveň platí, že práva subjektů údajů (právo na přístup, právo na výmaz a další) je prvotně nutné uplatnit u správce. Pokud se tak nestalo, je stěžovateli sděleno, že stížnost je předčasná a je nutné nejprve se obrátit na správce s žádostí o výkon některého z práv založených GDPR.

Analýza stížností a částečně i podnětů ukazuje na aktuální trendy v oblasti ochrany osobních údajů. Mimo rekordního počtu stížností na model *consent or pay* provozovaný některými online platformami, se v agendě podnětů a stížností objevovala následující témata.

Zpracování osobních údajů za účelem personalizace reklamy

ÚOOÚ v poměrně krátkém čase obdržel přibližně 80 stížností ohledně modelu *consent or pay*, z čehož se asi 70 týkalo konkrétního správce osobních údajů. Problematičnost užívaného modelu spočívá v posouzení, zda je souhlas se zpracováním osobních údajů udělený v rámci tohoto modelu svobodný. Je totiž třeba brát v úvahu výrazný nepoměr stran (online platforma vůči uživateli) a také fakt, že v případě neudělení souhlasu může být uživateli způsobena újma (bude mu odepřena pro něj klíčová služba). Nutné je rovněž posoudit výši poplatku, jenž je uživateli účtován za to, že jeho osobní údaje nejsou zpracovávány za účelem personalizace reklamy.

Tyto problematické skutečnosti reflektoval Evropský sbor pro ochranu osobních údajů (EDPB), jenž zaujal negativní postoj k využívání modelu *consent or pay* velkými online platformami. Ve svém stanovisku uvádí, že *„ve většině případů nebude možné, aby velké online platformy splňovaly požadavky na platný souhlas, pokud konfrontují uživatele pouze s binární volbou mezi udělením souhlasu se zpracováním osobních údajů pro účely behaviorální reklamy a zaplacením poplatku.“*

Rekordní množství stížností a podnětů na pozadí postoje EDPB se stalo důvodem, proč Úřad zahájil správní řízení s významnou online platformou o nápravném opatření, jehož předmětem je posouzení užívaného modelu *consent or pay*. Spolu se zahájením řízení ÚOOÚ vydal předběžné opatření, jímž zakázal nucení uživatelů online platformy k binár-

ní volbě. Poté platforma od tohoto systému ustoupila. Úřad nicméně pokračuje ve vedení řízení a nadále posuzuje, zda je model *consent or pay* v souladu s GDPR.

Zpracování osobních údajů v rámci zákona č. 106/1999 Sb.

Často se na Úřad obracejí lidé se stížnostmi na zveřejnění jejich osobních údajů coby žadatelů o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Nejčastěji se jedná o případy, kdy obec spolu se zveřejněním informace publikuje i žádost včetně osobních údajů žadatele, či s nedostatečně anonymizovanými údaji. ÚOOÚ se obvykle obrátí na subjekt, který žádost zveřejnil, a upozorní jej, že takový postup není v souladu s GDPR. Mnohdy již na základě upozornění dochází k nápravě stavu.

Zpracování osobních údajů ve školství

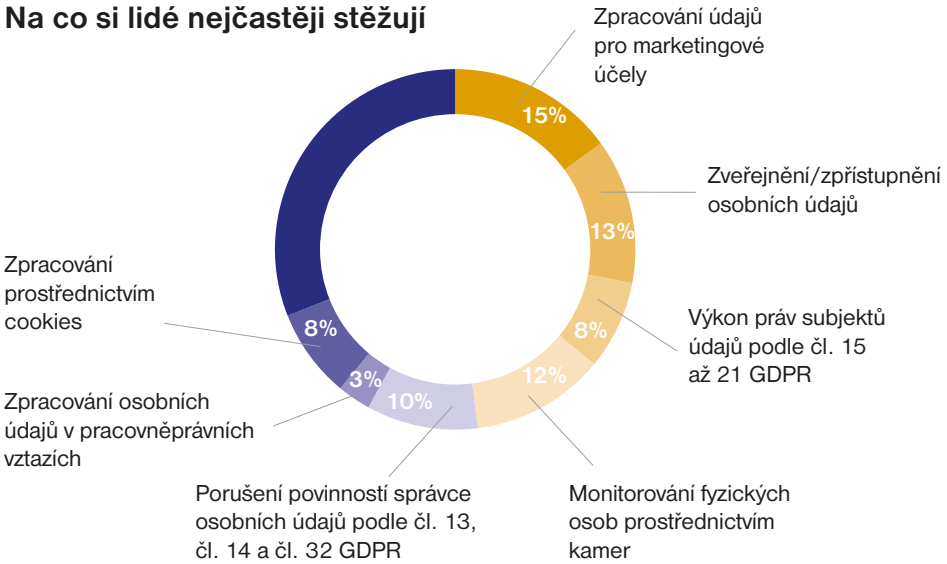
Úřad se průběžně zabývá stížnostmi na zpracování osobních údajů speciálně pedagogickými centry (SPC). Jde především o předání osobních údajů a jejich další zpracování SPC z pohledu zákonnosti zpracování a doby uchování. Šetření nadále probíhají. Nedostatky byly dosud shledány minimálně v plnění informační povinnosti.

Standardně jsou řešena podání obsahující neoprávněné zveřejňování či zpřístupňování osobních údajů žáků, studentů, zákonných zástupců či pedagogů. Po upozornění Úřadu obvykle dochází k nápravě nežádoucího stavu a k přijetí opatření vedoucích k eliminaci pochybení v budoucnu.

Stížnosti na sledování ze strany zaměstnavatele

ÚOOÚ pravidelně dostává stížnosti týkající se sledování zaměstnanců v souvislosti s využíváním kamerového systému nebo nahlížením do e-mailových schránek. Takové jednání může být porušením zákona č. 262/2006 Sb., zákoník práce, a přestupkem v této oblasti, proto jsou stížnosti postupovány příslušnému inspektorátu práce. Ve vztahu k provozování kamerových systémů na pracovišti se Úřad z hlediska své působnosti zabývá postupem správců při plnění informační povinnosti. Na základě upozornění Úřadu zaměstnavatelé obvykle uvedou poskytované informace do souladu s GDPR.

Na co si lidé nejčastěji stěžují



Zpracování osobních údajů společenstvím vlastníků jednotek (SVJ) a bytovým družstvem

Opakovaně je předmětem stížností neplnění informační povinnosti a nevyřizování přijatých žádostí členů SVJ či bytových družstev. Často se stížnosti vztahují také k neoprávněnému zveřejňování osobních údajů členů, například vyvěšením na veřejné nástěnce v bytovém domě. Protože se zpravidla nejedná o správce, kteří provádějí rozsáhlé zpracování osobních údajů, Úřad tyto stížnosti obvykle řeší upozorněním na pochybení a poučením o povinnostech vyplývajících z GDPR. Správci v drtivé většině pochybení napravují a přijímají adekvátní opatření k zamezení podobných případů.

Nevyžádaná sdělení zasílaná poštou s využitím údajů z veřejných rejstříků

Úřad se setkal se stížností, kdy byl stěžovatel písemně požádán o příspěvek na činnost neziskové organizace, která jeho kontaktní údaje získala z otevřených dat, např. ze živnostenského rejstříku. ÚOOÚ nevyhodnotil jednání jako porušení GDPR, protože správce se opíral o oprávněný zájem spočívající v zajištění finančních prostředků pro svou charitativní činnost. V podobných případech Úřad poučuje subjekty údajů o nutnosti vznést proti předmětnému zpracování osobních údajů námitku a požádat o výmaz osobních údajů, tedy nabádá stěžovatele, aby u správce sami uplatnili práva vyplývající z kapitoly III GDPR. ÚOOÚ posléze může přezkoumat, jakým způsobem správce reagoval, a zda tak učinil v souladu s GDPR. V posuzovaném případě správce po vznesení námitky osobní údaje subjektu vymazal.

Také v roce 2024 se značná část stížností týkala využití osobních údajů z katastru nemovitostí realitními subjekty pro zaslání návrhu na odkup nemovitosti nebo jejich podílu. Při každém zpracování osobních údajů musí správce disponovat relevantním odůvodněním ve smyslu čl. 6 GDPR, přičemž nejčastějším odůvodněním je oprávněný zájem [čl. 6 odst. 1 písm. f) GDPR]. Správce však musí mít na paměti, že jeho zájmy musí převážit nad zájmy nebo základními právy a svobodami subjektů údajů, což ve většině případů hromadných rozesílek s cílem náhodně „odchytit“ případného prodejce nemovitosti naplněno není. Konkrétně se ÚOOÚ zabýval stížnostmi, v nichž stěžovatelé namítali, že realitní kancelář podmiňovala vyřízení žádosti o výkon práv dle GDPR sdělením katastrálního území a čísla listu vlastnictví ze strany stěžovatelů. Ty potom obeslala nevyžádanými nabídkami odkupu podílů nemovitostí formou poštovních zásilek s odůvodněním, že neeviduje obesílané subjekty údajů podle jména. Avšak pokud je subjekt údajů oslovován formou poštovní zásilky, odesílatel prokazatelně disponuje jménem, příjmením a adresou daného subjektu. Nadto je správce povinen usnadňovat výkon práv subjektu údajů dle GDPR. Předmětná realitní společnost na základě komunikace s Úřadem přehodnotila svůj dosavadní postup s tím, že v obdobných případech již nebude požadovat sdělení katastrálního území a list vlastnictví jako povinný údaj nutný k vyřízení uplatněné námitky.

Zpracování osobních údajů prostřednictvím kamerových systémů

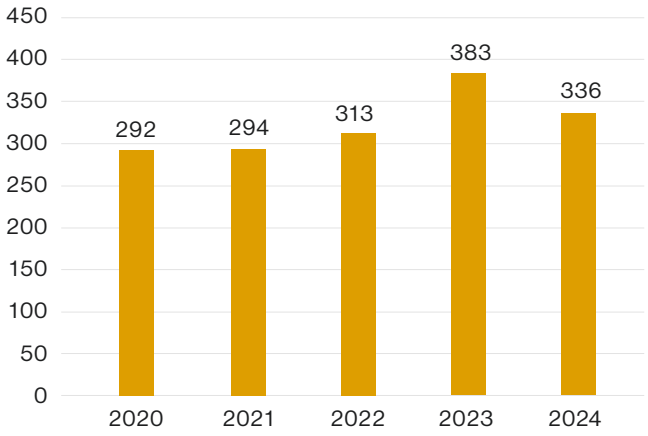
Značná část řešených podnětů a stížností se i v roce 2024 týkala zpracování osobních údajů prostřednictvím kamerových systémů, dveřních digitálních kukátek a fotopastí, a to především v souvislosti s dlouhodobými sousedskými nebo rodinnými spory, případně s ochranou majetku, bezpečnosti a zdraví osob. V této oblasti Úřad dlouhodobě upřednostňuje edukační přístup. Informuje správce především o jejich povinnostech jakožto správců osobních údajů a podatele seznamuje s řešením spočívajícím v podání podnětu na přestupek

proti občanskému soužití u obce s rozšířenou působností. Možností je rovněž účinně se bránit prostřednictvím občanskoprávní žaloby na ochranu osobnosti u příslušného soudu.

I.5. OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Úřad eviduje 336 ohlášení porušení zabezpečení osobních údajů. U menších společností, bytových družstev a orgánů veřejné správy, zejména obecních úřadů, jsou nadále nejčastější příčinou porušení zabezpečení osobních údajů útoky typu *phishing*, chybná odesílání e-mailů třetím osobám a ransomwarové útoky.

Počet ohlášených porušení zabezpečení osobních údajů v letech 2020–2024



Větší společnosti, ale i společnosti se zahraniční účastí, stále častěji čelí sofistikovaným kybernetickým útokům. Tyto útoky většinou spočívají v tom, že útočníci prostřednictvím škodlivého kódu po delší čas skenují dění v ICT infrastruktuře správce a analyzují možnost zranitelnosti systému, jako je např. *zero-day*, aby mohli získat např. přístup do prostředí správce prostřednictvím neoprávněně získaných uživatelských přihlašovacích údajů v důsledku tzv. *credential dumping*. Většina těchto společností však zkušenosti s různými druhy kybernetických útoků má a uplatňuje odpovídající technická opatření, jako je např. EDR technologie, *rate limiting* apod. Zároveň společnosti zaznamenaly, že se pachatelé specifickými kombinacemi přihlašovacích údajů (např. e-mail + heslo) snažili proniknout do ICT infrastruktury správce, avšak tyto kombinace útočníci získali z jiných zdrojů než v důsledku úniku u správce. Mohlo se jednat o únik informací jiného provozovatele služby nebo o důsledek nezodpovědného chování klienta na sociálních sítích.

V případě ohlášení porušení zabezpečení ze strany orgánů činných v trestním řízení se jednalo převážně o neoprávněné lustrace v informačních systémech Policie ČR. Zaznamenáno bylo také pochybení při odeslání dokumentů s osobními údaji do datové schránky, čímž došlo ke zpřístupnění osobních údajů v rámci trestního řízení jiné osobě.

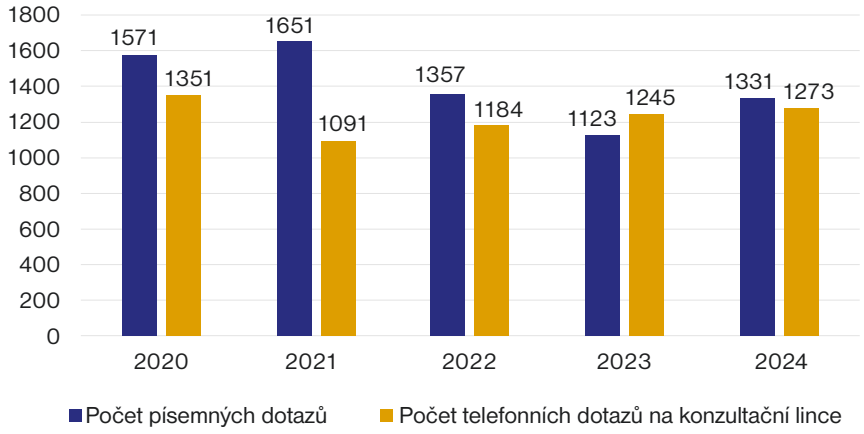
I.6. KONZULTACE

Podobně jako v předchozích letech obdržel Úřad množství písemných dotazů ze strany institucí i veřejnosti a rovněž dotazů prostřednictvím telefonní informační linky. Mnohé se tradičně týkaly kamerových systémů, bytových domů, obecních záležitostí či zdravotnictví.

Osobní konzultace byly poskytnuty zástupcům vysokých škol na téma bezpečnostních opatření zvažovaných v souvislosti s útokem na Filozofickou fakultu Univerzity Karlovy

v prosinci 2023 v kontextu ochrany osobních údajů. S Ministerstvem práce a sociálních věcí bylo projednáno oslovení jednotlivých donorů a příjemců finančních prostředků pro podporu výkonu sociálních služeb či sociální práce a obdobných aktivit na podporu integrace osob s dočasnou ochranou v ČR. S Řízením letového provozu České republiky, státní podnik, byla projednána problematika kamer umístěných na dronech. Rovněž byla poskytnuta osobní konzultace Masarykovu onkologickému ústavu ve věci aplikace právních titulů u vědeckého výzkumu, který provádí poskytovatelé zdravotních služeb. Konzultováno bylo také monitorování pracovního vybavení pracovníků úklidu a jeho vhodnost vzhledem k ochraně osobních údajů ze strany Technické správy komunikací hl. m. Prahy, a.s.

Vývoj počtu písemných a telefonních dotazů v letech 2020–2024



S Úřadem vlády ČR bylo prostřednictvím videokonference prodiskutováno elektronické potvrzení o studiu vysokoškolských studentů (elektronicky vedené sdružené informace matrik studentů, eSIMS). Telefonicky byly vyřizovány dotazy Policie ČR na oprávněnost užívání kamerových systémů a zveřejňování údajů na sociálních sítích. Společně s Národním úřadem pro kybernetickou a informační bezpečnost se ÚOOÚ podílel na vydání společného prohlášení upozorňujícího na e-shopové aplikace, které požadují nestandardní oprávnění v zařízení uživatele a mohou sbírat nadměrné množství uživatelských dat včetně osobních údajů.

Tak jako v předchozích letech, ani v roce 2024 neobdržel Úřad žádost, která by splňovala požadavky na poskytnutí konzultace podle čl. 36 obecného nařízení. V předmětném roce Úřad neobdržel ani žádost o projednání ve věci vzniku nové evidence v rámci spravujícího orgánu podle § 38 odst. 1 zákona č. 110/2019 Sb.

Poradenství a konzultace byly i v roce 2024 poskytovány telefonicky prostřednictvím informační linky, a to každé úterý a čtvrtek od 13:00 do 15:30 hod.

Povinnost vést logy

ÚOOÚ obdržel dotazy na případnou povinnost vést tzv. logy, a to jak v obecné rovině, tak v rámci přístupu do zdravotnické dokumentace. Logy jsou textové soubory obsahující

záznamy o činnosti nějaké konkrétní aplikace. V případě webových serverů jsou do logů ukládány veškeré požadavky vznesené na server, a zpětnou analýzou těchto dat lze pak zjistit cenné informace o fungování sledovaného webu. V rámci předmětné problematiky bylo sděleno, že obecné nařízení neukládá vedení tzv. logů výslovně. V závislosti na povaze a rozsahu zpracování jsou však logy prakticky nezbytným technickým opatřením k doložení souladu s obecným nařízením ve smyslu čl. 24 a 32 obecného nařízení.

K výše uvedenému bylo doplněno, že dle čl. 5 odst. 1 písm. f) obecného nařízení je stanoveno, že osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření. Správce osobních údajů je odpovědný za dodržování základních zásad zpracování osobních údajů a dodržení uvedeného souladu musí být schopen doložit. Aby byl správce schopen v praxi doložit faktické splnění citované zásady integrity a důvěrnosti, je při zpracování osobních údajů v rámci evidence elektronickou formou vedení tzv. logů prakticky nezbytné. Současně by měl správce předcházet situacím, kdy se prostřednictvím jednoho přístupového účtu do nemocničního informačního systému či obdobného systému, ve kterém je vedena zdravotnická dokumentace, přistupuje vícero zaměstnanců. Nutno doplnit, že daný poskytovatel zdravotních služeb může být také sankcionován ze strany odpovědných orgánů v případě porušení ustanovení vztahujících se k neoprávněnému nahlížení do zdravotnické dokumentace dle § 117 odst. 3 písm. d) a popřípadě h) zákona č. 372/2011 Sb., o zdravotních službách.

Posouzení vlivu na ochranu osobních údajů v kontextu nemocničních informačních systémů

Úřad se vyjadřoval k případné povinnosti vypracovat posouzení vlivu na ochranu osobních údajů dle čl. 35 obecného nařízení u nemocničních informačních systémů. V dané věci bylo uvedeno, že povinnost vypracovat posouzení vlivu na ochranu osobních údajů zavedlo pro široký okruh správců obecné nařízení v roce 2018. K jeho implementaci byla vydána řada pokynů, které se více či méně konkrétně věnují jednotlivým tématům.

K posouzení vlivu vypracoval ÚOOÚ specifický metodický materiál *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů,* jenž uvádí seznam deseti kritérií, která by měl správce zvážit, aby zjistil, zda má povinnost provést posouzení vlivu na ochranu osobních údajů. Nutno uvést, že v případě implementace nemocničního informačního systému se správce nevyhnutelně dotkne zvláštní kategorie osobních údajů dle čl. 9 obecného nařízení i rozsáhlého množství subjektů údajů.

Evidence docházky elektronickým systémem zaznamenávajícím fotografii obličeje zaměstnanců

V rámci dotazu týkajícího se docházkového systému elektronicky zaznamenávajícího fotografii obličeje zaměstnanců Úřad uvedl, že účelem zpracování osobních údajů zaměstnanců získaných tímto způsobem je evidence dodržování pracovní doby zaměstnanců, a případně také evidence jejich docházky pro možné uplatnění pracovněprávních nároků zaměstnavatele vyplývajících z pracovních smluv.

V případě, že takto získané fotografie obličejů zaměstnanců nejsou biometrickými údaji definovanými v čl. 4 bodu 14) obecného nařízení, v němž je stanoveno, že *„pro účely tohoto nařízení se rozumí „biometrickými údaji" osobní údaje vyplývající z konkrétního tech-*

nického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje", a tedy tento elektronický systém evidence docházky nezpracovává biometrické údaje, pak předmětné zpracování osobních údajů není apriori v rozporu s obecným nařízením.

V takovém případě se pravděpodobně jedná o zpracování osobních údajů příslušným zaměstnavatelem dle čl. 6 odst. 1 písm. f) obecného nařízení, tj. pro účely oprávněných zájmů zmíněného správce, které je prováděno bez souhlasu subjektu údajů, tedy bez souhlasu zaměstnanců. To samozřejmě platí za předpokladu, že v dané věci byl řádně proveden test proporcionality, jímž byla odůvodněna nezbytnost a účelnost zpracování předmětných fotografií oproti jiným standardním řešením, jako je např. použití čipového systému.

Poskytování údajů ze zdravotnické dokumentace zaměstnavateli

ÚOOÚ řešil dotaz, zda je zaměstnavatel oprávněn požadovat po svém zaměstnanci zdravotnickou dokumentaci v případě, že došlo k pracovnímu úrazu. Úřad zaujal stanovisko, že zaměstnavatel v souladu s ustanoveními zákoníku práce může vyžadovat posudek od poskytovatele pracovně lékařských služeb, který je kompetentní ke zjištění, zda je zaměstnanec schopen či neschopen práce a za jakých podmínek. Nelze však požadovat rozšíření dokumentace předávané zaměstnavateli např. na propouštěcí zprávu od poskytovatele zdravotních služeb či zprávy od specialistů, pokud není sledován zákonný titul ke zpracování daných údajů. Zaměstnavateli v daném případě nevychází vstříc ani žádná z výjimek ze zákazu zpracování zvláštní kategorie osobních údajů dle čl. 9 odst. 2 obecného nařízení.

Kamerový systém u dětského bazénu

V případě kamery umístěné u dětského bazénku v prostorách sportovního zařízení Úřad upozornil správce, aby zvážil zpřístupňování záběrů z dětského bazénu na svých internetových stránkách, resp. jeho nezbytnost pro informování veřejnosti o dostupnosti služeb. K danému zpracování osobních údajů, kde jsou převážně zachycovány nezletilé osoby, je nezbytné řádné provedení testu proporcionality, jehož pozitivní výsledek je v daném případě nepravděpodobný.

Určení právních titulů u druhotného využití osobních údajů klinického hodnocení léčiv

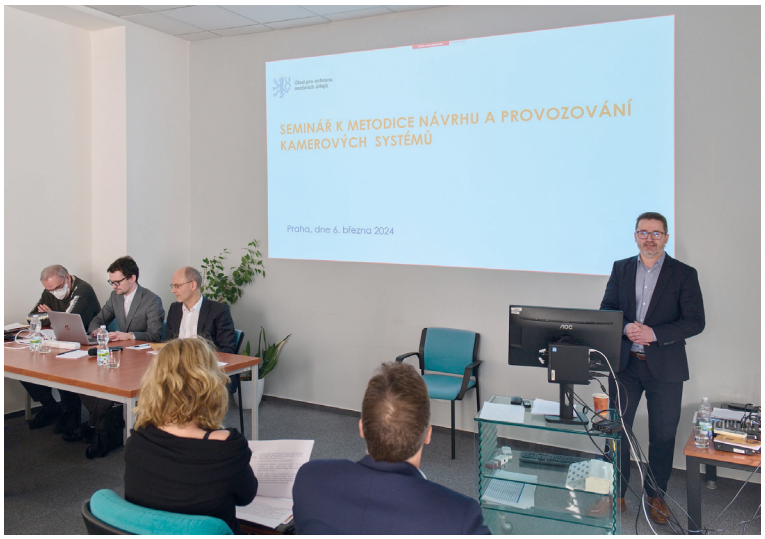
Ohledně právních titulů u klinických hodnocení léčiv Úřad poukázal na stanovisko EDPB č. 3/2019 k otázkám a odpovědím týkajícím se vzájemného působení nařízení o klinických hodnoceních a obecného nařízení [čl. 70 odst. 1 písm. b)]. Ve stanovisku je uvedeno, že *„správci údajů by se měli zaměřit zejména na podmínky „svobodně uděleného" souhlasu. Jak je stanoveno v pokynech pro souhlas Pracovní skupiny podle článku 29, předpokládá tento prvek skutečnou volbu a kontrolu ze strany subjektů údajů. Kromě toho by souhlas neměl představovat platný právní důvod pro zpracování osobních údajů ve zvláštním případě, kdy mezi subjektem údajů a správcem existuje jasná nerovnováha. V závislosti na okolnostech klinického hodnocení mohou nastat situace nerovnováhy sil mezi zadavatelem/zkoušejícím a účastníky. Nařízení o klinických hodnoceních tato rizika výslovně řeší a požaduje, aby zkoušející vzal v úvahu všechny relevantní okolnosti, zejména to, zda potenciální subjekt hodnocení patří do hospodářsky či sociálně znevýhodněné skupiny nebo je v situaci institucionální či hierarchické závislosti, což by mohlo nevhodně ovlivnit jeho rozhodnutí o účasti… Evropský sbor pro ochranu osobních údajů je tudíž toho názoru, že správci údajů by měli zejména řádně posoudit okol-*

nosti klinického hodnocení před tím, než se opřou o souhlas jednotlivců jako o právní základ pro zpracování osobních údajů pro účely výzkumných činností daného hodnocení.“

Co se týče možnosti aplikovat jako právní titul souhlas, Úřad nezastává odlišné stanovisko, neboť uvedené znění vychází ze základních náležitostí souhlasu uvedeného v čl. 4 bod 11) obecného nařízení a podmínek jeho vyjádření dle čl. 7 obecného nařízení. Nelze tedy aplikovaný souhlas v prostředí zdravotnictví, konkrétně klinického hodnocení a sekundárního využití pro vědecké účely apriori odmítnout. Správce je však povinen dodržet všechny povinnosti vztahující se k využití daného právního titulu dle obecného nařízení, zejména se zaměřením na svobodné udělení souhlasu. Obdobně se k závěru výše uvedeného stanoviska staví EDPB, který spatřuje jako vhodnější v daném případě aplikovat veřejný či oprávněný zájem správce dle čl. 6 písm. e) či f) obecného nařízení v závislosti na specifičnosti daného konkrétního vědeckého výzkumu.

Kamerový systém se záznamem na základní škole

ÚOOÚ se zabýval dotazem ohledně kamerového systému se záznamem užívaným ve školním zařízení. Konkrétně se jednalo o umístění kamer v odborných učebnách, přičemž žáci a zaměstnanci podepsali souhlas se zpracováním obrazového i zvukového záznamu v rámci školy. Ve své odpovědi Úřad zdůraznil okolnost, že v praxi zpravidla považuje kamery umístěné v učebnách školy za nepřiměřené oproti zájmům a základním právům a svobodám dotčených subjektů údajů. Dále Úřad upozornil, že provádět předmětné zpracování na základě souhlasu také obvykle nepovažuje za vhodné. Pro faktickou nerovnováhu mezi školou a subjekty údajů lze totiž pochybovat o dobrovolnosti udělení, rovněž odvolatelnost souhlasu v kontextu účelu předmětného zpracování je snadná.



Seminář „K metodice návrhu a provozování kamerových systémů“, Praha 6. 3. 2024

I.7. AKTIVITY PRO VEŘEJNOST

V rámci své osvětové činnosti ÚOOÚ v roce 2024 pokračoval v pořádání odborných seminářů pro veřejnost. V rámci prvního semináře v březnu 2024, kterého se zúčastnilo více než 600 účastníků, byla představena *Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů*. Úřad dále navázal semináři *K dozorové činnosti ÚOOÚ v oblasti zpracování osobních údajů* a *K právu na informace v kontextu ochrany osobních údajů a soukromí*. Všech seminářů bylo možno zúčastnit se jak prezenční, tak online formou.

Setrvalý zájem veřejnosti týkající se provozování kamerových systémů Úřad aktivně reflektoval koncipováním materiálů formou doporučení. Doporučení ve specifických oblastech doplňují již dříve zpracovanou *Metodiku k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů*. Konkrétně se jedná o *Doporučení ÚOOÚ č. 01/2024 ke zpracování osobních údajů prostřednictvím záznamu z kamer, kterými jsou vybavena bezpilotní letadla* (drony) a o *Doporučení ke kamerovým systémům umístěným ve školách a školských zařízeních,* které bylo předloženo k veřejné konzultaci.

Na alarmující trend omezování úvazků, dokonce rušení pozic pověřenců pro ochranu osobních údajů v institucích samosprávy a státní správy, Úřad reagoval koncipováním *Doporučení ÚOOÚ č. 2/2024 k postavení pověřenců pro ochranu osobních údajů.*

V rámci zvyšování povědomí veřejnosti o ochraně osobních údajů Úřad pokračoval ve vydávání osvětových materiálů formou informačních tiskovin týkajících se např. posouzení vlivu na ochranu osobních údajů (DPIA), Schengenského informačního systému či obrany před nevyžádaným marketingem.

Společné jednání zástupců Úřadu s poslanci Petičního výboru Poslanecké sněmovny Parlamentu ČR, Praha 8. 10. 2024

Představitelé a experti ÚOOÚ se zúčastnili řady odborných konferencí a seminářů zaměřených na problematiku zpracování osobních údajů, ať již s úvodním projevem nebo s odbornou prezentací. Účast ÚOOÚ tak byla zajištěna na konferencích s mezinárodní účastí *Privacy Days 2024* či online konferenci *Call for GDPR update?* pořádaných Spolkem pro ochranu osobních údajů a dalšími zahraničními organizacemi. Úvodním příspěvkem k postavení pověřenců v Evropě byl rovněž zahájen seminář *GDPR a ochrana osobních údajů z pohledu nových bezpečnostních hrozeb a praxe do oblasti kybernetické bezpečnosti*, který byl pořádán v Poslanecké sněmovně Parlamentu ČR. Z dalších odborných seminářů zaměřených více na praktické aspekty se jednalo např. o setkání pověřenců v oblasti zdravotnictví ve Zlíně organizované Spolkem pro ochranu osobních údajů, v oblasti veřejné správy pak o účast na konferenci Svazu měst a obcí na téma *Dobrá obec dělá dobrou školu*. Zástupci ÚOOÚ dále přijali účast na seminářích organizovaných Asociací pověřenců ČR *Kamerové systémy a zpracování biometrických údajů* či *K problematice role pověřence pro ochranu osobních údajů.* Další akce s účastí Úřadu byly například kulatý stůl k problematice zpracování zvláštních kategorií osobních údajů, organizovaný Asociací inkasních agentur, konference Českého telekomunikačního úřadu k novému evropskému nařízení o digitálních službách či společná porada vedoucích pracovníků bytových družstev Moravy a Slezska v Prostějově k tématu kamerových systémů.

I.8. LEGISLATIVA

Legislativní činnost Úřadu v oblasti ochrany osobních údajů spočívá především v přípravě připomínek předsedy ÚOOÚ k návrhům právních předpisů, vyjednávání mezinárodních smluv a nelegislativních dokumentů. V roce 2024 obdržel ÚOOÚ celkem 240 žádostí o stanovisko. Úřad uplatnil celkem 134 souhrnů připomínek, ke zbytku připomínky neuplatnil.

Umělá inteligence

Dne 30. listopadu 2022 společnost OpenAI představila aplikaci ChatGPT, čímž započal velký rozmach generativní umělé inteligence. EU proto urychlila schvalování *nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)*. Toto nařízení je platné od 12. července 2024 a účinné bude převážně od 2. srpna 2025 a 2. srpna 2026. Jeho účelem je zlepšit fungování vnitřního trhu, podporovat inovace a zavádění důvěryhodné umělé inteligence zaměřené na člověka a zároveň zajistit vysokou úroveň ochrany zdraví, bezpečnosti, základních práv zakotvených v Listině základních práv Evropské unie, včetně demokracie, právního státu a ochrany životního prostředí před škodlivými účinky.

Adaptace českého právního řádu bude mít podobu úpravy stávajících právních předpisů. Do konce roku 2024 ČR nerozhodla, který orgán veřejné správy bude plnit roli orgánu dozoru nad trhem podle čl. 3 bodu 26 a čl. 70 odst. 1.

Cílem adaptace českého právního řádu na čl. 3 bod 42 nařízení o umělé inteligenci je zavést regulaci „izolovaného systému", čímž se rozumí systém umělé inteligence pro vzdálenou biometrickou identifikaci fyzických osob v reálném čase. Nosičem je sněmovní tisk 807, *vládní návrh zákona, kterým se mění zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, a některé další zákony.* Použití izolovaného systému je omezeno na mezinárodní letiště, kterých je v ČR šest: Letiště Václava Havla Praha, Letiště Brno-Tuřany, Letiště Leoše Janáčka Ostrava, Letiště Pardubice, Letiště Karlovy Vary a Letiště Mnichovo Hradiště. Součástí je také změna zákona č. 110/2019 Sb., o zpracování osobních údajů, kde by mělo dojít ke dvěma substantivním změnám tohoto zákona po pěti letech od jeho účinnosti. Zásadní bude změna pravomoci ÚOOÚ vydávat vyhlášky na pravomoc vydávat opatření obecné povahy, což lépe vyhovuje potřebám praxe. Současně by mělo dojít ke snížení věkové hranice pro pozici místopředsedů ze 40 let na 35 let.

Příprava procesní adaptace na GDPR

Výsledkem dlouhodobého trendu posilování individuálních oprávnění v řízení je nedávná judikatura SDEU a na ni navazující judikatura NSS, která pro procesní postup akcentuje na základě stížnosti podle čl. 77 obecného nařízení o ochraně osobních údajů správní řízení o žádosti (dříve tzv. návrhové řízení) a dává mu přednost před řízením *ex officio*, tedy řízením zahajovanému z moci úřední.

Při přípravě adaptace českého právního řádu na GDPR bylo pečlivě zvažováno, jak který instrument promítnout do českého právního řádu. Co se týká typu správního řízení, jako preferované bylo zvoleno právě řízení z úřední povinnosti, protože je pro ochranu veřejného zájmu typické, a to zejména v přestupkovém řízení. Návrhové řízení bylo tradičně

používáno pro případ, že žadatel chce získat od státu nějaké oprávnění či povolení (např. živnostenské oprávnění, stavební povolení nebo licenci pro regulovanou činnost). Oproti tomu stížnost byla doposud chápána jako podnět k zahájení správního řízení ve vlastní věci. Nyní je ale výkladový trend v justici odlišný. Proto je i ÚOOÚ nucen na základě stížnosti subjektů údajů podle čl. 77 obecného nařízení transformovat procesní postupy na řízení o žádosti či návrhové řízení. Také ve správním trestání jsou výkladovým trendem justice oprávnění oznamovatele značně posílena.

Zákon č. 110/2019 Sb. však na tento posun není připraven, protože vycházel z odlišného pohledu. Jeví se jako nezbytné uzpůsobit národní legislativu tak, že bude formálně i materiálně zpřesněn nebo nově vymezen pojem stížnosti (jako stížnosti subjektu údajů podle čl. 77 obecného nařízení na zpracování jeho osobních údajů porušující toto nařízení), má-li jí být zahajováno návrhové řízení podle části druhé hlavy VI správního řádu, jak dovozuje NSS. Také nároky kladené na žadatele o vydání povolení či oprávnění jsou standardně jiné, přísnější než na podatele podnětu k zahájení řízení, zejména pokud jde o rozsah povinnosti doložit splnění podmínek pro vyhovění jeho žádosti. Má-li tedy stížnost subjektu údajů být chápána jako žádost, je také vhodné se výslovně vypořádat s dispoziční zásadou, jejíž plné promítnutí by znamenalo, že je odpovědností stěžovatele u porušení obecného nařízení nejen tvrdit, že k němu aktuálně dochází, ale také navrhnout konkrétní důkazy k prokázání svých tvrzení.

Dalším aspektem, který by bylo vhodné postavit najisto, je otázka lhůt pro vydání rozhodnutí o stížnosti. Standardní lhůta pro vydání rozhodnutí činí podle správního řádu měsíc, doslova „30 dnů“ v jednoduchých případech a dva měsíce, doslova „60 dnů“ ve složitých případech. Pokud žadatel potřebné podklady nedoložil a správní úřad ho vyzve k odstranění zjištěných nedostatků žádosti, lhůta pro rozhodnutí po dobu, než žadatel svou žádost doplní, neběží. Nicméně pro řádné prověření a zjištění, zda jsou zpracovány osobní údaje stěžovatele namítané jeho stížností a zda takové zpracování porušuje obecné nařízení, jsou uvedené lhůty příliš krátké a nelze během nich adekvátně posoudit zejména komplexní zpracování osobních údajů, které se týká širšího či velkého okruhu subjektů údajů. Správce či zpracovatel také mají v řízení vůči nim procesní práva, která nelze pominout, zejména právo vyjádřit se k podkladům rozhodnutí. Ostatně i obecné nařízení o ochraně osobních údajů samo v čl. 78 předvídá, že šetření stížnosti subjektu údajů může trvat podstatně déle než 30 či 60 dnů. Proto by měly být stanoveny realističtější lhůty pro vydání rozhodnutí o stížnosti.

Výsledkem reforem by rovněž mělo být nové zamyšlení nad opravnými prostředky ve správním řízení. Důvodem jejich plejády byla buď úplná absence správního soudnictví, nebo později neúplná jurisdikce správních soudů. To však již od zřízení NSS a přebudování správního soudnictví neplatí. Proto se v takto komplikovaném řízení v prvním stupni jeví jako neúčelné poskytovat jiné opravné prostředky než soudní, typicky správní žalobu.

Procesní nařízení

Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679 byl předložen Evropskou komisí dne 4. července 2023. Jedním z impulsů pro vypracování návrhu byl seznam procesních aspektů, které by mohly být harmonizovány s cílem zlepšit spolupráci mezi úřady pro ochranu osobních údajů v přeshraničních případech, který EDPB publikoval v říjnu 2022. Ná-

vrh nařízení byl paralelně projednáván jak v Radě EU, tak v Evropském parlamentu. Dne 10. dubna 2024 přijal Evropský parlament postoj v prvním čtení. Paralelně na předpisu pracovala Rada EU, která se dne 13. června 2024 dohodla na tzv. obecném přístupu. Maďarské předsednictví Rady EU se ve druhé polovině roku neúspěšně snažilo dosáhnout dohody s Evropským parlamentem a Evropskou komisí v tzv. trialozích, nicméně jednání pokračují i v roce 2025 a adaptace českého právního řádu tedy zatím formálně nemohla započít.

ÚOOÚ do sjednávání vstupoval pouze nepřímo na základě aktivní účasti ve vnitrostátních koordinačních mechanismech a při přípravě Stanoviska EDPB 4/2024 k legislativnímu vývoji návrhu procesního nařízení (září 2024). Do procesu Úřad vstupoval s obavami, že se návrh odchyluje od žádoucího zvýšení efektivity řízení a že uvažované znásobení procesní a administrativní zátěže v přeshraničních případech, jichž je menšina, se promítne i do vnitrostátních řízení, tedy do všech řízení vedených Úřadem. Ze systémového hlediska se nicméně Úřad soustředil na aspekty průřezového charakteru, k nimž náleží zachování pojetí stížnosti jako nástroje ochrany subjektivního práva stěžovatele (v kontextu tendence vytvořit přesah stížnosti do sféry veřejného zájmu) a chápání nově přiznávaných procesních práv stěžovatele jako relativních ve vztahu k tvrzenému porušení vlastního práva (v kontextu tendence k formálnímu pojetí účastníka řízení bez ohledu na jeho vztah k celé šíři skutkového a právního stavu). Toto pojetí následně podpořil ve svém Stanovisku 4/2024 i EDPB. Předmětem zájmu Úřadu byly rovněž mechanismy zrychleného vyřizování v jednoduchých či nesporných věcech, přizpůsobení některých ustanovení realitě dvoustupňových správních úřadů či přístup účastníků řízení do spisu. Konečné přijetí nařízení lze předpokládat v roce 2025.

eTurista

Předmětem velkých kontroverzí je *návrh zákona, kterým se mění zákon č. 159/1999 Sb., o některých podmínkách podnikání a o výkonu některých činností v oblasti cestovního ruchu, ve znění pozdějších předpisů, a další související zákony*, který od 26. července 2024 projednává Poslanecká sněmovna jako sněmovní tisk 761.

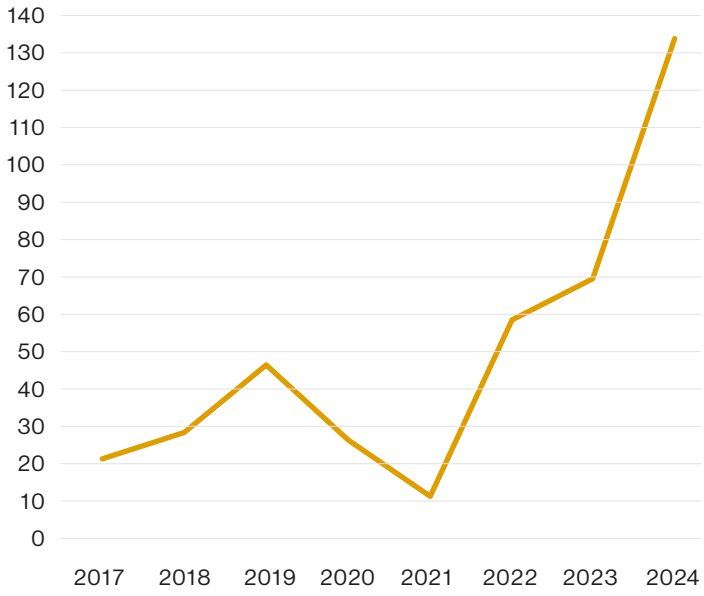
Podstatou je, že má být zaveden *Registr ubytovacích zařízení a ubytovaných osob* (eTurista), který má nahradit dosavadní hlášení ubytovatelů různým institucím. ÚOOÚ má k tomuto návrhu obdobné připomínky, jako měl Evropský inspektor ochrany údajů k *návrhu nařízení Evropského parlamentu a Rady (EU) o shromažďování a sdílení údajů týkajících se služeb v oblasti krátkodobých pronájmů a ubytování* – vyloučit použití osobních údajů ubytovaných pro účely vymáhání práva nebo pro účely daní a cel. Hlavní vadou eTuristy proto je, že zahrnuje i ubytované osoby, což je v rozporu s unijním právem. V návrhu dále chybí jasně vymezené účely zpracování osobních údajů.

Legislativa obchodních sdělení a politické reklamy

V Poslanecké sněmovně pokračuje projednávání sněmovního tisku 776, *návrh zákona o digitální ekonomice a o změně některých souvisejících zákonů*. Jeho cílem je adaptovat český právní řád na *nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách)* a rovněž transponovat *směrnici 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)*, ve znění pozdějších předpisů.

Tento návrh plně nahrazuje stávající *zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů*. Vzniká složitý ekosystém *zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)*, který reguluje elektronické komunikace, *zákona č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů*, který reguluje reklamu, *návrhu zákona o digitální ekonomice*, který reguluje obchodní sdělení, *návrhu zákona o transparentnosti a cílení politické reklamy a o změně některých souvisejících zákonů*, který reguluje politickou reklamu, a *GDPR*, které reguluje zpracování osobních údajů. V tomto kontextu je GDPR obecným předpisem pro zpracování elektronických kontaktů, tj. e-mailových adres, telefonních čísel apod. pro marketingové účely. Rovněž stanoví náležitosti souhlasu subjektu údajů s tímto zpracováním.

Počet připomínkovaných návrhů legislativních a nelegislativních materiálů v letech 2017–2024



Zákon o elektronických komunikacích se vztahuje na hlasové služby, včetně přímého marketingu uskutečňovaného prostřednictvím telefonních hovorů *(telemarketing)*. Pokud hovoříme o písemných či audiovizuálních zprávách, je třeba rozlišovat, zda jsou ukládány přímo v profilu nebo účtu uživatele, pak se jedná o *obchodní sdělení*, nebo jen zobrazovány, pak se jedná o *reklamu*. Míří-li reklama na konkrétního čtenáře, posluchače či diváka, jde o cílenou reklamu. Dozor nad přímým marketingem (kromě výše uvedeného telemarketingu, který je v působnosti Českého telekomunikačního úřadu) a cílenou reklamou je v působnosti ÚOOÚ.

Správa dat

Digitální a informační agentura (DIA) připravila adaptaci českého právního řádu na *nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat)*, prostřednictvím *návrhu zákona o správě dat a o řízeném přístupu k datům a o změně některých souvisejících zákonů* (zákon o správě dat a o řízeném přístupu k datům), který byl předložen vládě.

ÚOOÚ upozornil gestora na to, že předmětem návrhu zákona jsou vysoce riskantní zpracování osobních údajů jednak o všech občanech, jednak prakticky všechna státu nuceně poskytnutá data. Ačkoliv lze mnohé záruky implicitně dovodit, nejsou pro adresáta právního předpisu dostatečně zřetelné a měly by být formulovány výslovně. Právní předpis je pokynem zákonodárce, jak mají adresáti právního předpisu postupovat, a proto je vhodné, aby právní normy byly instruktivnější. V opačném případě zůstanou zamýšlené záruky ochrany soukromí jen na papíře.

Rodné číslo ve vztahu k identifikaci

ÚOOÚ se vyjadřoval ke spolehlivé identifikaci zákazníků nebo žadatelů. S tím souvisí *nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu*, které bude DIA v roce 2025 implementovat do českého právního řádu a které zavádí evropskou peněženku digitální identity (EUDIW) jako obecnou elektronickou identifikaci v soukromém sektoru (v ČR již dnes existuje bankovní identita).

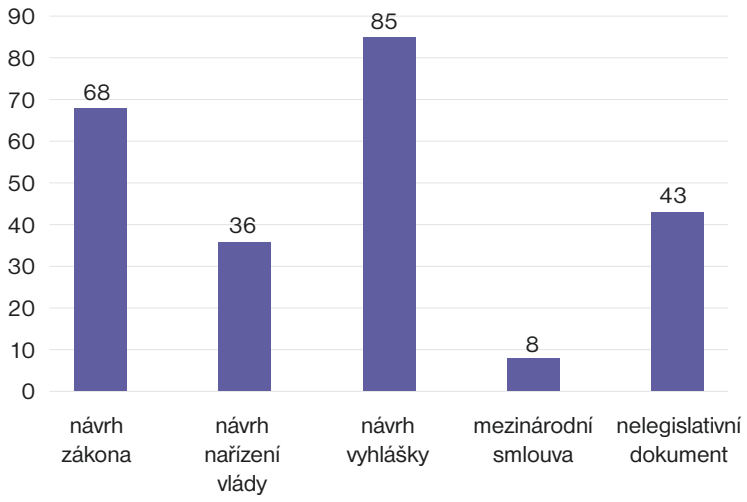
Zůstává však problém identifikace v čase (správce již má o člověku důležitá data z minulosti a potřebuje k nim přidat nová) či prostoru (pro spolehlivé předání údajů mezi různými subjekty). ÚOOÚ se stále domnívá, že pro tyto účely je rodné číslo z mnoha důvodů překonaný identifikátor, který by měl nahradit klientský identifikátor fyzické osoby (KIFO) daný speciálním zákonem pro konkrétní oblast právních vztahů, nebo obecně bezvýznamový směrový identifikátor (BSI) zavedený od 1. července 2022 v § 12a zákona č. 12/2020 Sb., o právu na digitální služby.

Formuláře žádostí v právních předpisech

Jedním z fenoménů roku 2024 bylo množství vyhlášení nejrůznějších tiskopisů či formulářů právními předpisy, ačkoliv to z povahy věci právní předpisy nejsou. Povinnost vydat formulář právním předpisem vychází z nálezu ÚS (sp. zn. Pl. ÚS 32/15), který uvádí: „*To nevylučuje případné zákonné zmocnění (čl. 79 odst. 3 Ústavy) ke stanovení konkrétních jednotlivých údajů Ministerstvem financí. Avšak muselo by se tak stát formou právního předpisu.*“ Nicméně v dané věci šlo o poměrně častá hlášení, přičemž jejich bližší vymezení v zákoně absentovalo.

V nálezu Ústavního soudu (sp. zn. Pl. ÚS 19/17) byl tento právní závěr rozšířen na formulář registrace k dani: „*V posuzované věci zákonodárce stanovil určité náležitosti a pravidla, které jsou upraveny pouze ve formuláři vydaném Ministerstvem financí, a nezmocnil Ministerstvo financí k vydání podzákonného právního předpisu. Přitom nebylo zákonodárcem určeno, jaké údaje mohou být ve formulářích požadovány.*“ Jako pozitivní příklad uvedl ÚS vyhlášku č. 79/2017 Sb., o stanovení struktury a formátu oznámení podle zákona o střetu zájmů.

Druhy připomínkovaných návrhů legislativních a nelegislativních materiálů v roce 2024



Lze tedy uzavřít, že výklad resortů, že judikatura ukládá vydávat veškeré tiskopisy či formuláře právním předpisem, je excesivní. Pokud právní předpis, optimálně zákon, stanoví kategorie osobních údajů, které se mají veřejnému úřadu předávat, je to dostačující.

Z připomínkovaných materiálů bylo nejvíce zásadních připomínek uplatněno k nedostačujícímu nebo chybějícímu posouzení vlivu na ochranu osobních údajů v návrzích.

I.9. POKYNY A STANOVISKA EDPB

Evropský sbor pro ochranu osobních údajů (EDPB) vydává nejrůznější dokumenty, přičemž významným zdrojem informací pro odbornou i laickou veřejnost jsou zejména pokyny (*guidelines*), stanoviska (*opinions*), rozhodnutí (*decisions*) a doporučení (*recommendations*). Cílem je usnadnit porozumění zákonným požadavkům GDPR a podpořit jejich jednotné uplatňování.

Pokyny

V roce 2024 EDPB schválil následující pokyny:

- **Pokyny 2/2023 k technickému rozsahu čl. 5(3) směrnice 2002/58/ES.** Důvodem revize pokynů bylo zavádění nových sledovacích metod, které jednak nahrazují dosavadní prostředky (například cookies) a jednak vytváří nové obchodní modely. U některých sledovacích metod (typicky cookies) je uplatnitelnost čl. 5 odst. 3 směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích, ePD) dobře řešena, v případě nově se objevujících nástrojů sledování se ukázala potřeba řešení určitých nejasností. Pokyny identifikují a analyzují tři klíčové prvky pro použitelnost čl. 5 odst. 3 ePD, konkrétně „informace", „koncové zařízení účastníka nebo uživatele" a „získávání přístupu a ukládání informací a uložených informací". Pokyny byly EDPB schváleny dne 14. listopadu 2023 a postoupeny do veřejné konzultace, která byla ukončena 18. ledna 2024. Následně byla vypracována aktualizovaná verze pokynů.

- **Pokyny 01/2023 k čl. 37 trestněprávní směrnice.** Plenární zasedání EDPB v září 2023 jednomyslně přijalo pokyny k výkladu čl. 37 LED. Členové EDPB se současně dohodli, že pokyny předloží k veřejné konzultaci po dobu 6 týdnů, počínaje 27. zářím 2023 a konče 8. listopadu 2023. V souladu s úkoly svěřenými EDPB v čl. 51 LED podávají pokyny výklad EDPB týkající se závazného právního rámce vztahujícího se na předávání údajů do třetích zemí, kdy by při výkladu práva měly být zohledněny praktické potřeby a podmínky, avšak závazné právní požadavky stanoví pro takový výklad meze, které je třeba dodržovat.

Další pokyny byly v roce 2024 předloženy do veřejné konzultace a budou schvalovány v roce 2025.

- **Pokyny 1/2024 ke zpracování osobních údajů podle čl. 6 odst. 1 písm. f) GDPR.** Pokyny byly zpracovávány od roku 2020. V této fázi je ukončena veřejná konzultace. První část obsahuje úvod k čl. 6 odst. 1 písm. f) GDPR jakožto právnímu základu. Druhá část nabízí analýzu prvků, které mají být správcem vzaty v úvahu při posuzování uplatnitelnosti čl. 6 odst. 1 písm. f) GDPR na dané zpracování. Třetí část ilustruje vztah existující mezi čl. 6 odst. 1 písm. f) GDPR a několikerými právy subjektu údajů (právo na informace, právo na přístup, právo námitky, právo na výmaz atd.). Ve čtvrté části je popis některých konkrétních kontextů, ve kterých se lze opřít o čl. 6 odst. 1 písm. f) GDPR.

- **Pokyny 2/2024 k čl. 48 GDPR.** Pokyny objasňují, že rozhodnutí soudů nebo správních orgánů třetích zemí, které vyžadují přenos nebo zpřístupnění osobních údajů, mohou být uznána nebo vykonatelná pouze na základě mezinárodní dohody, jako je smlouva o vzájemné právní pomoci, platné mezi požadující třetí zemí a EU nebo členským státem. Zabývají se výhradně dopadem čl. 48 GDPR na soukromé společnosti v roli správ-

ce či zpracovatele. Základním východiskem pokynů je výklad, že čl. 48 GDPR má pouze deklaratorní, vysvětlující význam a neukládá soukromým subjektům žádnou novou povinnost, protože adresátem tohoto mezinárodněprávního ustanovení nejsou a nemohou být soukromé společnosti, ale vlastní členské státy EU. Podstata výkladu čl. 48 GDPR spočívá v tom, že v každém případě musí správce/zpracovatel předání realizovat v souladu s GDPR, tzn. musí provést dvoustupňový test: mít pro předání právní titul podle čl. 6 GDPR a mít nástroj k předávání podle kapitoly V. GDPR.

Stanoviska

Podle čl. 64 odst. 2 GDPR může kterýkoli dozorový orgán, předseda EDPB nebo Evropská komise požádat EDPB o vydání stanoviska k záležitostem s obecným uplatněním nebo s účinky ve více než jednom členském státě EU. Cílem je zajistit jednotné uplatňování pravidel GDPR napříč členskými státy.

V minulém roce byla přijata stanoviska podle čl. 64 odst. 2 GDPR v následujících případech:

- **Stanovisko 08/2024, o platném souhlasu v kontextu modelů *consent or pay* (souhlas, nebo zaplať) implementovaných velkými online platformami.** EDPB ve svém stanovisku uvedl, že model *consent or pay* používaný velkými online platformami, kde uživatelé musí buď souhlasit se zpracováním osobních údajů pro behaviorální reklamu, nebo zaplatit poplatek, většinou nesplňuje požadavky na svobodný souhlas. Pohlíželo se na celkový účinek na subjekt údajů, nikoliv na pouhé formální požadavky souhlasu. EDPB zdůrazňuje, že osobní údaje nejsou obchodovatelnou komoditou a že by platformy měly nabídnout skutečnou alternativu, která nevyžaduje platbu ani zpracování osobních údajů pro behaviorální reklamu. Toto stanovisko má za cíl zajistit, aby ochrana osobních údajů zůstala základním právem a nebyla obchodovatelnou komoditou. Stanovisko bude dále rozpracováno v pokynech EDPB.

- **Stanovisko 11/2024, o použití rozpoznávání obličeje ke zjednodušení toku cestujících na letištích [kompatibilita s čl. 5 odst. 1 písm. e) a f), 25 a 32 GDPR]** se zabývá použitím technologie rozpoznávání obličeje (FRT) na letištích provozovateli letišť a leteckými společnostmi pro zefektivnění toku cestujících, přičemž se zaměřuje na dodržování požadavků GDPR. EDPB zdůrazňuje, že cestující musí mít maximální kontrolu nad svými biometrickými údaji, což znamená, že biometrické šablony by měly být ideálně uloženy lokálně na zařízení cestujícího a dešifrovací klíče by měly být také pod jejich kontrolou. Stanovisko také zdůrazňuje důležitost implementace ochrany soukromí již od návrhu a ve výchozím nastavení, což znamená, že opatření na ochranu dat by měla být integrována do zpracovatelských aktivit od samého počátku. Musí být zavedena adekvátní bezpečnostní opatření na ochranu biometrických údajů, včetně šifrování a minimalizace doby uchovávání údajů. Použití FRT musí být nezbytné a přiměřené zamýšlenému účelu, přičemž by měly být zváženy méně invazivní alternativy. Účelem stanoviska je zajistit, aby nasazení technologie rozpoznávání obličeje na letištích respektovalo soukromí cestujících a bylo v souladu s GDPR.

- **Stanovisko 04/2024, o pojmu hlavní provozovny správce v Unii podle čl. 4 odst. 16 písm. a) GDPR.** EDPB zde objasňuje kritéria pro určení hlavní provozovny správce nebo zpracovatele v EU, což je klíčové pro uplatnění mechanismu jednotného kontaktního místa podle GDPR. Stanovisko zdůrazňuje, že hlavní sídlo správce musí být mís-

tem, kde se přijímají rozhodnutí o účelech a prostředcích zpracování osobních údajů a kde je zajištěna jejich implementace. Správci musí poskytnout důkazy, že jejich hlavní provozovna v EU tato rozhodnutí přijímá a má pravomoc je implementovat. Dozorové orgány mohou zpochybnit tvrzení správce o hlavní provozovně na základě objektivního zkoumání relevantních faktů. Pokud jsou tato rozhodnutí přijímána mimo EU, nelze toto místo považovat za hlavní sídlo podle čl. 4 odst. 16 písm. a) GDPR a mechanismus jednotného kontaktního místa by se neměl uplatňovat.

- **Stanovisko 22/2024, o určitých povinnostech vyplývajících při angažování zpracovatelů a dílčích zpracovatelů** se zaměřuje na situace, kdy správci spoléhají na jednoho nebo více zpracovatelů nebo dílčích zpracovatelů, a řeší osm otázek týkajících se povinností správců a formulací smluv mezi správci a zpracovateli. Správci musí zajistit, že zpracovatelé a dílčí zpracovatelé poskytují dostatečné záruky pro implementaci vhodných technických a organizačních opatření, jak vyžaduje čl. 28 GDPR, a jsou odpovědní za ověření těchto záruk. Správci musí mít vždy k dispozici informace o identitě všech zpracovatelů a podzpracovatelů. Konečné rozhodnutí o zapojení (dílčího) zpracovatele zůstává na správci. Správci nemají povinnost systematicky kontrolovat zpracovatelské smlouvy s dílčími zpracovateli, ale měli by posoudit, zda je kontrola nutná pro prokázání souladu s GDPR. Při přenosech osobních údajů mimo EU by měl zpracovatel jako vývozce údajů připravit příslušnou dokumentaci, kterou správce posoudí a předloží příslušnému úřadu pro ochranu osobních údajů.

- **Stanovisko 28/2024, k používání osobních údajů při vývoji a zavádění modelů umělé inteligence** se zaměřuje na několik klíčových otázek. Jednou z nich je anonymita. Model je považován za anonymní, pokud je velmi nepravděpodobné, že by osoby, jejichž údaje byly použity, mohly být identifikovány, nebo že by jejich údaje mohly být z modelu extrahovány. Posuzování, zda jsou modely umělé inteligence anonymní, by mělo být prováděno případ od případu. Stanovisko obsahuje nezávazný a neúplný seznam metod k prokázání anonymity. Stanovisko také poskytuje obecné úvahy pro posouzení, zda je oprávněný zájem vhodným právním základem pro zpracování osobních údajů v AI modelech. EDPB se dále zabývá situacemi, kdy byl model vyvinut s nezákonně zpracovanými osobními údaji. V takových případech může být ovlivněna zákonnost jeho zavedení, pokud model nebyl řádně anonymizován. Kromě toho stanovisko obsahuje kritéria pro posouzení očekávání jednotlivců ohledně použití jejich osobních údajů a příklady zmírňujících opatření, která mohou omezit negativní dopady na jednotlivce. Při přípravě stanoviska uspořádal EDPB akci pro zúčastněné strany a vyměnil si názory s unijním Úřadem pro AI (*AI Office*).

I.10. PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Revize rozhodnutí Komise o odpovídající ochraně

Rok 2024 lze s trochou nadsázky označit jako období, ve kterém byly potvrzeny význam a efektivita institutu rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů podle čl. 45 obecného nařízení. *Zprávou Komise o prvním přezkumu fungování rozhodnutí o odpovídající ochraně přijatých podle čl. 25 odst. 6 směrnice 95/46/ES* završila Evropská komise

v lednu 2024 svou práci na hodnocení všech jedenácti starých rozhodnutí o odpovídající úrovni vydaných ještě před účinností obecného nařízení, čímž splnila povinnost stanovenou jí čl. 97 odst. 2 písm. a) obecného nařízení. Komise hodnotila vývoj právního rámce ochrany osobních údajů v každé ze zmíněných zemí (Andorra, Argentina, Kanada, Faerské ostrovy, Guernsey, Ostrov Man, Izrael, Jersey, Nový Zéland, Švýcarsko, Uruguay), a to včetně pravidel upravujících přístup orgánů veřejné moci těchto zemí k osobním údajům.

Intenzivní dlouhodobá komunikace Komise s dotčenými státy vedla přitom k tomu, že v průběhu procesu hodnocení samotné státy modernizovaly své právní předpisy, aby odpovídaly zvýšeným standardům ochrany osobních údajů. Díky tomuto vstřícnému dialogu mohla ve výsledku Komise konstatovat, že každá z uvedených jedenácti zemí a území nadále zajišťuje odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie ve smyslu čl. 45 obecného nařízení.

Rámec ochrany soukromí mezi EU a USA

V červenci 2024, v souladu se zněním prováděcího rozhodnutí Komise 2023/1975 o odpovídající úrovni ochrany osobních údajů poskytované Rámcem ochrany soukromí mezi EU a USA (*Data Privacy Framework*, DPF), proběhlo první společné hodnocení fungování DPF. Hodnocení se z evropské strany vedle zástupců Komise zúčastnili i zástupci Sboru.

Ze strany Spojených států amerických to byli především zástupci Ministerstva obchodu (*Department of Commerce*, DoC) a Federální obchodní komise (*Federal Trade Commission*, FTC), kteří doložili, že certifikační proces společností, které se zúčastní programu DPF, byl ze strany DoC a FTC plně implementován včetně několika způsobů vyřizování stížností a žádostí o odškodnění. Dále se hodnocení účastnili také zástupci amerických státních orgánů, kteří prokázali, že všechny prvky stížnostních a odvolacích procedur ve věci přístupu tamních orgánů k evropským osobním údajům, jak jsou zakotveny v prováděcím rozhodnutí Komise 2023/1975, byly uvedeny v život, a to včetně jmenování osmi soudců a dvou zvláštních advokátů zvláštního odvolacího soudu pro tyto stížnosti (*Data Protection Review Court*).

Tyto pozitivní skutečnosti tak mohla ocenit jak Zpráva Komise, tak i Zpráva Sboru, které ovšem obě upozorňují na skutečnost, že s ohledem na zanedbatelný počet dosud podaných stížností nebyly implementované postupy dosud ověřeny v praxi. Dále obě zprávy konstatují, že by bylo vhodné, aby DoC a FTC prováděly proaktivní kontroly DPF certifikovaných společností *ex officio*, aby vypracovaly přehledné pokyny DPF, v nichž by důsledně osvětlily zásady pro další předání (*onward transfers*) a sjednotily výklad toho, co se rozumí „zpracováním HR dat“ podle DPF.

Dopad rozhodnutí Evropského inspektora ochrany údajů (EDPS) na používání cloudových nástrojů

Událostí, která v roce 2024 vyvolala v oblasti předávání osobních údajů do třetích zemí největší rozruch a obavy správců, bylo *rozhodnutí Evropského inspektora ochrany údajů ze dne 8. března 2024 týkající se jeho šetření používání Microsoft 365 Evropskou komisí ve věci 2021–0518*. EDPS v tomto rozhodnutí konstatoval, že Evropská komise při používání cloudových nástrojů Microsoft 365 porušuje *nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES*.

Pokud převedeme zjištění EDPS do povinností podle obecného nařízení, tak Evropská komise podle těchto zjištění při používání nástrojů Microsoft 365 pro zpracování osobních údajů porušila základní zásadu odpovědnosti odpovídající čl. 5 odst. 2 obecného nařízení a zároveň zásady účelového omezení, minimalizace údajů a zákonnosti, korektnosti a transparentnosti odpovídající čl. 5 odst. 1 písm. a), b) a c) obecného nařízení, protože nestanovila účely zpracování osobních údajů, ani kategorie osobních údajů, které mají být v rámci daného zpracování zpracovávány.

Výše uvedené základní porušení zásady odpovědnosti se pak zároveň také zákonitě přeneslo do porušení povinností správce při předávání osobních údajů mimo Evropskou unii, resp. EHP, kdy zpracovatelská smlouva, konkrétně meziinstitucionální licenční dohoda uzavřená roku 2021 se společností Microsoft Ireland, přestože její součástí byly standardní smluvní doložky podle rozhodnutí Komise, neobsahovala všechny povinné náležitosti odpovídající čl. 44 a čl. 46 obecného nařízení, poněvadž neobsahovala dostatečné vymezení účelů zpracování a typů zpracovávaných osobních údajů. Evropský inspektor konstatoval i absenci relevantního *Transfer Impact Assessmentu*, tj. vyhodnocení ze strany vývozce údajů, zda zvolený nástroj pro předání osobních údajů odpovídající některému z nástrojů podle čl. 46 obecného nařízení opravdu poskytne předaným údajům v zásadě rovnocennou ochranu, nebo zda je nezbytné přijmout dodatečná opatření.

Zjištění Evropského inspektora a jím uložená nápravná opatření nelze interpretovat tím způsobem, že by se změnily nebo zpřísnily podmínky používání nástrojů Microsoft 365, a to ani pro entity, které zpracovávají osobní údaje v režimu obecného nařízení.

Dále lze konstatovat, že v případě předávání osobních údajů společnosti Microsoft Corporation do Spojených států amerických v současné době probíhá předávání v režimu čl. 45 obecného nařízení, neboť společnost Microsoft Corporation je účastníkem programu Rámec ochrany soukromí, který poskytuje odpovídající úroveň ochrany podle čl. 45 obecného nařízení na základě prováděcího rozhodnutí Komise 2023/1975. Nakonec je třeba upozornit na skutečnost, že od rozhodnutí EDPS se odvolala k Tribunálu EU jak Evropská komise (případ T-262/24), tak i společnost Microsoft Ireland Operations Ltd. (případ T-265/24).

Výhledy

V roce 2025 bude s největší pravděpodobností završena práce Komise a Sboru na nových standardních smluvních doložkách pro předávání osobních údajů do třetích zemí entitám, jejichž zpracování osobních údajů podléhá obecnému nařízení podle čl. 3 odst. 2 tohoto nařízení.

I.11. SCHENGENSKÁ SPOLUPRÁCE

Dohled nad informačními systémy

Stejně jako v předchozích letech, také v roce 2024 plnil Úřad roli vnitrostátního dozorového orgánu, kterému přísluší dohled nad zpracováním osobních údajů v rozsáhlých evropských informačních systémech provozovaných v rámci schengenské spolupráce. V této roli Úřad dohlíží na dodržování příslušných právních předpisů a napomáhá k ochraně zá-

kladních práv a svobod osob, jejichž údaje jsou v takových systémech zpracovávány. Konkrétně jde o Schengenský informační systém (SIS), jehož nová, již třetí generace byla spuštěna 7. března 2023, a dále o 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 a v průběhu roku se připravoval na svou roli dozorového orgánu ve vztahu k připravovanému Systému vstupu/výstupu (EES), jenž však oproti původním předpokladům nebyl v roce 2024 spuštěn.

ÚOOÚ v rámci dohledu nad shora uvedenými informačními systémy v roce 2024 provedl kontrolu u Ministerstva vnitra ČR, a to v souvislosti se zpracováním osobních údajů v Schengenském informačním systému. Při kontrole se Úřad v návaznosti na dvě přijaté stížnosti zaměřil též na postupy v oblasti konzultačních řízení. Konzultační řízení jsou procesním institutem, při kterém dochází k výměně informací mezi členskými státy. Cílem těchto řízení je zabránit situacím, kdy by cizinec, který má pobytové oprávnění v členském státě, byl zároveň veden v SIS jako osoba, která nemůže v schengenském prostoru pobývat na základě záznamu jiného členského státu. V rámci kontroly byly sice shledány dílčí nedostatky (konkrétní technické problémy), nebyly však vyhodnoceny jako porušení právních předpisů v oblasti ochrany osobních údajů.

Kontrola cílená na zpracování osobních údajů v souvislosti se Schengenským informačním systémem byla Úřadem v souladu s kontrolním plánem pro rok 2024 zahájena též u Policie ČR, a to se zaměřením na činnosti cizinecké policie. Úřad v této kontrole provedl dvě ústní jednání a místní šetření, kdy jedno z nich bylo realizováno též v prostorách Letiště Václava Havla Praha.

Úřad dále provedl kontrolu Celního informačního systému, a to u Generálního ředitelství cel. Účelem tohoto informačního systému je napomáhat příslušným orgánům členských států při předcházení, vyšetřování nebo stíhání případů porušení celních nebo zemědělských předpisů EU tím, že zvyšuje účinnost postupů spolupráce a kontrolních postupů rychlou distribucí údajů a informací. Kontrolou nebyla zjištěna žádná porušení povinností při zpracování osobních údajů v Celním informačním systému. Úřad nicméně konstatoval několik dílčích nedostatků, zejména že některé interní předpisy kontrolované osoby a také některé z informací poskytovaných veřejnosti plně nereflektovaly aktuální organizační strukturu a platnou a účinnou právní úpravu. Již v rámci kontroly však Generální ředitelství cel přijímalo některá opatření k zajištění aktuálnosti a souladu.

Po námitkách byla v roce 2024 též ukončena kontrola prováděná u Ministerstva zahraničních věcí, jejímž předmětem bylo zpracování osobních údajů ve Vízovém informačním systému a při vyřizování žádostí o krátkodobá (schengenská) víza, která jsou jedním z prvků společné politiky Evropské unie. V rámci této kontroly Úřad realizoval místní šetření na Velvyslanectví České republiky v Astaně a Velvyslanectví České republiky v Abú Dhabí a v jimi využívaných vízových centrech externího poskytovatele služeb, přičemž Úřad o svých zjištěních v této věci již informoval ve své výroční zprávě za rok 2023.

V kontrolní činnosti zaměřené na zpracování osobních údajů ve Vízovém informačním systému a při vízovém procesu na zastupitelských úřadech České republiky v zahraničí pokračoval Úřad i v roce 2024. V této souvislosti byla zahájena kontrola, v jejímž rámci

bylo realizováno místní šetření na Velvyslanectví České republiky v Novém Dillí a v příslušném vízovém centru tamtéž.

Úřad je ze své pozice příslušný také k vyřizování podání souvisejících se zpracováním osobních údajů ve zmíněných informačních systémech. V roce 2024 Úřad obdržel a vyřídil celkem 34 podnětů týkajících se SIS (stížnosti, žádosti o konzultaci či o přístup k osobním údajům, jejich opravu či výmaz) a také dvě podání vztahující se ke zpracování osobních údajů ve VIS (stížnost a žádosti o konzultaci, resp. opravu a výmaz). Z hlediska ostatních systémů nebyla žádná podání učiněna.

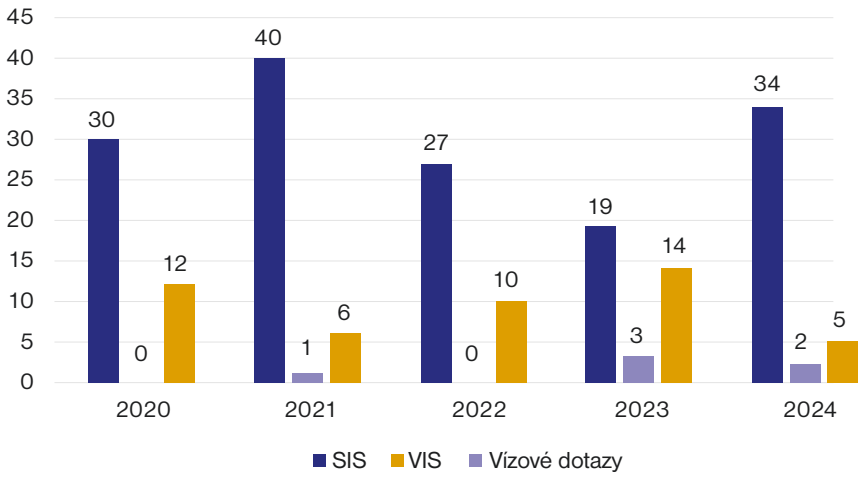
Úřadu bylo v roce 2024 doručeno 5 dotazů týkajících se vízové problematiky. Tyto dotazy byly, stejně jako v předchozích letech, Úřadu adresovány i přesto, že vízová politika České republiky není v jeho působnosti. Ve všech případech Úřad jednotlivým žadatelům objasnil své zákonné kompetence a poskytl relevantní informace a kontaktní údaje na příslušné orgány s cílem pomoci žadatelům s řešením jejich životní situace. Přestože jsou ÚOOÚ výše uvedená podání často zasílána také v anglickém, ukrajinském či ruském jazyce, Úřad se vždy žadatelům snaží poskytnout všechny potřebné informace v pro ně srozumitelné podobě.

Při své činnosti související se schengenskou agendou Úřad spolupracuje s dozorovými úřady ostatních členských států a také s Evropským inspektorem ochrany údajů (EDPS), s nimiž se pravidelně setkává v rámci tří koordinačních skupin a v rámci výboru pro koordinovaný dozor. V roce 2024 se zástupci ÚOOÚ zúčastnili všech 13 uskutečněných jednání.

Schengenské evaluace

Za další formu schengenské spolupráce lze považovat hodnotící a monitorovací mechanismus k ověření uplatňování tzv. schengenské evaluace, při kterých je v jednotlivých členských státech vyhodnocován soulad s evropským právem v oblastech jako 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 hodnotitelé pro oblast ochrany osobních údajů byli Evropskou komisí zařazeni do skupiny expertů a jeden z nich byl zároveň vybrán pro konkrétní evaluaci. Zástupkyně ÚOOÚ tak byla členem hodnotícího týmu pro evaluaci Maďarska a osobně se účastnila šetření, realizovaného v Maďarsku v červnu 2024. Z hlediska schengenských evaluací byl pro Úřad významný zejména listopad 2024, kdy bylo náročné šetření hodnotícího týmu realizováno v České republice. Závěry tohoto šetření, resp. celé evaluace, jsou očekávány v roce 2025.

Počty vyřízených podání



I.12. EVROPSKÁ A ZAHRANIČNÍ SPOLUPRÁCE

Evropský sbor pro ochranu osobních údajů

Úřad je členem Evropského sboru pro ochranu osobních údajů (EDPB), který byl ustaven podle čl. 68 GDPR. EDPB vydává i stanoviska a písemná vyjádření podle vyžádání různých veřejných institucí, například Evropské komise nebo Evropského parlamentu, a spolupracuje s Evropským inspektorem ochrany údajů (EDPS).

Jednání s bavorským zemským komisařem pro ochranu osobních údajů, Praha 11. 4. 2024

ÚOOÚ se podílí na řadě aktivit EDPB, zejména během přípravy odborných dokumentů, jako jsou nejrůznější pokyny, doporučení, stanoviska a rozhodnutí. Zástupce ÚOOÚ se účastnil všech 12 plenárních zasedání EDPB, z nichž 5 proběhlo prezenčně v Bruselu a zbývající se uskutečnily online. Vedle pléna jakožto vrcholného orgánu jsou v rámci EDPB ustaveny tematicky specializované pracovní odborné skupiny (*expert subgroups*), složené z odborníků nominovaných členskými úřady. V roce 2024 ÚOOÚ delegoval své odborné pracovníky do tří dalších odborných skupin.

Z celkového počtu 12 pracovních odborných skupin EDPB má nyní Úřad svého delegáta v 11 z nich. Jsou to: Strategické poradenství (*Strategic Advisory*), Spolupráce (*Cooperation*), Technologie (*Technology*), Hranice, cestování a prosazování práva (*Borders, Travel and Law Enforcement*), Mezinárodní převody (*International Transfers*), Klíčová ustanovení (*Key Provisions*), Prosazování práva *(Enforcement*), IT uživatelé IT (*IT Users*), Sociální média (*Social Media*), Právní soulad, e-government a zdravotnictví (*Compliance, E-Government and Health*) a Finanční záležitosti (*Financial Matters*).

Během roku 2024 se v odborných skupinách se zastoupením ÚOOÚ uskutečnilo asi 120 pracovních schůzí, přičemž účast delegátů Úřadu dosáhla přibližně 75 %. EDPB v rámci

svého programu podpory stáží pro rok 2025 schválil vyslání zaměstnankyně ÚOOÚ na třítýdenní stáž k partnerskému dozorovému úřadu v Estonsku. Recipročně ÚOOÚ přijme na tři týdny stážistu z německého spolkového dozorového úřadu a stážistku z nizozemského dozorového úřadu.

Pracovní návštěva bavorského zemského komisaře pro ochranu osobních údajů, Praha 11. 4. 2024

Mechanismus spolupráce

Spolupráci mezi dozorovými úřady v dozorové a konzultační oblasti upravuje GDPR. K podpoře této spolupráce úřady využívají elektronický Systém pro výměnu informací o vnitřním trhu (*Internal Market Information System,* IMI).

Nejčastějším typem spolupráce je postup podle čl. 61 GDPR, **vzájemná dobrovolná spolupráce**, která není striktně povinná a umožňuje méně formální přístup. Tento postup je uplatňován pro vzájemné konzultace, předávání důležitých informací o konkrétních případech a vedených šetřeních, nebo pro výměnu informací, u nichž se předpokládá, že budou přínosné a využitelné i pro ostatní úřady. Během roku 2024 bylo do systému IMI vloženo přibližně 300 žádostí o dobrovolnou spolupráci podle čl. 61 GDPR, jejichž adresátem byl kromě jiných dozorových úřadů také ÚOOÚ. Sám Úřad do systému vložil 28 žádostí.

Druhou nejpoužívanější formou spolupráce je **mechanismus jediného kontaktního místa** (*one-stop-shop*). Uplatňuje se při šetření přeshraničních případů, kdy zpracování osobních údajů probíhá ve více členských zemích EU, anebo tímto zpracováním mohou být dotčeny subjekty údajů sídlící ve více členských státech. V takových situacích je nejprve postupem podle čl. 56 GDPR stanoven vedoucí dozorový úřad, který se stane jediným kontaktním místem a vede šetření konkrétního případu, přičemž spolupracuje s dotčenými dozorovými úřady podle čl. 60 GDPR. ÚOOÚ na základě obdržených podnětů inicioval celkem 15 procedur podle čl. 56 GDPR, kdy navrhl některý zahraniční dozorový úřad, aby se věcí zabýval z pozice vedoucího dozorového úřadu. Naopak do této role byl ÚOOÚ navržen v 15 případech a ve všech roli vedoucího dozorového úřadu přijal.

Rada Evropy

Zástupkyně ÚOOÚ se zúčastnila červnového plenárního zasedání Poradního výboru Rady Evropy pro Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat (T-PD) ve francouzském Štrasburku. V návaznosti na *Vzorové smluvní doložky pro přeshraniční toky osobních údajů pro předávání údajů mezi správci* (Module 1) a *mezi správcem a zpracovatelem* (Module 2), které byly přijaty v loňském roce, výbor schválil a publikoval *Vzorové smluvní doložky pro předávání osobních údajů mezi zpracovateli* (Module 3). Výbor dále mimo jiné schválil a publikoval Pokyny ke zpracování osobních údajů v rámci hlasování a voleb.

Global Privacy Assembly

V pořadí 46. výroční konference Světového shromáždění pro ochranu soukromí *Global Privacy Assembly* (GPA) se uskutečnila ve dnech 31. října – 1. listopadu 2024 na ostrově Jersey. Jejím mottem byla *Síla informací*. Konference schválila pět usnesení: *O pravidlech a postupech GPA*, *O zásadách zpracování osobních údajů v neurovědách a neurotechnologiích*, *Usnesení, jímž se schvaluje a podporuje používání mechanismů pro vydávání osvědčení o ochraně údajů*, *O volném toku dat s důvěrou a účinné regulaci globálních datových toků* a *O sledování a ochraně práva jednotlivců na soukromí*.

Konference evropských dozorových úřadů

Každoroční Evropskou konferenci úřadů pro ochranu osobních údajů, tzv. Jarní konferenci (*The Spring Conference of European Data Protection Authorities*), hostil lotyšský dozorový úřad v Rize ve dnech 14. – 16. května 2024. Jednalo se o 32. ročník za účasti dozorových úřadů z EU a EHP. ÚOOÚ byl na akci zastoupen dvěma delegáty. Během konference byla probírána role dozorových úřadů v době rozvoje digitálních technologií a inovací, otázky regulace těchto technologií při respektování zásad ochrany osobních údajů, problematika vztahu GDPR a předpisů na ochranu proti praní špinavých peněz (AML). Diskutována byla také relevantní evropská a mezinárodní judikatura. Delegáti schválili *Rezoluci o posílení spolupráce a ustavení pracovních skupin pro dozorové úřady v oblasti ochrany osobních údajů*.

Praktické školení k auditům mobilních aplikací

Druhý ročník praktického školení, organizátory zvaného „bootcamp", proběhl v Bruselu ve dnech 18. – 19. září 2024 a byl věnován auditům mobilních aplikací. Také letos se akce zúčastnil odborník Úřadu. Toto odborné školení je zaměřeno primárně na technické aspekty kontrolní činnosti. Přineslo cenné poznatky zejména z oblasti analýzy souladu internetových stránek a mobilních aplikací, se zaměřením na konkrétní postupy při jejich kontrole. Potvrdilo se, že analýzy prováděné Úřadem jsou plně v souladu s evropskou praxí, přičemž používané metody lze označit za efektivní a prakticky aplikovatelné.

Bilaterální aktivity

Ve dnech 4. – 5. ledna 2024 byla v Praze na pracovní návštěvě ÚOOÚ místopředsedkyně *Úradu pre ochranu osobních údajov Slovenskej republiky*. Hlavními tématy rozhovorů s předsedou Úřadu byla příprava schengenského hodnocení, které mělo zakrátko proběhnout v obou zemích, zhodnocení pětileté zkušenosti a poznatků s praktickým uplatňováním GDPR a výměna zkušeností z dozorové činnosti.

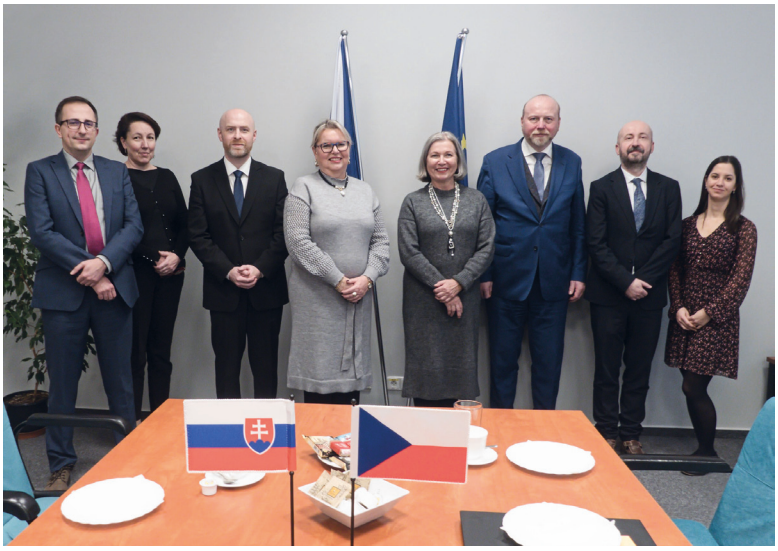
Ve dnech 11. – 12. dubna 2024 přijal předseda Úřadu v Praze delegaci z bavorského zemského dozorového úřadu (*Bayerische Landesbeauftragte für den Datenschutz*) vedenou jejím předsedou. Obě strany měly příležitost vyměnit si své zkušenosti a poznatky s prosazováním GDPR a také tzv. trestněprávní směrnice. Z konkrétních témat stojí za zmínku metodologie kontroly policejních databází, používání souborů cookies veřejnými institucemi, procesní aspekty provádění kontrol a činnost v rámci pracovních formací EDPB, především Skupiny pro strategické poradenství.

Koncem května 2024 proběhlo v sídle ÚOOÚ dvoudenní pracovní setkání s delegací nizozemského dozorového úřadu *Autoriteit Persoonsgegevens*, které se stalo důležitým milníkem v prohlubování mezinárodní spolupráce mezi oběma dozorovými orgány. V rámci

setkání proběhly odborné diskuse, týkající se zejména výzev spojených s dozorem nad zpracováním osobních údajů v digitálním prostředí. Úřad prezentoval inovativní technická řešení v rámci posuzování internetových stránek, v konstruktivní a kolegiální atmosféře byly podrobně probírány postupy a možnosti optimalizace prováděných analýz. Diskuse se soustředila na tři klíčové oblasti: kontrolu používání cookies, zpracování osobních údajů na sociálních sítích a model *consent or pay*.

Setkání zástupců dozorových úřadů z Rakouska, Maďarska, Česka, Slovenska a Slovinska

Ve dnech 11. – 13. září 2024 se na pozvání rakouského dozorového úřadu (*Datenschutzbehörde*) uskutečnilo ve Vídni dvoudenní jednání zástupců vedení úřadů pro ochranu osobních údajů. Úřady účastnických zemí mají srovnatelnou velikost i obdobné problémy. Diskutovány byly hlavně otázky vnitřní organizace úřadů, rozpočtového a personálního zajištění činnosti, spolupráce na evropské úrovni a rozšiřování kompetencí o svobodný přístup k informacím či digitální agendy.



Pracovní setkání s místopředsedkyní Úradu pre ochranu osobných údajov Slovenskej republiky, Praha 5. 1. 2024

European Blockchain Sandbox

V roce 2024 se Úřad zapojil do činnosti platformy *European Blockchain Sandbox*, která sdružuje národní i unijní regulační a dozorové orgány spolu s poskytovateli inovativních blockchainových řešení. Jedná se o kontrolované prostředí, ve kterém mohou vývojáři a společnosti testovat a implementovat svá řešení založená na blockchainu (technologie, která umožňuje bezpečnou a transparentní evidenci dat a transakcí) v souladu s platnými právními předpisy. Cílem je vytvořit jednotný evropský rámec pro diskusi o regulaci blockchainových technologií, zejména nalézt vhodné právní a regulační přístupy v prostředí, kde je možné otevřeně identifikovat možné problémy a navrhovat jejich řešení. Prostřednictvím těchto dialogů ÚOOÚ pomáhá rozpoznat a vyhodnocovat rizika spojená s implementací blockchainových aplikací z pohledu ochrany osobních údajů, především ve vztahu k požadavkům GDPR.

Předávání osobních údajů do třetích zemí

Úřad se aktivně účastní řešení problematiky předávání osobních údajů do třetích zemí v EDPB, a to především v rámci skupiny pro předávání *(International Transfers Subgroup*). Tato odborná skupina pracuje průběžně, 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 intencích koordinační procedury (WP263) mají zajistit, aby do procedury podle čl. 64 odst. 1 písm. f) obecné-

Společné jednání odborníků nizozemského a českého dozorového úřadu, Praha 30. 5. 2024

ho nařízení byly přijímány pouze již dobře propracované návrhy. Úřad se v roce 2024 zapojil do hodnocení jednotlivých návrhů závazných podnikových pravidel vypracovaných konkrétními skupinami podniků. Ve 2 případech ÚOOÚ vykonával roli spoluhodnotitelského úřadu (Accenture BCR-P, Aramex BCR-C). V 5 případech se Úřad jako spolureportér podílel na formulaci vlastního stanoviska EDPB k návrhu závazných podnikových pravidel (Accenture BCR-P, MAPFRE BCR-C, Avature BCR-P, Avature BCR-C, FCC BCR-C).

V rámci implementace prováděcího rozhodnutí Komise 2023/1975 o odpovídající úrovni ochrany osobních údajů poskytované Rámcem ochrany soukromí mezi EU a USA (*Data Privacy Framework*, DPF) se Úřad podílel na formulaci procedurálních pravidel vyřizování stížností podaných k tzv. Neformálnímu panelu evropských dozorových úřadů (*Informal Panel*, který je v souladu s US-EU *Data Privacy Framework* kompetentní pro stížnosti na zpracování personalistických dat) a procedurálních pravidel vyřizování stížností na přístup k osobním údajům ze strany zpravodajských služeb Spojených států.

II. Svobodný přístup k informacím

ÚOOÚ vykonává působnost vyplývající ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve třech oblastech: **je nadřízeným orgánem** těch povinných subjektů, jejichž nadřízený orgán nelze určit podle § 178 správního řádu, **je přezkumným orgánem** a **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. Tyto pravomoci Úřad vykonává od 2. ledna 2020. Po nabytí účinnosti novely zákona č. 106/1999 Sb. z roku 2022 se významně rozšířil okruh povinných subjektů, k nimž nově přibyly veřejné podniky. Úřad se tak stal nadřízeným orgánem další poměrně velké skupiny povinných subjektů, které jsou kromě jiného nadány veřejnými subjektivními právy, jež mohou aktivně hájit ve správním soudnictví.

Oblast svobodného přístupu k informacím dlouhodobě trpí absencí jasného určení příslušného ústředního orgánu státní správy. ÚOOÚ tímto ústředním orgánem státní správy není, neboť mu jsou v této oblasti svěřeny pouze dílčí kompetence ve stanoveném rozsahu. Úřad rovněž nemá žádný praktický vliv na připravované změny zákona č. 106/1999 Sb. a je tak oprávněn pouze vykládat příslušné právní předpisy v rámci individuálního správního rozhodování. Své právní názory na legislativu a další důležité otázky spojené se svobodným přístupem k informacím se Úřad snaží prezentovat alespoň jinými cestami. Děje se tak formou odborných seminářů určených například pověřencům pro ochranu osobních údajů či prostřednictvím účasti zástupců Úřadu na workshopech, kulatých stolech a jiných setkáních, kde lze představit závěry z rozhodovací praxe ÚOOÚ.

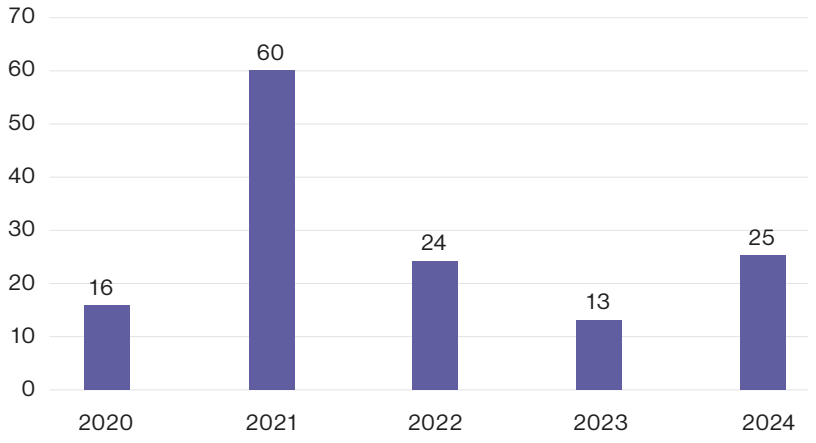
II.1. ROZHODOVACÍ PRAXE A SOUDNÍ ŘÍZENÍ

Ve své činnosti se Úřad i v roce 2024 setkával s některými opakujícími se nedostatky v praxi povinných subjektů, jež komplikují rozhodování a prodlužují správní řízení. Jedná se o chybné vedení spisů, které mnohdy nejsou řádně žurnalizované a chybí v nich důležité dokumenty (samotné informace, které jsou předmětem žádosti, ale též úřední záznamy, doručenky či formální záznamy o skutkových zjištěních). Povinné subjekty také opakovaně chybují při doručování písemností prostřednictvím datové schránky (nevyznačení příznaku pro doručení do vlastních rukou žadatele) i prostřednictvím elektronické pošty (absence kvalifikovaného potvrzení o doručení písemnosti).

Oproti předchozím letům, kdy Úřad opakovaně vstupoval do již zahájených soudních řízení vedených o žalobách napadajících rozhodnutí jiných nadřízených orgánů v roli jejich procesního nástupce, tento trend v roce 2024 ustoupil. Souvisí to se skutečností, že Úřad v této oblasti vykonával působnost již pátým rokem. Přesto se s důsledky těchto změn potýká i nadále, když je nucen aktivně hájit správní rozhodnutí vydaná před mnoha lety jinými subjekty, ačkoliv související správní řízení Úřad nevede a požadovanými informacemi v zásadě nedisponuje.

V roce 2024 však došlo k nárůstu počtu žalob podávaných dle § 65 odst. 1 soudního řádu správního některými povinnými subjekty proti rozhodnutím Úřadu vydaným ve

Počet soudních řízení s účastí Úřadu týkajících se zákona č. 106/1999 Sb. oznámených Úřadu v letech 2020–2024



Poznámka: 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.

druhém stupni správního řízení. Povinné subjekty, které jsou veřejnoprávními korporacemi nebo osobami soukromého práva, totiž 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 č. 106/1999 Sb. Takové subjekty reálně rozhodují o svých subjektivních právech, a proto mohou proti rozhodnutí Úřadu vydanému v odvolacím řízení brojit žalobou. To samozřejmě přináší zvýšené nároky spojené se zastupováním Úřadu v soudních řízeních.

Podmínky pro aplikaci výluky vymezené v § 11 odst. 1 písm. g) zákona č. 106/1999 Sb.

Jednou z otázek, kterými se Úřad již od roku 2023 intenzivně zabýval, byl výklad nově koncipované výluky z práva na informace vymezené v § 11 odst. 1 písm. g) zákona č. 106/1999 Sb., podle něhož povinný subjekt může omezit poskytnutí informace, pokud byla vytvořena nebo získána v přímé souvislosti se soudním, rozhodčím, správním nebo obdobným řízením, a to i před jeho zahájením, a jejíž poskytnutí může ohrozit rovnost účastníků tohoto řízení. Aby tedy mohl povinný subjekt omezit poskytnutí informace dle citovaného ustanovení, musí se nejprve vypořádat s tím, zda je splněna již první zákonná podmínka, tedy že informace byla vytvořena nebo získána v přímé souvislosti se soudním řízením. Nepostačuje přitom jakákoliv souvislost, nýbrž souvislost přímá. Požadované informace tudíž musí být vytvořeny přímo pro účely konkrétního soudního řízení a nemůže se jednat například o informace vypovídající o základní činnosti a působnosti povinného subjektu, pro kterou byl zřízen. Splnění druhé podmínky, totiž že poskytnutí informace může ohrozit rovnost účastníků takového řízení, je třeba posuzovat teprve následně, neboť nesplnění první podmínky brání účinné aplikaci předmětné výluky z práva na informace.

Správní rozhodnutí Úřadu zabývající se touto právní otázkou byla opakovaně předmětem soudního přezkumu, přičemž jak Městský soud v Praze, tak Nejvyšší správní soud se ztotožnily s výkladem citovaného ustanovení podaným Úřadem. Tento výklad svému přezkumu podrobil rovněž Ústavní soud, který jej označil za srozumitelný a logicky obhajitelný.

Poskytování údajů vypovídajících o veřejné či úřední činnosti nebo o funkčním či pracovním zařazení

Úřad byl v rámci své rozhodovací činnosti opakovaně konfrontován s otázkou, na jaký okruh osob a informací o nich dopadá ustanovení § 8a odst. 2 zákona č. 106/1999 Sb. To

představuje ve vztahu k osobním údajům speciální právní úpravu a výjimku vůči obecnému ustanovení § 8a odst. 1, když stanoví, že osobní údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti nebo o jeho funkčním nebo pracovním zařazení, se v zásadě poskytují. Pod pojem „veřejná a úřední činnost" je přitom třeba zařadit též informace o dosaženém vzdělání a odborné praxi zaměstnanců veřejné správy, včetně údaje o konkrétní škole, na níž vzdělání získal, neboť tyto informace náleží z hlediska zákona č. 106/1999 Sb. také do veřejné sféry. Údaje vztahující se k pracovnímu zařazení zaměstnance povinného subjektu a informace o jeho dosaženém vzdělání nepředstavují za běžných okolností žádnou podstatnou újmu. K tomu NSS opakovaně konstatoval, že zájem na transparentnosti veřejné správy a její kontrole existuje nejen u osob, které reprezentují daný subjekt navenek, tj. zastávají nejvyšší pozice, ale i u dalších osob, které se na výkonu veřejné správy podílejí. Ustanovení § 8a odst. 2 zákona č. 106/1999 Sb. je tak aplikovatelné na všechny zaměstnance povinného subjektu bez ohledu na jejich postavení v hierarchické struktuře povinného subjektu.

Naplnění podmínek vymezených v § 8a odst. 2 zákona č. 106/1999 Sb. přesto neznamená poskytnutí takových informací bez dalšího. Povinný subjekt musí současně vždy vyhodnotit, zda v daném konkrétním případě neexistují individuální skutkové okolnosti, které by mohly vést k závěru, že nad právem na informace přesto převáží právo na ochranu osobních údajů dotčené fyzické osoby či jejího soukromí. Taková situace může nastat např., svědčí-li skutkové okolnosti tomu, že zjevným cílem žádosti je dotčenou osobu poškodit, šikanovat, vydírat, snižovat její lidskou důstojnost apod. K posouzení toho, které ze základních vzájemně kolidujících práv v dané věci převáží, je třeba využít test proporcionality.

Postavení povinného subjektu při plnění povinností vyplývajících ze zákona č. 106/1999 Sb.

Městský soud v Praze potvrdil dlouhodobě ustálenou judikaturu, podle níž povinný subjekt při plnění povinností vyplývajících ze zákona č. 106/1999 Sb. vystupuje v postavení orgánu veřejné moci, a to bez ohledu na skutečnost, o jaký typ povinného subjektu se jedná a jaká je povaha jeho vzniku (veřejnoprávní či soukromoprávní). Zákon č. 106/1999 Sb. totiž povinným subjektům svěřil autoritativní rozhodování o uspokojení (respektive o odmítnutí uspokojení) veřejného politického práva na informace, a proto jsou povinné subjekty při tomto rozhodování nepochybně správními orgány ve smyslu § 4 odst. 1 písm. a) soudního řádu správního.

Charakter lhůty stanovené pro odmítnutí žádosti v § 11a zákona č. 106/1999 Sb.

Úřad se v rámci své rozhodovací činnosti opakovaně setkal s otázkou, jaký charakter má lhůta stanovená v § 11a zákona č. 106/1999 Sb. Jelikož zmíněné ustanovení fakticky vymezuje dvě skutkové podstaty, kdy povinný subjekt může přistoupit k odmítnutí žádosti bez ohledu na požadované informace samotné, přičemž vychází pouze z úvahy, že žadatel své právo na informace reálně zneužívá, zákonodárce přistoupil k větší přísnosti při možné aplikaci tohoto důvodu. Ta nabyla podoby prekluzivního charakteru sedmidenní lhůty ode dne přijetí žádosti, v níž je možné tento důvod uplatnit. Po jejím uplynutí již citované ustanovení pro odmítnutí žádosti nelze použít.

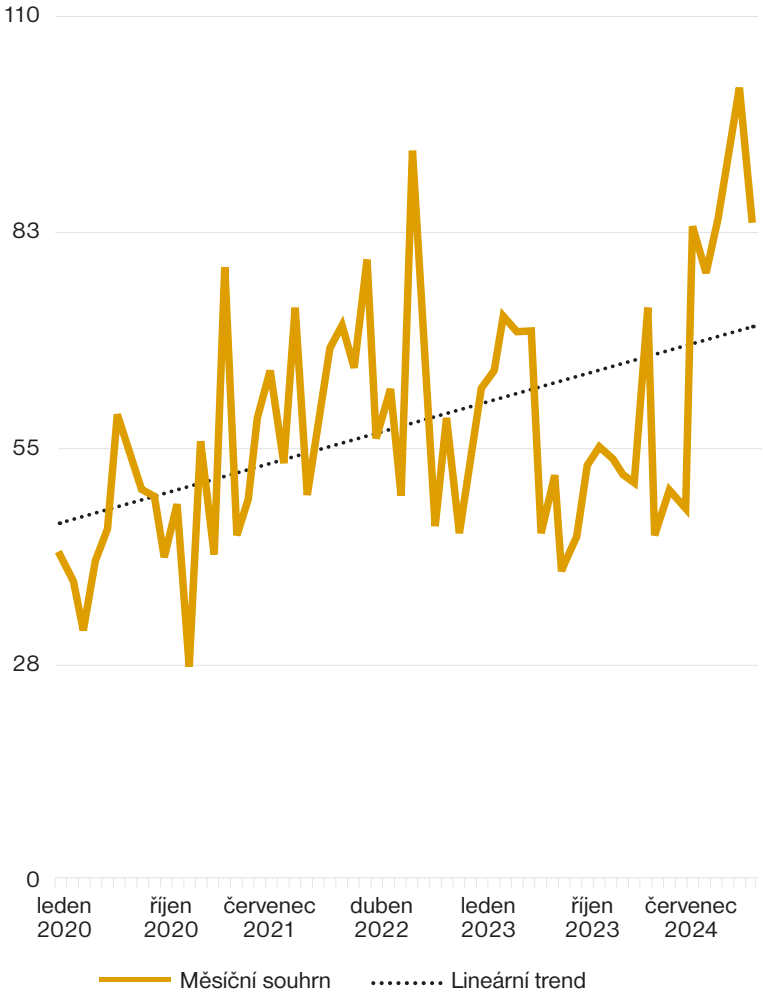
Využití kvalifikovaného odhadu při stanovení úhrady nákladů spojených s mimořádně rozsáhlým vyhledáváním informací

V případě mimořádně rozsáhlého vyhledávání informací může povinný subjekt přistoupit k určení nákladů s tím spojených na základě tzv. kvalifikovaného odhadu. Takový odhad vychází z vyhledání části požadovaných informací, které představují dostatečně reprezentativní vzorek, a následné aplikaci takto zjištěných hodnot na celou žádost. Tento postup již v minulosti označil za korektní též Ústavní soud. Kvalifikovaný odhad je však nutné jednak srozumitelně odůvodnit a náležitě popsat v oznámení o výši nákladů zasílaném žadateli, jednak o něm současně musí být i záznam ve spisovém materiálu. Pouze při dodržení tohoto postupu je pak nadřízený správní orgán schopen náležitě přezkoumat oprávněnost stanovené výše úhrady za vyhledání informací.

Povinný subjekt nemůže odůvodnit odmítnutí žádosti o informace vícero důvody, které vůči sobě uplatní zástupně

Městský soud v Praze v rámci soudního přezkumu posuzoval rozhodnutí povinného subjektu, jehož odůvodnění spočívalo na vícero důvodech, které byly vůči sobě uplatněny zástupně (ve smyslu pokud se neuplatní jeden důvod, uplatní se další). Takto koncipovaná argumentace dle soudu nemůže obstát. Přestože lze přirozeně odůvodnit neposkytnutí informací souběžně více důvody, nemohou se vzájemně vylučovat. Správní orgán tedy nemůže koncipovat odůvodnění svého rozhodnutí tak, že pokud neobstojí první důvod (v daném případě, že požadované informace neexistují a bylo by je potřeba vytvořit ve smyslu § 2 odst. 4 zákona č. 106/1999 Sb.), nastupuje důvod další [výluka dle § 11 odst. 2 písm. a) zákona č. 106/1999 Sb.], a pokud se neuplatní ani tento důvod, pak se uplatní další důvod v pořadí, vzájemně se vylučující s předchozím (výluka dle § 11 odst. 3 zákona č. 106/1999 Sb.). Odůvodnění rozhodnutí, v němž správní orgán označí více vzájemně se zastupujících a vylučujících důvodů a v podstatě očekává, který z nich následně obstojí při přezkumu (odvolacím orgánem či soudem), nelze považovat za řádné odůvodnění správního rozhodnutí. Pro adresáta takto koncipovaného rozhodnutí není totiž jednoznačně srozumitelné, který ze zákonných důvodů pro odmítnutí v daném případě skutečně povinný subjekt uplatňuje.

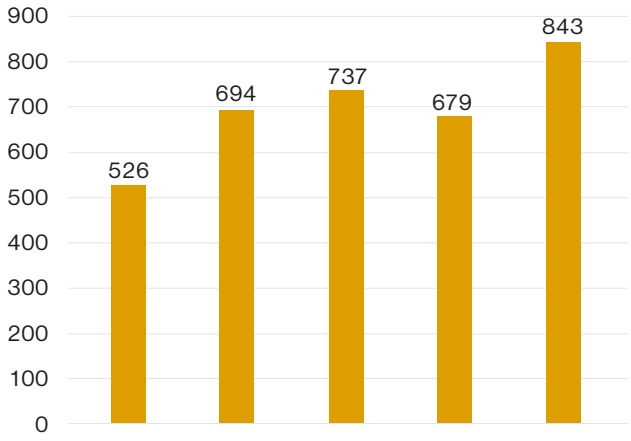
Vývoj měsíčního počtu podání a podnětů agendy podle zákona č. 106/1999 Sb. v letech 2020–2024



Rozhodce rozhodující konkrétní spor v řízení vedeném rozhodčím soudem je soukromou osobou

Městský soud v Praze se zabýval otázkou, jakou povahu mají údaje o rozhodcích rozhodujících v konkrétních sporech, načež dospěl k závěru, že tyto údaje nelze považovat za údaje ve smyslu § 8a odst. 2 zákona č. 106/1999 Sb., tj. za údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti nebo o jeho funkčním nebo pracovním zařazení. Rozhodce rozhodující konkrétní spor v řízení vedeném rozhodčím soudem je totiž soukromou osobou, nejedná se o veřejně činnou osobu, funkcionáře či zaměstnance veřejné správy, jako je tomu například u soudců. Obrátit se na rozhodčí soud jako na alternativu soudního řízení je pouze právem dotčených osob, nikoli povinností uloženou zákonem, přičemž informace o určených rozhodcích či způsobu jejich určení, které jsou obsahem rozhodčí smlouvy uzavřené mezi stranami, nejsou strany sporu povinny poskytnout.

Vývoj počtu podání a podnětů v agendě dle zákona č. 106/1999 Sb.



Český olympijský výbor není povinným subjektem ve smyslu zákona č. 106/1999 Sb.

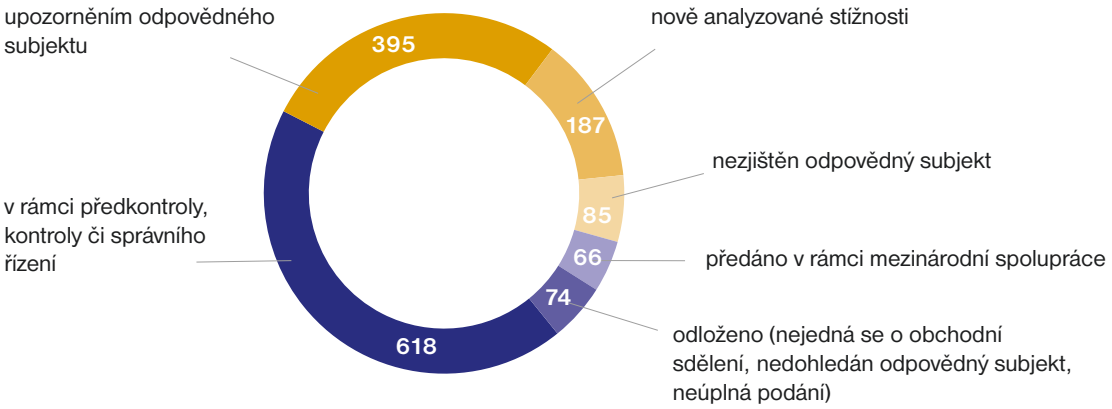
Úřad byl v rámci výkonu své působnosti postaven před otázku, zda Český olympijský výbor je povinným subjektem ve smyslu zákona č. 106/1999 Sb. Úřad se detailně zabýval charakterem subjektu a dospěl k závěru, že Český olympijský výbor není státním orgánem, ani územním samosprávným celkem a jeho orgánem, není veřejnou institucí, neboť nenaplňuje typické znaky veřejné instituce vymezené ustálenou judikaturou, nelze jej podřadit ani pod kategorii veřejného podniku, neboť zákonné podmínky vymezené pro veřejný podnik nelze vůči tomuto subjektu uplatnit s ohledem na povahu jeho činnosti, právní formu a pravidla jeho fungování, a není ani osobou, které zákon svěřil výkon veřejné moci ve smyslu ustanovení § 2 odst. 2 zákona č. 106/1999 Sb. Český olympijský výbor tedy není povinným subjektem, a proto na něj nedopadá povinnost poskytovat informace vymezená v zákoně č. 106/1999 Sb.

III. Nevyžádaná obchodní sdělení

V oblasti nevyžádaných obchodních sdělení ÚOOÚ řeší všechny obdržené stížnosti či podněty, a to i ty podané anonymně. Stejně tak Úřad nečiní rozdíl mezi adresátem nevyžádaného obchodního sdělení coby fyzickou osobou a právnickou osobou. Součástí každého podání však musí být dostatečně doložené předmětné „nevyžádané" obchodní sdělení. V případě e-mailové zprávy je třeba doložit celou zprávu včetně hlavičky e-mailové zprávy, v případě SMS zprávy či jiného typu uložené zprávy je postačující printscreen či alespoň přepis zprávy s údaji, od koho byla zpráva zaslána a na jaké telefonní číslo. Na základě těchto doložených informací pak Úřad zjišťuje faktického odesílatele a podnikatelský subjekt, v jehož prospěch bylo obchodní sdělení zasláno.

Za rok 2024 obdržel Úřad celkem 1425 stížností týkajících se nevyžádaných obchodních sdělení. Z toho se 36 % stížností týkalo nevyžádaných obchodních sdělení zasílaných na e-mailové adresy a obsahujících zálohové faktury na služby, které si příjemci neobjednali.

Způsob vyřízení 1425 stížností podaných v roce 2024



III.1. KONTROLY A SPRÁVNÍ ŘÍZENÍ

V roce 2024 zahájil ÚOOÚ celkem 13 kontrol týkajících se obchodních sdělení. Správních řízení zahájil Úřad 32, přičemž pravomocně ukončených správních řízení bylo 31 a celková výše sankcí činila 7 124 000 Kč. Podobně jako v minulém roce se správní řízení často týkala opakovaných porušení zákona při zasílání obchodních sdělení, čemuž následně odpovídala i výše uložené sankce. Ve 2 případech byla uložena pořádková pokuta za nesoučinnost, a to v celkové výši 100 000 Kč. V případě méně závažných pochybení Úřad pokračuje v upozorňování subjektů na možná pochybení při zasílání obchodních sdělení a vyzývá k nápravě ve vztahu k podané stížnosti. Úřad takto upozornil 359 subjektů.

V rámci mezinárodní spolupráce podle nařízení Evropského parlamentu a Rady (EU) 2017/2394 předal Úřad celkem 60 stížností k provedení donucujících opatření či poskytnutí informací. Stejně jako v roce 2023 bylo nejvíce stížností předáno na Slovensko, dále do Polska, Litvy, Slovinska, Nizozemska, Maďarska a Itálie. Naopak ze zahraničí Úřad

neobdržel žádnou stížnost k provedení příslušných opatření vůči českému podnikatelskému subjektu.

Nejčastějším protiprávním jednáním je zasílání obchodních sdělení bez příslušného právního titulu. Tento přestupek je také nejzávažnější, neboť právní titul je stěžejním bodem v rámci ochrany elektronické komunikace, potažmo ochrany soukromí v elektronické komunikaci. Ostatní porušení se týkají náležitostí, které musí být při šíření obchodních sdělení elektronickou poštou splněny.

Katalogové podvody

Na tzv. katalogové podvody ÚOOÚ obdržel několik stovek stížností. Jedná se o šíření obchodní nabídky cílené na e-mailové adresy společností či podnikajících fyzických osob, jejichž přílohou je zálohová faktura za dosud neobjednané služby, případně upomínka o zaplacení či různé informace týkající se porušení všeobecných obchodních podmínek. Tato činnost je klamavá obchodní praktika směřující k neúmyslnému uzavření obchodně-závazkového vztahu ze strany osloveného (podnikatelského subjektu) a k následnému využití tohoto aktu podvodnou katalogovou firmou k neoprávněnému obohacení.

Úřad tyto stížnosti vyhodnocuje jako stížnosti na zasílání nevyžádaných obchodních sdělení. Jedná se o zaslání cenové nabídky na poskytované služby a vzhledem k tomu, že zákon č. 480/2004 Sb. nerozlišuje mezi zasláním obchodního sdělení fyzické či právnické osobě, lze tak za zasílání těchto obchodních sdělení dané odesílatele postihnout.

Úřad opakovaně upozorňuje na to, že nelze využívat různé dostupné databáze kontaktů k zasílání obchodních sdělení. Zasílat obchodní sdělení lze pouze na základě předchozího souhlasu adresáta, který musí odpovídat požadavkům pro získání platného souhlasu dle nařízení (EU) 2016/679, nebo v souvislosti se zákaznickým vztahem (oprávněný zájem) při dodržení dalších podmínek uvedených v § 7 odst. 3 zákona č. 480/2004 Sb. Účelem veřejně dostupných databází je poskytnout uživateli informace o subjektech zařazených v databázi. V případě, že se uživatel rozhodne takové údaje dále zpracovávat (vyjma zpracování prováděného fyzickou osobou v průběhu výlučně osobních nebo domácích činností), stává se automaticky správcem těchto údajů a je povinen si sám zajistit právní titul zpracování tak, aby toto zpracování bylo prováděno v souladu s nařízením (EU) 2016/679. V rámci právní úpravy veřejných databází se také často vyskytuje ustanovení, kde je výslovně uveden zákaz šířit prostřednictvím uvedených kontaktů obchodní sdělení v rozporu s podmínkami stanovenými zákonem č. 480/2004 Sb.

Úřad v této věci ukončil 4 kontroly společností, kterým následně za zasílání obchodních sdělení bez právního titulu uložil příslušnou sankci v celkové výši 5 465 000 Kč. Všechna rozhodnutí jsou pravomocná. Kontrola dalších 2 společností nadále probíhá.

Jako poznatek z kontrol lze uvést, že tyto společnosti bývají různě personálně propojené a před ukončením kontroly většinou dochází ke změnám jednatelů či rovnou k ukončení činnosti, případně stejná činnost (zasílání zálohových faktur) pokračuje pod hlavičkou jiné společnosti.

Úřad předal své poznatky z kontrol Policii ČR a Finančnímu analytickému úřadu k posouzení, zda nedochází k podvodnému jednání či porušení daňových předpisů.

III.2. SOUDNÍ ROZHODNUTÍ

Městský soud v Praze svým rozsudkem čj. 8 A 102/2023-59 ze dne 26. června 2024 potvrdil dlouhodobý výklad ÚOOÚ týkající se povinnosti zřetelně označovat obchodní sdělení již na samotném počátku sdělení. Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud není zřetelně a jasně označena jako obchodní sdělení.

Městský soud v Praze k tomu uvedl, že adresátovi obchodního sdělení má být již na počátku poskytnuta informace, že se jedná o obchodní sdělení, aby se mohl rozhodnout, zda takovou poštu vůbec otevře a bude se zajímat o její obsah. Aby byla zajištěna ochrana fyzických i právnických osob před nežádoucím obtěžováním, musí mít adresáti možnost nejen předem souhlasit se zasíláním obchodních sdělení, resp. možnost zastavit jejich další zasílání, ale rovněž možnost zaslaná obchodní sdělení vůbec nečíst. Uvedený rozsudek byl napaden kasační stížností. Nejvyšší správní soud kasační stížnost zamítl a ve svém odůvodnění potvrdil výklad Úřadu.

III.3. LEGISLATIVA

Návrh zákona o digitální ekonomice a o změně souvisejících zákonů nahradí stávající zákon č. 480/2004 Sb., který mimo jiné upravuje podmínky šíření obchodních sdělení elektronickými prostředky. V tomto návrhu jsou přesněji definovány dva právní tituly, na základě kterých lze obchodní sdělení šířit. Jedním je oprávněný zájem za současného splnění vyjmenovaných podmínek a druhým je předchozí souhlas, přičemž je jednoznačně uvedeno, že se jedná o souhlas ve smyslu čl. 4 bodu 11 nařízení (EU) 2016/679.

Stejně jako v současné právní úpravě jsou v návrhu stanoveny náležitosti, které musí každé obchodní sdělení obsahovat. Nutností je zřetelné a jasné označení, identifikace podnikatele, jehož jménem nebo na jehož účet se komunikace uskutečňuje, a uvedení informace o možnosti příjemce doručit námitku proti využití jeho elektronického kontaktu či odvolat poskytnutý souhlas.

Jednou z navržených změn je možnost ÚOOÚ uložit kromě pokuty za porušení příslušných ustanovení také nápravná opatření. V případě méně závažných porušení bude mít Úřad možnost upozornit šiřitele obchodních sdělení na porušení povinnosti a vyzvat jej k nápravě.

Nejvíce diskutovanou změnou je zvýšení horní hranice pokuty. Vyšší horní hranice pokuty bude stanovena s ohledem na čl. 15 odst. 2 směrnice o soukromí a elektronických komunikacích, ze kterého ve spojení s čl. 94 GDPR vyplývá, že sankce za porušení úpravy podle této směrnice by měly být ukládány podle GDPR.

IV. Informační systém ORG

Na základě zákona č. 111/2009 Sb., o základních registrech, a jeho změny zákonem č. 100/2010 Sb. Úřad provozuje 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 neveřejné zdrojové identifikátory fyzických osob (ZIFO) a agendové identifikátory fyzických osob (AIFO).

Aby mimo zákonný rámec nebylo možné spojovat údaje o občanovi vedené v různých agendách, zákon o základních registrech zavedl pro občana vícenásobnou digitální identitu, tedy v různých agendách je občan veden pod odlišným identifikátorem (AIFO). Vytváření a transformace AIFO je úkolem informačního systému ORG označovaného také jako „převodník identifikátorů".

ZIFO je vytvořen Informačním systémem ORG, 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, který je také jediným místem, které umí převést AIFO jedné agendy na AIFO agendy jiné.

IS ORG neuchovává a ani nezpracovává žádné osobní údaje, je neveřejný a komunikuje výhradně s informačním systémem základních registrů (ISZR). Při každé komunikaci agendových informačních systémů s ISZR (a základními registry) dochází k ověřování oprávnění úředníka či uživatele k požadované operaci. IS ORG je uplatněním zákona na ochranu osobních údajů v praxi a je zásadní součástí systému základních registrů (ZR), řešící bezpečnost osobních dat ZR.

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

V roce 2024 uběhlo dvanáct let od začátku fungování základních registrů. Za tuto dobu převratně narostla míra jejich využívání. Jen počet provedených transakcí v IS ORG oproti roku jejich zavedení vzrostl více než desetinásobně, přičemž transakcí se rozumí operace prováděná v IS ORG (založení ZIFO, generování AIFO, překlad AIFO pro jinou agendu a další).

Roku 2024 bylo zaznamenáno vyšší využití základních registrů a tím i IS ORG v souvislosti se spuštěním aplikace eDoklady, s elektronickými přihláškami na střední školy, volbami do Evropského parlamentu a krajskými volbami. Oproti roku 2023 počet provedených transakcí narostl o 21,66 %. Nebyl zaznamenán žádný bezpečnostní incident.

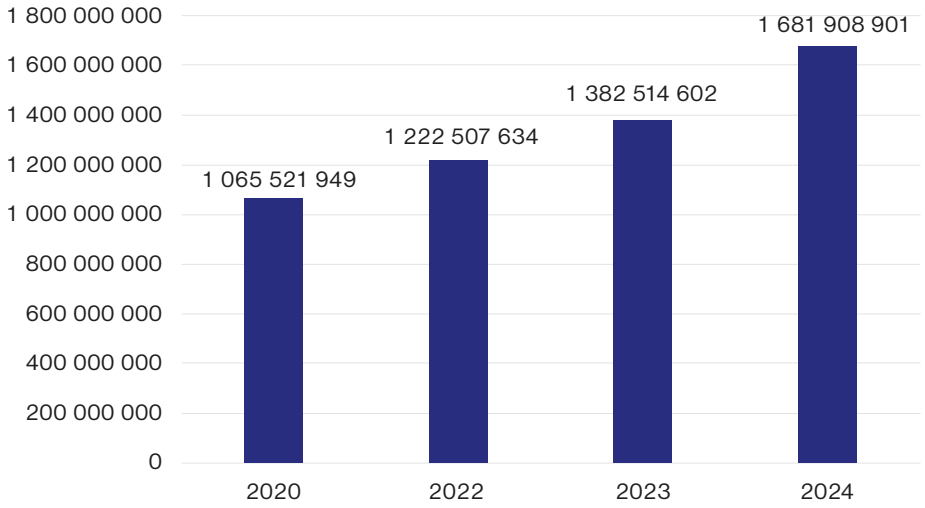
V listopadu 2024 proběhl 2. dozorový audit v rámci certifikace IS ORG dle ČSN EN ISO/IEC 27001:2014 bez nálezu neshody. Průběžně pokračuje úprava dokumentace tak, aby byla v souladu s novou verzí normy a aby IS ORG mohl být v roce 2025 certifikován po-

dle nové normy ČSN EN ISO/IEC 27001:2023. Kyberbezpečnost je pro provoz IS ORG absolutní prioritou.

Trend rostoucího využívání základních registrů stále pokračuje, také v závislosti na obecném rozvoji propojeného datového fondu. V roce 2024 byla schválena nová strategie IS ORG na roky 2024–2028, která se orientuje především na udržení dobré kondice systému, zejména s ohledem na obnovu hardwaru s končící podporou, na soulad s moderními trendy v kyberbezpečnosti pro potřeby udržení certifikace ČSN EN ISO/IEC 27001:2014, ve vztahu k přípravě na splnění požadavků normy ČSN EN ISO/IEC 27001:2023 a hlavně s ohledem na nové úkoly spojené s dalším rozvojem základních registrů.

V oblasti využívání IS ORG lze očekávat dynamický vývoj, a to vzhledem k probíhajícím změnám ve správě základních registrů v souvislosti s projektem Základní registry nové generace.

Celkový počet transakcí v letech 2021–2024



V. Digitální agendy

V průběhu roku 2024 se tematika tzv. digitálních agend stala pravidelnou součástí aktivit řešených na úrovni evropských dozorových úřadů na ochranu osobních údajů. Došlo k tomu v návaznosti na přípravu a přijetí „nových velkých evropských aktů regulujících digitální prostředí", jak lze souhrnně nazvat regulatorní akty připravované v posledních letech na úrovni EU. Pojem „digitální agendy" je přitom pojem pracovní a ne zcela přesně vystihuje charakter nových předpisů, jejichž jednotícím znakem je druh regulace ve virtuálním prostředí. Nové právní předpisy se týkají specifických právních vztahů nebo hodnot, na jejichž ochraně v digitálním prostředí existuje v EU shoda. Sledují v nich uvedené účely, jako podporu digitálních služeb na jednotném vnitřním trhu EU, ochranu práv spotřebitelů digitálních služeb, ochranu dětí na sociálních sítích, poučené zacházení s dezinformacemi, posílení přístupu k datům, posílení informační povinnosti, transparentnost politické reklamy atd.

V oblastech upravených novými evropskými nařízeními jsou při konkrétních činnostech shromažďována či zaznamenávána data včetně osobních údajů. V průběhu přípravy nových evropských aktů regulujících digitální prostředí byly veřejností či odbornou veřejností vznášeny otázky a obavy týkající se ochrany osobních údajů. Ty lze zodpovědět po přijetí nových aktů, ke kterému již z velké části došlo, přičemž jejich interpretace z pohledu ochrany osobních údajů na úrovni Evropského sboru pro ochranu osobních údajů (EDPB) intenzivně probíhá a je upřesňována. Obecně nicméně platí, že pro dozorové úřady na ochranu osobních údajů zůstává východiskem pro posuzování náležitého zpracování osobních údajů platný právní rámec ochrany osobních údajů, a to i pokud jde o nově regulovaný digitální kontext. Ochrana osobních údajů je zachována, uplatňuje se ovšem v komplexním digitálním prostředí vyžadujícím specializované znalosti. Právo na ochranu osobních údajů se realizuje obvyklým způsobem prostřednictvím aplikace principů ochrany osobních údajů při současném respektování specifik upravených v nových aktech.

Český dozorový úřad začal řešit problematiku svého zapojení ve vztahu k novým evropským digitálním aktům včas, a to v době, kdy byly zveřejněny návrhy těchto předpisů, ačkoli nastoupení jejich účinnosti nebylo jednotné. V ČR však mnohdy dosud nebyly přijaty prováděcí vnitrostátní právní předpisy, přičemž jejich návrhy se aktuálně nacházejí na různé úrovni rozpracovanosti. Koncem roku 2024 byl v Parlamentu ČR projednáván návrh zákona o digitální ekonomice, byl připraven návrh zákona o správě dat a o řízeném přístupu k datům a byl ukončen termín pro podávání připomínek k návrhu zákona o transparentnosti a cílení politické reklamy a o změně některých souvisejících zákonů.

ÚOOÚ se začal intenzivně zabývat otázkami tzv. digitálních agend již před rokem 2024, kdy vytvořil dosud stále fungující interní pracovní skupinu složenou z vlastních zaměstnanců. V průběhu roku 2024 Úřad začlenil digitální agendy do nově vzniklého odboru stížností a digitálních agend. Jde přitom o problematiku prolínající se dalšími činnostmi Úřadu, např. oblastí legislativní, analytickou, vzdělávací, kontrolní či oblastí mezinárodní spolupráce.

Z praktického hlediska je důležitá platnost a účinnost výše zmíněných předpisů, stav připravenosti vnitrostátní právní úpravy, analýza výkonu agend a odhad počtu pracovní-

ků ÚOOÚ pro výkon nových činností. Konkrétně se jedná o nařízení o digitálních službách (DSA), akt o správě dat (DGA), nařízení o datech (DA), nařízení o digitálních trzích (DMA), nařízení o transparentnosti a cílení politické reklamy (PAR) a akt o umělé inteligenci (AI Akt). Ve všech případech jde o rozdílné právní úpravy chránící různá práva či zájmy, s odlišnými kompetencemi příslušných orgánů, využívající odlišné nástroje a instituty.

V.1. AKTUÁLNÍ EVROPSKÁ LEGISLATIVA

Nařízení o digitálních službách (DSA)

Oblast digitálních služeb je v současnosti nejvíc rozpracovanou agendou, a to s ohledem na její robustnost, univerzalitu a již účinnou právní úpravu. Nařízení o digitálních službách stanovuje pro poskytovatele zprostředkovatelských služeb např. požadavky týkající se náležité péče, pokud jde o způsoby řešení nezákonného obsahu, dezinformace na internetu a další společenská rizika. Cílem nařízení o digitálních službách (a později zákona o digitální ekonomice) je především zajistit vytvoření jasného a předvídatelného právního rámce pro fungování digitálních služeb. To zahrnuje jednak určení příslušných orgánů, které odpovídají za vymáhání nařízení o digitálních službách, k nimž patří ÚOOÚ, jednak stanovení pravidel sankcí za porušení nařízení. Dojde také ke změně právní úpravy v oblasti zprostředkovatelských služeb.

Nařízení DSA předpokládá vydání vnitrostátního předpisu, tj. návrhu zákona o digitální ekonomice a o změně některých souvisejících zákonů, který je aktuálně projednáván v Poslanecké sněmovně Parlamentu ČR jako tisk č. 760. Účinnost tohoto předpisu se předpokládá na začátku roku 2025. Zákon zruší současný právní rámec, který je upraven zákonem č. 480/2004 Sb., o některých službách informační společnosti.

Návrh zákona o digitální ekonomice stanoví nové povinnosti ÚOOÚ, k nimž patří:

- dozor nad povinnostmi vztahujícími se k reklamě dle čl. 26 DSA, např. nad povinností zprostředkovatele určit, že informace jsou reklamou, určit příjemce reklamy, poskytnout informaci, zda jde o obchodní sdělení či zda poskytovatel online platformy neposkytuje služby na základě profilování;

- zákaz pro poskytovatele online platformy prezentovat reklamy založené na profilování podle čl. 28 odst. 2 DSA, pokud jsou si s odpovídající jistotou vědomi toho, že příjemcem služby je nezletilá osoba;

- poskytování stanovisek na žádost Českého telekomunikačního úřadu (ČTÚ), pokud řízení, které vede, souvisí s povinnostmi v oblasti ochrany osobních údajů;

- spolupráce s ČTÚ při výměně informací a podkladů potřebných pro řádné zajišťování dozoru dle nařízení o digitálních službách;

- vyhodnocování podnětů zaslaných orgány veřejné moci, které mohou být relevantní pro výkon dozoru Úřadem;

- zpracování stanovisek pro Evropský sbor pro digitální služby, pokud se jeho jednání bude týkat působnosti Úřadu, případně účast na jednání Sboru;
- podávání návrhů na omezení přístupu ke službě podle zákona o digitální ekonomice příslušným justičním orgánům;
- návrh na zahájení řízení o prodloužení omezení služby, pokud původní soudní řízení nevedlo k potřebné nápravě;
- ukládání nápravných opatření v oblasti agendy šíření obchodních sdělení;
- vedení řízení o nově upravených přestupcích podle zákona o digitální ekonomice, pokud je k nim Úřad příslušný;
- poskytování podkladů potřebných pro zpracování zprávy o činnosti ČTÚ;
- plnění dalších úkolů stanovených nařízením o digitálních službách a zákonem o digitální ekonomice.

Nařízení o digitálních službách je platné od listopadu 2023 a účinné od 17. února 2024 s některými výjimkami (např. informační povinnost poskytovatelů online platforem v souvislosti s transparentností, která platí od 17. února 2023, některé povinnosti velmi velkých online platforem a velmi velkých internetových vyhledávačů jako nezávislý audit, placení ročního poplatku za dohled apod.)

Nařízení o digitálních trzích (DMA)

Účelem nařízení o digitálních trzích (DMA) je podpořit otevřenost hospodářské soutěže a konkurenční prostředí pro trhy v digitálním odvětví obecně. Stanoví rámec pro regulaci velkých technologických společností, tzv. gatekeeperů neboli strážců přístupu, s cílem zajistit, aby nezneužívaly svou tržní sílu, a chránit soukromí a online souhlas uživatelů. Vymahatelem nařízení o digitálních službách na úrovni EU je Evropská komise. Za provádění a prosazování aktu o digitálních trzích odpovídá společný tým v generálním ředitelství pro hospodářskou soutěž (DG COMP) a pro komunikační sítě, obsah a technologie (DG CONNECT).

Nařízení o digitálních trzích stanoví rovněž povinnosti tzv. strážců přístupu v oblasti zpracování osobních údajů. Strážce přístupu např. nesmí zpracovávat pro účely poskytování online reklamních služeb osobní údaje koncových uživatelů využívajících služby třetích stran, které využívají hlavních služeb strážce přístupu, kombinovat osobní údaje z příslušné hlavní služby platformy s osobními údaji z jakýchkoliv dalších hlavních služeb platforem nebo služeb třetích stran apod., ledaže by koncovému uživateli byla předložena možnost volby a udělil souhlas ve smyslu čl. 4 bodu 11 a čl. 7 nařízení (EU) 2016/679.

Vzhledem k tomu, že nařízení o digitálních trzích nastavuje opatření ve vztahu ke strážcům přístupu, které se promítá do oblasti ochrany osobních údajů, nemůže zůstat zcela mimo pozornost ÚOOÚ. Problematika hospodářské soutěže ostatně byla nedávno předmětem diskuse v EDPB a předpokládá se spolupráce dozorových orgánů pro ochranu osobních údajů a orgánů pro hospodářskou soutěž.

Nařízení o digitálních trzích vstoupilo v platnost dvacátým dnem po vyhlášení, tj. od 1. listopadu 2022, a používá se s některými výjimkami od 2. května 2023.

Nařízení o správě dat (DGA)

Akt o správě dat je meziodvětvový nástroj, jehož úkolem je umožnit opakované použití veřejně držených/chráněných dat a posílit sdílení dat prostřednictvím regulace nových zprostředkovatelů dat a podporou sdílení dat pro altruistické účely. Navrhovaný akt má za cíl zavést principy správy dat veřejného sektoru a upravit regulaci řízeného přístupu k datům veřejného sektoru a možnost jejich opětovného užití. Tato problematika se pojmově může týkat i ochrany osobních údajů, pokud jsou předmětem sdílení. Akt předpokládá přijetí vnitrostátní právní úpravy, kterou v ČR představuje návrh zákona o správě dat a o řízeném přístupu k datům a o změně některých souvisejících zákonů (zákon o správě dat a o řízeném přístupu k datům) a zákon o digitální ekonomice. Návrh zákona o správě dat byl podle dostupných informací zpracován na úrovni připomínkového řízení a vložen do evidence.

Nárůst agendy ÚOOÚ bude spočívat především v provádění dozoru nad ochranou osobních údajů ve vztahu k držitelům dat, konkrétně zda data zpřístupnili v souladu s právními předpisy, a dále ve vztahu k uživatelům dat, konkrétně zda zpracovávají data v souladu s podmínkami zpřístupnění. Návrh zákona o správě dat předpokládá, že pokud vyjde najevo neoprávněné využívání osobních údajů osobou, které byl poskytnut řízený přístup k datům, schvalující orgán neprodleně informuje ÚOOÚ, jenž bude jednat. Problematika bude dále rozpracována v návaznosti na přípravu právní úpravy.

Akt o správě dat bude účinný od 24. září 2025.

Nařízení o datech (DA)

Nařízení či akt o datech byl přijat s cílem zvýšit dostupnost a sdílení dat v ekonomice, rozvíjet ekonomiku EU založenou na datech a podporovat jednotný a konkurenceschopný trh s daty. Jde o stanovení horizontálního souboru pravidel pro přístup k údajům a jejich využívání, který respektuje ochranu základních práv a měl by přinášet evropskému hospodářství a společnosti rozsáhlé výhody. Akt se vztahuje na dobrovolná ujednání o poskytování dat mezi soukromými a veřejnými podniky, může se však také vztahovat na předávání dat veřejným orgánům v případě krizových situací. Akt o datech doplňuje akt o správě dat jako časově předcházející výstup evropské strategie pro data, přičemž akt o správě dat vstoupil v platnost v září 2023.

Pokud jde o vztah GDPR a aktu o datech, akt opakovaně odkazuje na použití obecného nařízení o ochraně osobních údajů, jehož platnost není dotčena. Z pohledu ochrany osobních údajů bude akt o datech klást zvýšené nároky na ÚOOÚ při posouzení rozsáhlých zpracování dat vyskytujících se typicky v datové ekonomice, přičemž se může jednat o shromažďování informací v datových silech či cloudech, přístup k datům připojeného výrobku či souvisejících služeb, shromažďování dat o výkonnosti, použití nebo prostředí výrobků předávaných prostřednictvím služby elektronických komunikací, fyzického připojení nebo internetu věcí apod.

Nařízení o datech upravuje faktická ustanovení, která konkretizují náležité zpracování osobních údajů uživatelů. Nárůst agendy Úřadu bude spočívat ve vymáhání příslušných ustanovení aktu o datech, které upravují zpracování osobních údajů.

Akt o datech byl zveřejněn v Úředním věstníku EU dne 22. prosince 2023 a vstoupí v platnost dne 12. září 2025. Dosud však není jasné, jak bude nařízení o datech implementováno do vnitrostátního právního řádu ČR.

Nařízení o umělé inteligenci

Účelem nařízení o umělé inteligenci (AI akt) je zlepšit fungování vnitřního trhu EU stanovením jednotného právního rámce pro vývoj, uvádění na trh, uvádění do provozu a používání systémů umělé inteligence v souladu s hodnotami EU. Systémy AI se mohou podílet na široké škále hospodářských, environmentálních a společenských přínosů v řadě průmyslových odvětví a sociálních aktivit. AI akt zavádí přiměřený a účinný soubor závazných pravidel pro systémy AI, který je založen na posouzení rizik.

Nařízením není dotčeno uplatňování stávajícího právního rámce zpracování osobních údajů podle práva EU, včetně úkolů a pravomocí nezávislých dozorových orgánů příslušných pro sledování dodržování těchto nástrojů, a nejsou dotčeny povinnosti poskytovatelů systémů AI a zavádějících subjektů v jejich úloze správců nebo zpracovatelů údajů, pokud návrh, vývoj nebo používání systémů AI zpracování osobních údajů zahrnuje.

V současné době se v ČR začíná připravovat vnitrostátní prováděcí předpis k AI aktu. Na základě usnesení vlády převzal akt o umělé inteligenci do své gesce člen vlády pověřený koordinací činnosti ústředních správních úřadů v oblasti digitalizace, který má do 30. dubna 2025 předložit vládě návrh adaptačního zákona.

AI akt je v současné době platný, nikoliv však účinný. Účinnost nastane od 2. srpna 2026. Nicméně akt o umělé inteligenci je z hlediska nastoupení účinnosti jednotlivých povinností diferencovaný, což znamená, že některé povinností budou platit od srpna 2025 (např. zřízení oznamujících orgánů), některé již od února 2025 (např. obecná ustanovení a zakázané postupy) a další od srpna 2027.

Nařízení o transparentnosti a cílení politické reklamy (PAR)

Nařízení o politické reklamě předpokládá, že potřeba zajistit transparentnost politické reklamy je legitimním veřejným cílem v souladu s hodnotami sdílenými Evropskou unií a jejími členskými státy, a vychází z faktu, že pro občany není vždy snadné rozpoznat politická reklamní sdělení a uplatňovat svá demokratická práva informovaným způsobem.

Na vnitrostátní úrovni bude pro provedení nařízení určen zákon o transparentnosti a cílení politické reklamy, jehož návrh se připravuje. Návrh zákona předpokládá, že ÚOOÚ bude vykonávat dozor nad dodržováním povinností určených v čl. 18 až 20 nařízení PAR, bude projednávat přestupky, vyřizovat stížnosti, zajišťovat přeshraniční spolupráci s dozorovými úřady v jiných státech a předávat Ministerstvu vnitra statistiku o správních trestech, které uloží v předcházejícím roce.

Nařízení vstoupilo v platnost dvacátým dnem po vyhlášení v Úředním věstníku EU a použije se ode dne 10. října 2025 s některými výjimkami.

Požadavky ÚOOÚ pro výkon digitálních agend

Digitální agendy představují širokou škálu regulačních předpisů, jejichž účinnost nastupuje postupně, přičemž v České republice dosud mnohdy nebyla přijata vnitrostátní

právní úprava. V oblastech upravených novými evropskými nařízeními jsou při konkrétních činnostech shromažďována či zaznamenávána data včetně osobních údajů. Obecně platí, že pro dozorové úřady na ochranu osobních údajů zůstává východiskem pro posuzování náležitého zpracování osobních údajů platný právní rámec ochrany osobních údajů, a to i pokud jde o nově regulovaný digitální kontext. Ochrana osobních údajů je zachována, uplatňuje se ovšem v komplexním digitálním prostředí vyžadujícím specializované znalosti.

Předpokladem vykonávání digitálních agend pracovníky dozorových úřadů je obecně znalost aplikace principů ochrany osobních údajů, provázená specializovanou znalostí jednotlivých aktů a vyžadující pochopení komplementarity fungování ochrany osobních údajů a specializované právní úpravy. K těmto znalostem musí nutně přistoupit znalost fungování technologií (např. algoritmů), minimálně na úrovni potřebné pro výkon dané agendy.

Výkon nových agend s sebou přirozeně nese zvýšené personální požadavky, které Úřad již opakovaně vznesl, ale dosud jim nebylo vyhověno. V každém případě již v současné době ÚOOÚ digitální agendu aktivně vykonává, protože se jí zabývají stávající pracovníci v rámci svých dosavadních povinností. Do budoucna však bude nutná specializace a navýšení pracovních míst, o které bude ÚOOÚ znovu žádat.

VI. Úřad

VI.1. PERSONALISTIKA

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

K 1. lednu 2024 byl celkový počet systemizovaných služebních a pracovních míst v Úřadu 114. V důsledku změny systemizace k 1. červenci 2024 došlo k vytvoření dvou systemizovaných míst pro zajištění agend souvisejících s návrhem zákona o digitální ekonomice (DSA). K 31. prosinci 2024 byl celkový počet systemizovaných míst v Úřadu 116.

Do služebního poměru bylo v roce 2024 nově přijato 14 státních zaměstnanců a 15 státních zaměstnanců služební poměr ukončilo, nebo došlo k jejich zařazení do jiného služebního úřadu. Do pracovního poměru bylo přijato 8 zaměstnanců, přičemž 10 zaměstnanců pracovní poměr ukončilo. K 1. lednu 2024 bylo v Úřadu v evidenčním stavu 106 zaměstnanců, k 31. prosinci 2024 jich bylo 105.

Průměrný přepočtený evidenční počet zaměstnanců za rok 2024 činil 103,28.

Dalších 49 osob vykonávalo v Úřadu činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr. Z toho 20 externích spolupracovníků vykonávalo činnosti spojené s rozhodováním rozkladové komise, 8 externích spolupracovníků zajišťovalo úklid objektu Úřadu a zbylí pracovníci s Úřadem spolupracovali zejména v oblasti expertních prací ve vztahu k informačním a komunikačním technologiím, procesům ekonomické a hospodářské správy nebo administrativní výpomoci.

V Úřadu pracují převážně zaměstnanci ve věku mezi 31 až 60 lety. Seniorní zaměstnanci mají kromě odpovídajícího vzdělání dlouhodobou praxi a velké zkušenosti, které předávají novým zaměstnancům. Předpoklad vysokoškolského vzdělání je stanoven u tří čtvrtin funkčních míst v Úřadu, zbývající čtvrtina míst předpokládá dosažení úplného středoškolského vzdělání.

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

Zvláštní část úřednické zkoušky pro obor Ochrana osobních údajů zajišťovanou Úřadem absolvovalo 17 žadatelů, z toho 15 žadatelů složilo zkoušku úspěšně.

Členění zaměstnanců Úřadu podle věku a pohlaví – stav k 31. prosinci 2024

Celý soubor	muži	ženy	celkem
do 20 let	0	0	0
od 21 do 30 let	2	7	9
od 31 do 40 let	14	8	22
od 41 do 50 let	9	16	25
od 51 do 60 let	12	19	31
61 a více	8	10	18
celkem	45	60	105

Také v roce 2024 plynule pokračoval chod jednotlivých procesů personální správy Úřadu, a to v návaznosti na vývoj legislativy v oblasti státní služby a pracovněprávních vztahů. Novela nařízení vlády ČR o pravidlech pro organizaci služebního úřadu účinná od 1. července 2024 znamenala nezbytnou a rozsáhlou reorganizaci Úřadu za účelem splnění podmínek minimálního počtu systemizovaných míst v jednotlivých útvarech.

Zásadní organizační změnou bylo zřízení nového odboru stížností a digitálních agend, jehož úkolem bude mimo jiné analýza, koordinace a metodické usměrňování činností souvisejících s evropskými předpisy upravujícími digitální ekonomiku (zejména akt o digitálních službách, akt o datech, akt o správě dat, akt o digitálních trzích či akt o umělé inteligenci), monitorování činnosti evropských orgánů působících v oblasti digitálních agend a součinnost s dalšími vnitrostátními orgány, kterým byla svěřena působnost na úseku digitálních agend, při prosazování ochrany osobních údajů. Nový odbor bylo nutné zřídit z vlastních zdrojů Úřadu na úkor stávajících agend. Na nové organizační nastavení se Úřad v průběhu 3. čtvrtletí roku 2024 postupně plně adaptoval.

Identifikované personální potřeby Úřadu

Personální potřeby identifikované již v roce 2023 byly v roce 2024 zohledněny prostřednictvím rozpočtových opatření, změn systemizace v průběhu roku a návrhu rozpočtu na rok 2025 pouze v minimálním rozsahu 4 nových systemizovaných míst. Z toho pouze 2 místa byla zabezpečena i po finanční stránce v rámci navýšení celkových výdajů rozpočtové kapitoly.

V roce 2024 ÚOOÚ provedl aktualizaci identifikovaných personálních potřeb. V rámci různých fází přípravy státního rozpočtu na rok 2025, střednědobého výhledu na léta 2026–2027 a systemizace na rok 2025 Úřad opakovaně uplatňoval své potřeby formou požadavků, které však ze strany Ministerstva financí pro rok 2025 nebyly zohledněny. Z hlediska významu těchto potřeb však bude nutnost jejich zabezpečení v průběhu času nabývat stále vyšší intenzity.

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím – 1 systemizované služební místo

Rozšíření působnosti Úřadu o agendy zákona č. 106/1999 Sb. bylo nezbytné reflektovat i v rovině personálního zabezpečení, aby bylo plnění této nové působnosti zajištěno v zákonných mezích. Agenda svobodného přístupu k informacím byla Úřadu paradoxně svěřena v době, kdy výrazně vzrostla zátěž v souvislosti s účinností obecného nařízení o ochraně osobních údajů, což by již samo o sobě zdůvodňovalo personální posílení. ÚOOÚ 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 orgánem přezkumným pro cca 15 000 povinných subjektů. Množství podřízených povinných subjektů se navíc oproti původním předpokladům průběžně rozšiřuje na základě judikatury správních soudů. (Lze zmínit například rozsudek Nejvyššího správního soudu čj. Komp 3/2021-26 ze dne 16. února 2022, v jehož důsledku narostl počet podřízených povinných subjektů o dalších zhruba 1 000.)

Odbor práva na informace se v roce 2024 podobně jako v roce předchozím potýkal s potížemi způsobenými nedostatečným personálním zajištěním. Pro výkon předmětné agendy Úřad aktuálně disponuje 10 systemizovanými služebními místy, z čehož pouze pět bylo pro tuto agendu nově vytvořeno za účelem výkonu působnosti v oblasti svobodného přístupu k in-

formacím. 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 zvláště v prvních letech účinnosti novely zákona o svobodném přístupu k informacím z roku 2019 nastupoval bez vlastního přičinění namísto původního žalovaného. 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 neustálého nárůstu počtu vyřizovaných věcí důvodem nesnadného obsazování uvolněných míst.

Členění zaměstnanců Úřadu podle vzdělání a pohlaví – stav k 31. prosinci 2024

Celý soubor	muži	ženy	celkem
Základní	0	0	0
Střední odborné + VL	1	0	1
Střední odborné	0	0	0
Úplné střední všeobecné	2	3	5
Úplné střední odborné + VL	0	0	0
Úplné střední odborné	5	12	17
Vyšší odborné vzdělání	0	1	1
Vysokoškolské – bakalářské	0	3	3
Vysokoškolské – magisterské a vyšší	37	41	78
celkem	45	60	105

Pro úplnost lze doplnit, že Petiční výbor Poslanecké sněmovny Parlamentu ČR již v roce 2020 doporučil 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.

Nové evropské systémy – 3 systemizovaná služební místa

Od roku 2025 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 o tzv. rámec pro interoperabilitu mezi informačními systémy EU v oblasti hranic a víz (Interoperabilita). V případě všech těchto systémů příslušná evropská právní norma ukládá národním dozorovým orgánům nové povinnosti. Jedná se zejména o 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. Navíc dozorovým úřadům vzniknou ve vztahu ke všem systémům další povinnosti jako 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 unijních nařízení, kterými jsou výše uvedené systémy zaváděny, je stanovena povinnost členských států zajistit pro svůj dozorový úřad dostatek zdrojů k plnění všech úkolů, které dané nařízení členským státům ukládá.

Národní Schengenský implementační plán 2021, který slouží k naplňování cílů *Koncepce schengenské spolupráce 2021–2027*, stanovil také 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 byl 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*“.

DSA – 2 systemizovaná služební místa

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 spadající 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 je návrh ve fázi projednávání Poslaneckou sněmovnou Parlamentu ČR.

Návrh zákona zavádí 2 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 4 nových systemizovaných služebních míst. Požadavek na vytvoření těchto míst byl projednán a odsouhlasen na úrovni ministra financí a ministra průmyslu a obchodu s tím, že dvě systemizovaná místa vznikla od 1. července 2024 na základě změny systemizace schválené vládou České republiky dne 26. června 2024. Další dvě systemizovaná místa měla vzniknout od 1. ledna 2025, avšak nevzniknou, protože nedošlo k zapracování dříve dojednaných výsledků jednání k uvedené problematice v rámci přípravy návrhu státního rozpočtu na rok 2025. Požadavek však s ohledem na nezbytnost zajištění agendy stále trvá.

Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679 – 5 systemizovaných služebních míst

V současné době je v rámci legislativního procesu EU řešena podoba návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679. Dá se předpokládat, že procesní nařízení v průběhu

roku 2025 nabude účinnosti. Toto nařízení stanoví množství nových povinností a postupů při vyřizování stížností týkajících se přeshraničního zpracování osobních údajů, které zásadně navýší administrativní náročnost vyřizování těchto věcí.

Již nařízení (EU) 2016/679 pro takové případy stanoví spolupráci mezi vedoucím dozorovým úřadem a dotčenými dozorovými úřady, avšak jen pro řešení návrhu rozhodnutí o vyřízení věci (tj. až ve zcela závěrečné fázi vyřizování věci). Procesní nařízení předpokládá formalizovanou spolupráci po celou dobu šetření stížnosti, včetně nejen zasílání např. dokumentů stěžovatelů a vyšetřovaných stran, ale i vypracovávání nových dokumentů. Návrh procesního nařízení obsahuje rovněž nová práva pro stěžovatele (např. přístup ke spisu či možnost vyjádřit se k závěrům vedoucího dozorového úřadu), jejichž naplnění ještě navýší administrativní náročnost celého procesu.

V posledních letech je ÚOOÚ navrhován jakožto vedoucí dozorový úřad ročně přibližně ve 30 případech stížností týkajících se přeshraničního zpracování osobních údajů. Lze předpokládat, že tento počet s přijetím procesního nařízení poroste.

Vzhledem k výše uvedeným skutečnostem je zcela nezbytné, aby byl ÚOOÚ posílen o 5 systemizovaných míst, aby mohly být nové procedury a postupy řešeny včas a nedocházelo k průtahům v řešení. Jedná se o minimalistický předpoklad nutnosti posílení Úřadu toliko pro přípravu na adaptaci nařízení, který bude dále významně ovlivněn konečnou podobou procesního nařízení.

Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy – 3 systemizovaná služební místa

Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy předpokládá pro Úřad dozor nad určitými aspekty politické reklamy, konkrétně nad technikami cílení a doručování reklamních sdělení v kontextu online reklamy. V rámci této nové agendy lze předpokládat nárůst zcela nového druhu stížností, což si vyžádá lidské zdroje nejen na vyřizování těchto stížností, ale s ohledem na novost agendy též lidské zdroje na nastavení přístupu k této agendě (např. vytváření stanovisek či metodik).

Nařízení zároveň předpokládá výraznou koordinaci zúčastněných orgánů veřejné moci nejen v rámci České republiky, ale také napříč Evropskou unií a na úrovni Evropské unie. Zajištění takové spolupráce si žádá další personální posílení.

S ohledem na uvedené skutečnosti Úřad žádá o tři systemizovaná služební místa na výkon agendy dle předmětného nařízení.

Celkové navýšení prostředků na platy a příslušenství

Ve smyslu shora uvedeného se jedná o identifikaci potřeby vzniku nových 14 systemizovaných služebních míst. K zabezpečení identifikovaných potřeb je nutné navýšit objem prostředků na platy na RP 5013 v celoročním vyjádření o 9 174 816 Kč s trvalým vlivem.

V rámci úpravy rozpočtu kapitoly bude nezbytné v této souvislosti zajistit i související příslušenství, které činí v celoročním vyjádření celkem 3 192 835 Kč a zahrnuje:

- navýšení sociálního pojištění za zaměstnavatele na RP 5031 s trvalým vlivem 2 275 354 Kč;
- navýšení zdravotního pojištění za zaměstnavatele na RP 5032 s trvalým vlivem: 825 733 Kč;
- navýšení přídělu do FKSP na RP 5342 s trvalým vlivem: 91 748 Kč.

Celkem se tedy jedná o legitimní potřebu navýšení výdajů rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů o 12 367 651 Kč, a to s trvalým vlivem.

VI.2. MEDIÁLNÍ KOMUNIKACE

Komunikační činnost ÚOOÚ byla v roce 2024 směřována k laické i odborné veřejnosti. Oproti předcházejícímu meziročnímu srovnání mezi lety 2022 a 2023 (+ 113 %) Úřad ohledně tématu ochrany osobních údajů vykázal mírné posílení mediálního zásahu, konkrétně + 15%.

Hlavní témata v oblasti mediální komunikace ÚOOÚ v roce 2024 navazovala na činnost a rozhodování partnerských dozorových úřadů, na vlastní činnost Úřadu a reflektovala mediální zájem v závislosti na společenském dění v ČR. Mezi mediálně nejvýznamnější témata aktivně komunikovaná Úřadem ve vazbě na činnost EDPB patří společná koordinovaná akce evropských dozorových Úřadů CEF 2024, zaměřená na postavení a úlohu pověřenců pro ochranu osobních údajů v rámci privátních i veřejných subjektů, rozhodnutí italského dozorového úřadu o porušení ochrany osobních údajů ze strany společnosti OpenAI provozující internetovou platformu ChatGPT a vydání stanoviska EDPB pro užívání modelu *consent or pay*.

Z domácích témat bylo Úřadem aktivně komunikováno udělení pokuty přes 351 milionů korun společnosti Avast Software s.r.o. za porušení GDPR neoprávněným zpracováním osobních údajů uživatelů jejího antivirového programu a jeho rozšíření internetových prohlížečů (Browser Extensions). Aktivně byly komunikovány semináře Úřadu určené odborné veřejnosti a vydání věcné metodiky k instalaci a provozování kamerových systémů, dále *Doporučení pro provozování kamerových systémů bezpilotními letadly* a *Doporučení pro provozování kamerových systémů ve školách a školských zařízeních*. Mediálně podpořeno bylo doporučení Úřadu k postavení pověřenců pro ochranu osobních údajů a varování ÚOOÚ před katalogovými podvody prováděnými formou zasílání e-mailových zpráv s fakturami. Již tradičně Úřad komunikačně podpořil vyhlášení nejlepšího pověřence pro ochranu osobních údajů za rok 2024, organizované českým Spolkem pro ochranu osobních údajů.

Nejsilnější zájem médií z pohledu četnosti dotazů zaznamenaly výsledky Úřadem prováděných šetření v případě správního řízení s TV Nova ve věci vysílání přímého přenosu ze soudního přelíčení s bývalým poslancem TOP 09 Dominikem Ferim, kde byly zveřejněny všechny dostupné osobní údaje účastníků řízení, včetně osobních údajů svědků. Dále se média zajímala o výsledek šetření stížnosti bývalého prezidenta České republiky

Miloše Zemana na postup a ochranu jeho osobních údajů ze strany Ústřední vojenské nemocnice Praha během jeho hospitalizace a o výsledek posouzení relevantnosti zveřejnění videostreamu zásahu Městské policie Praha proti moderátorovi České televize Jakubovi Železnému na Václavském náměstí v Praze. Média rovněž projevila zájem o edukativní komunikační podporu v rámci tématu sousedského provozování kamerových systémů.

VI.3. HOSPODAŘENÍ

Odbor ekonomiky a provozu v oblasti hospodaření Úřadu zodpovídá za řízení 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 2024

Hospodaření ÚOOÚ se v roce 2024 řídilo zákonem č. 433/2023, o státním rozpočtu České republiky na rok 2024. K zajištění činnosti Úřadu byly schváleny výdaje v celkové výši 186 278 tis. Kč a celkové příjmy ve výši 1 000 tis. Kč.

Ukazatele kapitoly 343 – Úřad pro ochranu osobních údajů

Souhrnné ukazatele	v Kč
Příjmy celkem	1 000 000
Výdaje celkem	186 277 988

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	186 277 988

Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	73 406 787
Povinné pojistné placené zaměstnavatelem*)	24 811 496
Základní příděl fondu kulturních a sociálních potřeb	715 159
Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	11 250 228
Platy zaměstnanců na služebních místech dle zákona o státní službě	53 963 247
Platy zaměstnanců v pracovním poměru odvozované od platů ústavních činitelů	6 302 400
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	9 404 000

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

ČERPÁNÍ ROZPOČTU V ROCE 2024

PŘÍJMY

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů byl naplněn částkou 352 898,05 tis. Kč

Jednalo se především o:

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

Úřad pro ochranu osobních údajů jako nezávislý orgán nemá příjmy z vlastní činnosti standardně zahrnuty do svého rozpočtu, veškeré příjmy Úřadu jsou odváděny do státního rozpočtu.

VÝDAJE

Čerpání výdajů kapitoly 343 – Úřad pro ochranu osobních údajů dosáhly výše 164 447,80 tis. Kč a zahrnují:

- náklady na platy a ostatní platby za provedenou práci, včetně souvisejících výdajů,
- kapitálové výdaje spojené se správou a údržbou budovy Úřadu, s obnovou informačních systémů, a to jak IS samotného Úřadu, tak i IS ORG jako prvku kritické informační infrastruktury státu,
- běžné výdaje související s chodem Úřadu a IT systémů, tj. zejména položky spojené s nákupem drobného hmotného majetku, materiálu, IT služeb, služeb spojených s provozem, údržbou a zabezpečením budovy Úřadu, výdaje na tuzemské i zahraniční cestovné, vzdělávání apod.,
- další výdaje představují mimořádné výdaje, jako například odvod do státního rozpočtu za porušení rozpočtové kázně, který byl Úřadu vyměřen platebním výměrem ze dne 8. března 2024 ve výši 2 513 788 Kč. Proti platebnímu výměru podal Úřad odvolání dne 8. dubna 2024. Přestože odvod vyměřený Úřadu platebním výměrem dosud není splatný, neboť odvolací řízení stále probíhá, nemá výše uvedené vliv na penále, které se počítá ode dne následujícího po dni, kdy došlo k porušení rozpočtové kázně (do dne, kdy byly prostředky odvedeny), a to ve výši „0,4 promile z částky odvodu za každý den prodlení“, bez ohledu na to, zda platební výměr nabyl právní moci nebo zda ještě běží odvolací řízení. Ačkoliv Úřad nadále se stanoveným odvodem nesouhlasí, s ohledem na zásadu péče řádného hospodáře byl nucen provést úhradu vyměřeného odvodu, aby zabránil navyšování penále.

Platy zaměstnanců a ostatní platby za provedenou práci, včetně souvisejících výdajů

Čerpání rozpočtu na platy zaměstnanců, ostatní výdaje za provedenou práci a související výdaje, včetně základního přídělu FKSP ve výši 96 021,41 tisíc Kč, je dáno kvalifikační strukturou a plněním plánu počtu pracovníků.

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

V souladu se schválenou dokumentací programu 343V02 „Rozvoj a obnova materiálně technické základny Úřadu pro ochranu osobních údajů od r. 2022" bylo v roce 2024 celkem čerpáno **3 368,54 tis. Kč.** Čerpání představovalo kapitálové výdaje na rozvoj a obnovu IS ORG (1 609,43 tis. Kč) a rozvoj a obnovu vnitřního IT Úřadu (1 759,11 tis. Kč).

Přehled čerpání rozpočtu v roce 2024

Položka	Název položky	Schválený rozpočet v Kč	Konečný rozpočet v Kč	Skutečnost v Kč
PŘÍJMY		**1 000 000,00**	**0,00**	**352 898 047,65**
1	Daňové příjmy			7 740,00
2	Nedaňové příjmy	1 000 000,00	0,00	352 855 903,33
4	Přijaté transfery			34 404,32
VÝDAJE		**186 277 988,00**	**198 073 884,79**	**164 447 795,53**
5	Běžné výdaje	176 873 988,00	180 585 552,79	161 079 254,13
50	Platy a obdobné a související výdaje	98 218 283,00	96 516 640,00	95 320 197,00
501	Platy	71 515 875,00	70 247 303,00	70 111 686,00
5011	Platy zaměstnanců v pracovním poměru vyjma zaměstnanců na služebních místech	11 250 228,00	10 090 458,00	9 962 981,00
5013	Platy zaměstnanců na služebních místech podle zákona o státní službě	53 963 247,00	54 792 805,00	54 790 253,00
5014	Platy zaměstnanců v pracovním poměru odvozené od platů ústavních činitelů	6 302 400,00	5 364 040,00	5 358 452,00
502	Ostatní platby za provedenou práci	1 890 912,00	1 890 912,00	1 580 535,00
5021	Ostatní osobní výdaje	1 890 912,00	1 890 912,00	1 580 535,00
503	Povinné pojistné placené zaměstnavatelem	24 811 496,00	24 378 425,00	23 627 976,00
5031	Povinné pojistné na sociální zabezpečení	18 204 885,00	17 887 130,00	17 282 889,00
5032	Povinné pojistné na veřejné zdravotní pojištění	6 606 611,00	6 491 295,00	6 345 087,00
51	Výdaje na neinvestiční nákupy a související výdaje	77 924 606,00	79 136 838,79	60 893 330,83

Přehled čerpání rozpočtu v roce 2024 (pokračování)

Položka	Název položky	Schválený rozpočet v Kč	Konečný rozpočet v Kč	Skutečnost v Kč
512	Výdaje na některé úpravy hmotných věcí a pořízení některých práv k hmotným věcem	0,00	10 000,00	
513	Výdaje na nákup materiálu	1 586 000,00	2 461 000,00	1 053 689,67
514	Úroky a ostatní finanční výdaje	40 000,00	50 000,00	25 276,45
515	Výdaje na nákup vody, paliv a energie	3 590 000,00	3 575 000,00	2 882 071,13
516	Výdaje na nákup služeb	67 838 906,00	67 049 081,79	54 966 156,49
517	Výdaje na ostatní nákupy	2 788 000,00	3 870 057,00	793 015,92
519	Výdaje související s neinvestičními nákupy, příspěvky, náhrady a věcné dary	2 081 700,00	2 121 700,00	1 173 121,17
53	Neinvestiční transfery veřejnoprávním subjektům a mezi peněžními fondy téže osoby a platby daní	731 099,00	3 232 074,00	3 222 238,30
534	Neinvestiční převody vlastním fondům a ve vztahu k útvarům bez plné právní subjektivity	715 159,00	702 346,00	701 210,30
536	Ostatní neinvestiční transfery jiným veřejným rozpočtům, platby daní a další povinné platby	15 940,00	2 529 728,00	2 521 028,00
54	Neinvestiční transfery a některé náhrady fyzickým osobám	0,00	1 700 000,00	1 643 488,00
549	Ostatní neinvestiční transfery fyzickým osobám	0,00	1 700 000,00	1 643 488,00
6	Kapitálové výdaje	9 404 000,00	17 488 332,00	3 368 541,40
61	Investiční nákupy a související výdaje	9 404 000,00	17 488 332,00	3 368 541,40
611	Pořízení dlouhodobého nehmotného majetku	0,00	1 878 717,00	1 711 073,10
612	Pořízení dlouhodobého hmotného majetku	9 404 000,00	15 609 615,00	1 657 468,30

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. prosince 2024.

VI.4. ÚČETNÍ ZÁVĚRKA

Schválení účetní závěrky za rok 2024 spolu s informací o jejím předání proběhne v řádném termínu do 31. července 2025 dle Přílohy č. 4 vyhlášky č. 383/2009 Sb., o účetních záznamech v technické formě vybraných účetních jednotek a jejich předávání do centrálního systému účetních informací státu a o požadavcích na technické a smíšené formy účetních záznamů. V souladu se sdělením Ministerstva financí ČR 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.

VI.5. INTERNÍ AUDIT

Činnost interního auditu Úřadu upravuje zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, prováděcí vyhláška č. 416/2004 Sb., k zákonu o finanční kontrole ve veřejné správě, a globální standardy interního auditu. Služební místo interního auditora bylo v roce 2024 organizačně odděleno od řídících a výkonných struktur. Auditor je funkčně nezávislý a je podřízen přímo předsedovi Úřadu.

V oblasti interního auditu se ÚOOÚ soustředil na 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 a zajišťování konzultační činnosti.

Činnost interního auditora v roce 2024 vycházela ze střednědobého plánu auditů, z výsledků předchozích auditů, z požadavků vedoucích zaměstnanců Úřadu a z ročního plánu interního auditu v souvislosti s riziky, identifikovanými na základě výsledků veřejnosprávních kontrol.

Pro rok 2024 byly naplánovány a realizovány audit **Poskytování záloh v podmínkách ÚOOÚ** za auditované období roku 2023 a audit **Vnitřní kontrolní systém ÚOOÚ** za auditované období roku 2024.

Závěry provedeného auditu **Poskytování záloh v podmínkách ÚOOÚ** jsou pozitivní, neboť auditní zpráva konstatovala splnění prověřovaného ustanovení § 49 odst. 2 zákona č. 218/2000 Sb., o rozpočtových pravidlech, u všech záloh, kde nebyly zjištěny nedostatky. Průběžně také v auditovaném období docházelo k úpravám dotčených vnitřních směrnic Úřadu, aby byla zajištěna jejich aktuálnost, a tak došlo k dalšímu zlepšení fungování vnitřního kontrolního systému Úřadu. Kromě toho došlo v rámci Úřadu ke zlepšení v prověřování hospodárnosti a rovněž k významnému zlepšení v oblasti veřejných zakázek, kde se zálohy u žádné z nich nevyskytovaly.

Audit **Vnitřní kontrolní systém ÚOOÚ,** jehož záměrem bylo prověřit přiměřenost a účinnost vnitřního kontrolního systému Úřadu, byl realizován v souladu s požadavkem usta-

novení § 30 odst. 7 zákona č. 320/2001 Sb., o finanční kontrole. Audit ve zjištěných závěrech konstatoval, že:

- Vnitřní kontrolní systém Úřadu naplňuje požadavky § 25 odst. 1 písm. a), b), c) zákona č. 320/2001 Sb. tím, že je způsobilý včas zjišťovat, vyhodnocovat a minimalizovat provozní, finanční, právní a další rizika vznikající v souvislosti s plněním schválených záměrů a cílů. Procesy sledování hospodárnosti, efektivnosti a účelnosti jsou nastaveny, a to včetně postupů pro včasné podávání relevantních informací a opatření k nápravě.

- V rámci vnitřního kontrolního systému Úřadu je zaveden rozsah a oddělenost pravomocí a odpovědností, které jsou potřeba při nakládání s veřejnými prostředky, včetně úplného a přesného vymezení povinností ve vztahu k jimi plněným úkolům v souladu s ustanovením § 25 odst. 2 písm. a), b) zákona č. 320/2001 Sb.

- Vnitřní kontrolní systém Úřadu rovněž v souladu s požadavky § 25 odst. 2 písm. c) zákona č. 320/2001 Sb. zajišťuje, aby o všech operacích a kontrolách byl proveden záznam a vedena příslušná dokumentace tím, že elektronický systém Croseus umožňuje dohledat a zdokumentovat průkaznou auditní stopu u všech záznamů.

- V rámci Úřadu je kladen důraz na včasnou aktualizaci vnitřních směrnic Úřadu a jejich vzájemný soulad. V této souvislosti interní audit v roce 2024 konstatoval zlepšení a zrychlení těchto procesů, včetně plnění harmonogramu IAŘ (interních aktů řízení) jakožto předpokladu k zabezpečení souladu vnitřních norem s aktuálními právními předpisy, což má pozitivní vliv na funkčnost vnitřního kontrolního systému Úřadu.

- Nástrojem řídící kontroly uvnitř Úřadu je systém Croseus, jenž dokáže odhalit jednotlivé výskyty nesouladů v souladu s požadavky § 25 odst. 1 písm. b) zákona č. 320/2001 Sb. tím, že v náhledu na „porušení“ či „rizika“ vykazuje upozornění na výskyt nesrovnalosti, resp. jednotlivých typů nesouladů (např. „nezdůvodněné porušení data splatnosti“).

- Naprostá většina auditovaných nesrovnalostí (93 %), zaznamenaná v systému Croseus v monitorovaném období, byla ve skutečnosti zdůvodněná, tzn. nejednalo se o reálné porušení či riziko.

- Analýzou Croseus Monitoring, který se týká vkládání údajů o smlouvách Úřadu do registru smluv, bylo zjištěno šest případů v režimu „porušení“ z minulých let. Interní audit shledal, že u všech případů se jednalo o formální skutečnosti, které nevedly k sankci v podobě zrušení smluv od počátku na základě ustanovení § 7 odst. 1 zákona č. 340/2015 Sb., o registru smluv. Rovněž ostatní kategorie (režimy „ověřit“ a „v pořádku - formalita“) byly interním auditem prověřeny a nedostatky nebyly zjištěny.

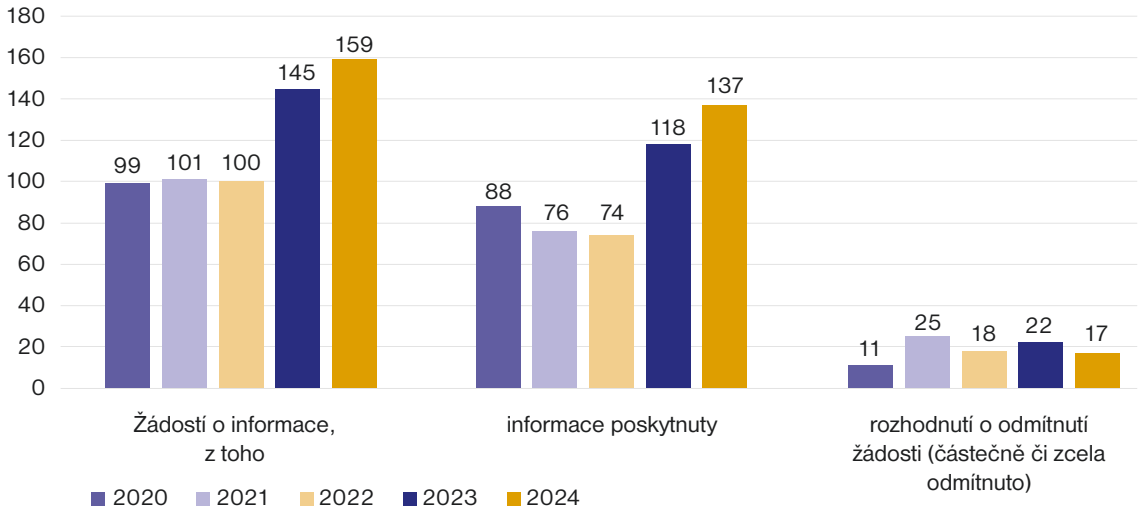
Celkový závěr auditu Vnitřní kontrolní systém ÚOOÚ za auditované období roku 2024 ve svém souhrnu konstatoval, že vnitřní kontrolní systém v rámci Úřadu je zavedený, udržovaný a funkční. Nedostatky popsané v předmětné auditní zprávě nebyly závažné, resp. nebyly systémového charakteru, lze je odstranit nebo již byly napraveny v průběhu interního auditu.

Závěry zpráv interního auditu v roce 2024 potvrdily, že přijatá opatření jdou správným směrem. Funkčnost dalších přijatých opatření bude přezkoumána interními audity naplánovanými pro rok 2025.

VI.6. POSKYTOVÁNÍ INFORMACÍ ÚŘADEM PODLE ZÁKONA Č. 106/1999 SB. JAKO POVINNÝM SUBJEKTEM

Úřad i v roce 2024 plnil své povinnosti povinného subjektu dle zákona č. 106/1999 Sb. a poskytoval informace vztahující se k jeho působnosti v rozsahu stanoveném tímto zákonem. ÚOOÚ provedl aktualizaci informací, které je dle § 5 odst. 1 a 2 zákona č. 106/1999 Sb. povinen zpřístupnit, na nových webových stránkách Úřadu uoou.gov.cz, které lze nově zobrazit na elektronické úřední desce umístěné na veřejně přístupném místě. Stejným způsobem Úřad zpřístupňoval informace poskytnuté dle § 5 odst. 3 zákona č. 106/1999 Sb.

Žádosti podle zákona č. 106/1999 Sb. v letech 2020–2024



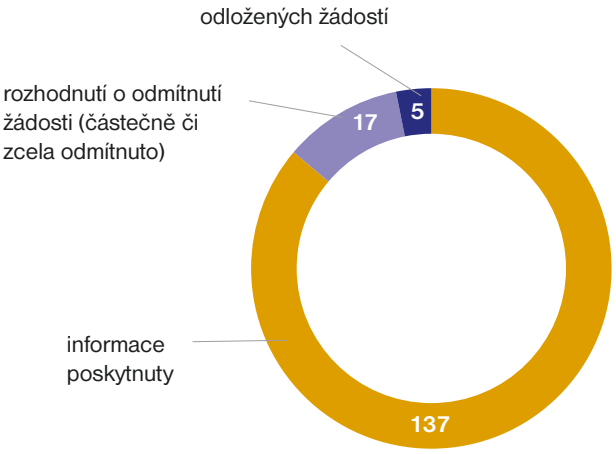
V roce 2024 Úřad zpracoval 159 žádostí podaných podle zákona č. 106/1999 Sb. Oproti předchozím letům došlo k opětovnému nárůstu počtu žádostí, přičemž reálný počet dotazů na základě zákona č. 106/1999 Sb. byl mnohonásobně vyšší, protože v převážné většině žádostí bylo požadováno poskytnutí několika informací zároveň.

V roce 2024 vydal Úřad rozhodnutí o odmítnutí žádosti, případně části žádosti v 17 případech. Rozhodnutí o odmítnutí celé žádosti bylo Úřadem vydáno v 10 případech. Nejčastěji bylo poskytnutí informace odmítnuto podle § 2 odst. 4, § 11b, případně § 2 odst. 3 zákona č. 106/1999 Sb., kdy se žadatelé domáhali zejména výkladu právních norem jiného věcného gestora, uvedení podrobností o jednotlivých krocích Úřadu, případně písemností, které Úřad zpracoval. Obecné dotazy v rozsahu působnosti Úřadu v oblasti ochrany osobních údajů spadající pod zákonné výluky zákona č. 106/1999 Sb. byly v souladu s praxí předchozích let předávány oddělení konzultací k poskytnutí požadované informace.

Proti rozhodnutí povinného subjektu o odmítnutí žádosti či její části bylo v roce 2024 podáno pouze šest rozkladů. Ve čtyřech případech předseda Úřadu jako nadřízený orgán svým rozhodnutím rozklad zamítl a napadené rozhodnutí potvrdil. V jednom případě bylo rozhodnutí I. stupně zrušeno a vráceno k dalšímu řízení a jeden rozklad byl vyřešen autoremedurou, tzn. bylo mu plně vyhověno.

V roce 2024 byla podána jedna žaloba ve věci přezkoumání zákonnosti rozhodnutí povinného subjektu o odmítnutí části žádosti.

Způsob vyřízení žádostí o informace podle zákona č. 106/1999 Sb. v roce 2024



Naprostou většinu požadovaných informací poskytl Úřad v roce 2024 bezplatně. V roce 2024 Úřad vyměřil úhradu za mimořádně rozsáhlé vyhledání v šesti případech v celkové výši 485 719 Kč. Vyměřená úhrada byla zaplacena ve třech případech v celkové výši 19 273 Kč. Tři žádosti byly odloženy z důvodu neuhrazení požadované úhrady. Ve všech žádostech se jednalo o poskytnutí velkého množství dokumentů, které musely být Úřadem vyhledány a anonymizovány.

Ve dvou případech Úřad žádost odložil, neboť se nevztahovala k jeho působnosti.

V roce 2024 nebyly Úřadem poskytnuty žádné výhradní licence.

V roce 2024 obdržel Úřad čtyři stížnosti dle § 16a zákona č. 106/1999 Sb. Důvodem pro podání dvou z nich bylo poskytnutí neúplné informace a zbylé dvě byly podány pro neposkytnutí informace v zákonné lhůtě. Ve třech případech Úřad doplnil poskytnuté informace, případně informaci poskytl. V jednom případě neúplně poskytnuté informace byla stížnost předsedou Úřadu shledána nedůvodnou.

VI.7. VYŘIZOVÁNÍ STÍŽNOSTÍ PODLE § 175 SPRÁVNÍHO ŘÁDU

Fyzickým i právnickým osobám nespokojeným s výstupy správních orgánů je umožněno podat stížnost dle § 175 zákona č. 500/2004 Sb. Dotčené osoby se mohou obracet na správní orgány se stížnostmi proti postupu správního orgánu nebo proti nevhodnému chování úředních osob. Takovou možnost stěžovatelé mají v případě, kdy jim správní řád neposkytuje jiné prostředky ochrany jako odvolání nebo jiné řádné či mimořádné opravné prostředky.

Úřad v roce 2024 obdržel celkem 27 nových podání podle § 175 správního řádu, a to 24 stížností a 3 žádosti o přešetření vyřízení stížnosti. Ve 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.

Ve stejném období Úřad vyřídil celkem 24 podání podle § 175 správního řádu, a to 21 stížností a 3 žádosti o přešetření vyřízení stížnosti. Z tohoto počtu bylo 6 stížností vyhodnoceno jako důvodných nebo částečně důvodných, 13 nedůvodných a 2 byly vyřízeny jiným způsobem. Všechny žádosti o přešetření byly vyhodnoceny jako nedůvodné. Ve všech případech stížnosti směřovaly proti postupu úřední osoby, žádná proti chování úřední osoby. Zbývajícími 5 stížnostmi z roku 2024 se bude Úřad zabývat v roce 2025.

VI.8. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

Úřad jako ústřední správní úřad pro oblast ochrany osobních údajů, tedy orgán veřejné moci, jmenoval v souladu s čl. 37 odst. 1 písm. a) obecného nařízení pověřence pro ochranu osobních údajů, jehož hlavní úkoly vyplývají z čl. 39 obecného nařízení. Pověřenec Úřadu zejména poskytuje informace a poradenství zaměstnancům, kteří se podílejí na zpracování osobních údajů, a zodpovídá dotazy subjektů údajů, jejichž osobní údaje zpracovává sám Úřad.

V roce 2024 pověřenec poskytoval konzultace uvnitř Úřadu spojené především s problematikou záznamů o činnostech zpracování, posouzení vlivu na ochranu osobních údajů, odběru novinek a zpracovatelské smlouvy s technickým provozovatelem webových stránek Úřadu. 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 až 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.

VI.9. ÚŘAD V ČÍSLECH

Dozorová činnost v oblasti ochrany osobních údajů

PODNĚTY A STÍŽNOSTI

Počet obdržených stížností	680
zahájeno šetření	680
Počet obdržených podnětů (včetně postoupení od orgánů veřejné moci a šetření zahajovaných ex officio)	1658
zahájeno šetření	1258

OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ DLE ČL. 33 GDPR

Počet ohlášení porušení zabezpečení osobních údajů	336
Počet doplnění ohlášení porušení zabezpečení osobních údajů	143

VYŘÍZENO PODNĚTŮ A STÍŽNOSTÍ (MIMO RÁMEC KONTROL A SPRÁVNÍCH ŘÍZENÍ)

Odpovědí po prošetření	1238
Odložením či předáním věcně příslušnému orgánu	119

KONTROLA

Počet zahájených kontrol	14
Počet ukončených kontrol	12
Počet podaných námitek dle § 13 kontrolního řádu	5
Počet vyřízených námitek (včetně předchozích let)	6
vyhověno	0
vráceno k došetření	0
částečně vyhověno	3
nedůvodné	3
Počet pravomocně uložených trestů za nesoučinnost podle kontrolního řádu	3
v celkové výši	200 000 Kč

SPRÁVNÍ ŘÍZENÍ

Počet zahájených správních řízení	35
Počet pravomocně ukončených správních řízení o přestupku	20
počet pokut	6
v celkové výši	351 234 000 Kč
napomenutí	12
upuštěno od potrestání dle § 63 odst. 5 zákona č. 110/2019 Sb.	2
Počet podaných rozkladů	9
Počet vyřízených rozkladů (včetně předchozích let)	11
potvrzeno rozhodnutí I. stupně a rozklad zamítnut	5
zrušeno rozhodnutí I. stupně a vráceno k dalšímu řízení	6
zrušeno rozhodnutí I. stupně a řízení zastaveno	0
změněno rozhodnutí I. stupně	0

DOTAZY A KONZULTACE

Počet písemných dotazů	1331
Počet telefonických dotazů na konzultační lince	1273

Rozhodovací činnost v oblasti svobodného přístupu k informacím

ÚŘAD JAKOŽTO NADŘÍZENÝ ORGÁN POVINNÝCH SUBJEKTŮ, JEJICHŽ NADŘÍZENÝ ORGÁN NELZE URČIT PODLE § 178 SPRÁVNÍHO ŘÁDU (§ 20 ODST. 5 ZÁKONA Č. 106/1999 SB.)

Odvolání	
Informační příkaz	12
V části vydán informační příkaz, v části rozhodnutí povinného subjektu zrušeno a věc vrácena k novému projednání	8
V části vydán informační příkaz, v části rozhodnutí povinného subjektu potvrzeno	4
Rozhodnutí povinného subjektu potvrzeno	44
Rozhodnutí povinného subjektu zrušeno, věc vrácena k novému projednání	93
Rozhodnutí povinného subjektu částečně potvrzeno, v části rozhodnutí povinného subjektu zrušeno a věc vrácena k novému projednání	2
Rozhodnutí povinného subjektu změněno a ve zbytku potvrzeno	6
Ostatní způsoby vyřízení	14
Stížnost na postup povinného subjektu	
Informační příkaz	1
Postup potvrzen	33
Příkaz povinnému subjektu vyřídit žádost	55
V části postup potvrzen, v části příkaz povinnému subjektu vyřídit žádost	8
Výše úhrady požadované povinným subjektem snížena	27
Ostatní způsoby vyřízení	8
Opravný prostředek postoupen jinému subjektu z důvodu nepříslušnosti Úřadu	33

ÚŘAD JAKOŽTO PŘEZKUMNÝ ORGÁN (§ 16B ODST. 1 A 2 ZÁKONA Č. 106/1999 SB.)

Přezkumné řízení nezahájeno	60
Přezkumné řízení nezahájeno sdělením předsedy Úřadu	4
Pozhodnutí nadřízeného orgánu zrušeno, věc vrácena	9
Rozhodnutí nadřízeného orgánu zrušeno pro nicotnost	2

ÚŘAD JAKOŽTO ORGÁN PŘÍSLUŠNÝ K PŘIJÍMÁNÍ OPATŘENÍ PROTI NEČINNOSTI (§ 16B ODST. 3 ZÁKONA Č. 106/1999 SB.)

Nedůvodný podnět	75
Opatření proti nečinnosti	114

Dozorová činnost v oblasti obchodních sdělení

STÍŽNOSTI

Počet obdržených stížností	1425

VYŘÍZENO STÍŽNOSTÍ (MIMO RÁMEC KONTROL A SPRÁVNÍCH ŘÍZENÍ)

Upozorňujícím dopisem jednotlivým subjektům (šetření v méně závažných případech)	359

KONTROLA

Počet zahájených kontrol	13
Počet ukončených kontrol	9
Počet podaných námitek dle § 13 kontrolního řádu	3
Počet vyřízených námitek	1
vyhověno	0
vráceno k došetření	0
částečně vyhověno	0
nedůvodné	1
Počet pravomocně uložených trestů za nesoučinnost podle kontrolního řádu	2
v celkové výši	100 000 Kč

SPRÁVNÍ ŘÍZENÍ

Počet zahájených správních řízení	32
Počet pravomocně ukončených správních řízení	31
v celkové výši uložených pravomocných pokut	7 124 000 Kč
Počet podaných rozkladů	1
Počet vyřízených rozkladů (včetně předchozích let)	3
potvrzeno rozhodnutí I. stupně a rozklad zamítnut	3
zrušeno rozhodnutí I. stupně a vráceno k dalšímu řízení	0
zrušeno rozhodnutí I. stupně a řízení zastaveno	0
změněno rozhodnutí I. stupně	0

Úřad v soudních řízeních

SOUDNÍ PŘEZKUM ROZHODNUTÍ PŘEDSEDY ÚŘADU V OBLASTI OCHRANY OSOBNÍCH ÚDAJŮ A OBCHODNÍCH SDĚLENÍ

Městský soud v Praze		
Podané žaloby proti rozhodnutí o pokutě		2
Vydaná rozhodnutí		4
	žaloba se zamítá	4
	rozhodnutí se ruší a věc se vrací k dalšímu řízení	0
Nejvyšší správní soud		
Podané kasační stížnosti		3
Vydaná rozhodnutí		3
	kasační stížnost se zamítá	2
	kasační stížnost se odmítá	1

SOUDEM VYŽÁDANÁ VYJÁDŘENÍ ÚŘADU V SOUDNÍCH ŘÍZENÍCH VE VĚCI OCHRANY OSOBNÍCH ÚDAJŮ **5**

Poznámka: V souvislosti s adaptací GDPR bylo do zákona č. 99/1963 Sb. vloženo ustanovení § 114a odst. 2 písm. f), podle něhož má soud zjistit názor Úřadu, pokud předmět řízení bezprostředně souvisí s otázkou ochrany osobních údajů. Uvedené ustanovení aplikují soudy i ve správním soudnictví, na základě přiměřené aplikace zákona č. 99/1963 Sb. předvídané § 64 zákona č. 150/2002 Sb.; alternativně se na Úřad obracejí se žádostí o vyjádření s odkazem na § 74 odst. 1 téhož zákona, podle něhož může předseda senátu uložit i jiným osobám ebo úřadům, aby sdělily své stanovisko ve věci.

SOUDNÍ ŘÍZENÍ S ÚČASTÍ ÚŘADU TÝKAJÍCÍ SE ZÁKONA Č. 106/1999 SB. OZNÁMENÁ ÚŘADU **25**

Poznámka: 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.

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

ŽÁDOSTI O INFORMACE

Žádosti o informace	**159**
informace poskytnuty	137
rozhodnutí o odmítnutí žádosti (částečném či úplném)	17
odložených žádostí	5

ROZKLADY

Rozklady proti rozhodnutí	**6**
potvrzeno rozhodnutí I. stupně a rozklad zamítnut	4
zrušeno rozhodnutí I. stupně a vráceno k dalšímu řízení	1
změněno rozhodnutí I. stupně	0
zastaveno řízení o rozkladu pro zpětvzetí	0
rozklad zamítnut pro opožděnost	0
rozklad zamítnut pro nepřípustnost	0
rozklad vyřízen v autoremeduře prvním stupněm	1
zrušeno rozhodnutí I. stupně a příkázáno povinnému subjektu informaci poskytnout	0

STÍŽNOSTI

Stížnosti podané podle § 16a	**4**
stížnosti zcela vyhověno a informace poskytnuta v souladu s § 16a odst. 5	3
postup povinného subjektu potvrzen	1
povinnému subjektu bylo přikázáno poskytnout informaci	0
nadřízený orgán věc převzal a poskytl informaci sám	0
odmítnutí stížnosti	0
výše úhrady nadřízeným orgánem potvrzena	0
výše úhrady nadřízeným orgánem snížena	0

ÚHRADA NÁKLADŮ

Požadavek na úhradu nákladů za mimořádně rozsáhlé vyhledávání informací	**6**
uhrazené náklady za mimořádné vyhledávání informací	3

SEZNAM ODKAZOVANÝCH ZÁKONŮ

Zákon č. 99/1963 Sb.	Zákon č. 99/1963 Sb., občanský soudní řád
Zákon č. 21/1992 Sb.	Zákon č. 21/1992 Sb., o bankách
Zákon č. 40/1995 Sb.	Zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů
Zákon č. 106/1999 Sb.	Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
Zákon č. 101/2000 Sb.	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
Zákon č. 218/2000 Sb.	Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla)
Zákon č. 320/2001 Sb.	Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů
Zákon č. 150/2002 Sb.	Zákon č. 150/2002 Sb., soudní řád správní
Zákon č. 480/2004 Sb.	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.	Zákon č. 500/2004 Sb., správní řád
Vyhláška č. 416/2004 Sb.	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.
Zákon č. 127/2005 Sb.	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
Zákon č. 262/2006 Sb.	Zákon č. 262/2006 Sb., zákoník práce
Zákon č. 273/2008 Sb.	Zákon č. 273/2008 Sb., o Policii České republiky
Zákon č. 111/2009 Sb.	Zákon č. 111/2009 Sb., o základních registrech
Vyhláška č. 383/2009 Sb.	Vyhláška 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)
Zákon č. 100/2010 Sb.	Zákon č. 100/2010 Sb., kterým se mění zákon č. 111/2009 Sb., o základních registrech
Zákon č. 372/2011 Sb.	Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)

Zákon č. 255/2012 Sb.	Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)
Zákon č. 181/2014 Sb.	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
Zákon č. 221/2015 Sb.	Zákon č. 221/2015 Sb., kterým se mění zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a některé další zákony
Zákon č. 250/2016 Sb.	Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízeních o nich
Vyhláška č. 79/2017 Sb.	Vyhláška č. 79/2017 Sb., o stanovení struktury a formátu oznámení podle zákona o střetu zájmů
Vyhláška č. 82/2018 Sb.	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
Zákon č. 110/2019 Sb.	Zákon č. 110/2019 Sb., o zpracování osobních údajů
Zákon č. 12/2020 Sb.	Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů
Zákon č. 433/2023 Sb.	Zákon č. 433/2023 Sb., zákon o státním rozpočtu České republiky na rok 2024

SEZNAM POUŽITÝCH ZKRATEK

AI akt / nařízení o umělé inteligenci	Artificial Intelligence Act - nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)
AIFO	Agendový identifikátor fyzické osoby
BCR	Binding Corporate Rules (Závazná vnitropodniková pravidla)
BSI	Bezvýznamový směrový identifikátor
CEF	Coordinated Enforcement Framework (Společná dozorová akce EDPB)
CIS	Celní informační systém
DA / nařízení o datech	Data Act - nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828 (nařízení o datech) a související národní legislativou
DGA / nařízení o správě dat	Data Governance Act - nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat) a související národní legislativou
DMA / nařízení o digitálních trzích	Digital Markets Act - nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích)
DSA / nařízení o digitálních službách	Digital Services Act - nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách)
DPIA	Data Protection Impact Assessment (Posouzení vlivu na ochranu osobních údajů)
EDPB / Sbor	European Data Protection Board (Evropský sbor pro ochranu osobních údajů)
EDPS	European Data Protection Supervisor (Úřad evropského inspektora pro ochranu osobních údajů)
ePD / ePrivacy směrnice / směrnice 2002/58/ES	ePrivacy Directive - směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)
EURODAC	European Asylum Dactyloscopy Database (Evropská databáze pro srovnání otisků prstů žadatelů o azyl a některých kategorií ilegálních přistěhovalců)

GDPR / obecné nařízení / nařízení (EU) 2016/679	General Data Protection Regulation - nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti osobních údajů a o volném pohybu těchto údajů, a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
GPA	Global Privacy Assembly (Světové shromáždění pro ochranu osobních údajů)
IS ORG	Informační systém ORG (Informační systém pro převod identifikátorů)
ISZR	Informační systém základních registrů
KIFO	Klientský identifikátor fyzické osoby
NSS	Nejvyšší správní soud
procesní nařízení	Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví další procesní pravidla týkající se prosazování nařízení (EU) 2016/679
ROB	Registr obyvatel České republiky
SDEU	Soudní dvůr Evropské unie
SIS	Schengenský informační systém
PAR / nařízení o politické reklamě	Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy
LED / trestněprávní směrnice / směrnice (EU) 2018/680	Law Enforcement Directive – 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
ÚOOÚ / Úřad	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud
VIS	Vízový informační systém
ZIFO	Zdrojový identifikátor fyzické osoby
ZR	Základní registry

Úřad pro ochranu
osobních údajů

Výroční zpráva
Úřadu pro ochranu osobních údajů
za rok 2024
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: Mgr. Alena Wagner Ježková, Ph.D.
Redakce: Mgr. Bc. David Burian
Grafická úprava a sazba: MgA. Mira Antonović
Jazyková korektura: Mgr. Aleš Pořízka,
Mgr. Věra Adina Šefraná, Ph.D.
Autor fotografií na s. 27, 28, 44 a 45: Milan Řepka
Tisk: AMOS TYPO, s. r. o.