15. 7. 2026

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Výroční zpráva ÚOOÚ za rok 2025: nové regulatorní priority v oblasti ochrany osobních údajů

Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) zveřejnil výroční zprávu za rok 2025, která vedle tradičního přehledu dozorové a rozhodovací činnosti nabízí i poměrně jasný obraz o tom, jakým směrem se oblast ochrany osobních údajů regulatorně posouvá. Zpráva reflektuje nejen pokračující digitalizaci veřejného i soukromého sektoru, ale také nástup umělé inteligence, rozvoj nových digitálních služeb a postupné rozšiřování evropské regulatorní agendy, která se ochrany osobních údajů bezprostředně dotýká. Současně potvrzuje, že ochranu osobních údajů již nelze vnímat čistě jako otázku souladu s obecným nařízením o ochraně osobních údajů (dále jen „GDPR“), ale stále více jako součást širšího regulatorního rámce digitální ekonomiky, pravidel nakládání s daty a odpovědného využívání nových technologií.

Rok 2025 byl pro ÚOOÚ významný i symbolicky – dne 1. června uplynulo 25 let od zahájení jeho činnosti. Výroční zpráva tak přináší nejen ohlédnutí za dosavadním vývojem ÚOOÚ a jeho činností v uplynulém roce, ale také konkrétní signál směrem ke správcům a zpracovatelům osobních údajů, jaké oblasti budou pod zvýšeným regulatorním dohledem a na jaké principy ochrany osobních údajů ÚOOÚ ve své činnosti klade důraz.

Kontrolní plán ÚOOÚ pro rok 2025 jako mapa regulatorních priorit

Výroční zpráva navazuje na kontrolní plán ÚOOÚ pro rok 2025, který se zaměřil na čtyři hlavní oblasti: i) zpracování osobních údajů ve věrnostních programech, ii) provozování kamerových systémů, iii) využívání dat z registrů a informačních systémů veřejné správy a iv) zpracování osobních údajů v Schengenském informačním systému. Vedle toho se ÚOOÚ zapojil do celoevropské koordinované dozorové akce Coordinated Enforcement Framework 2025 (dále jen „**CEF 2025**“), tentokrát zaměřené na uplatňování práva subjektu údajů na výmaz osobních údajů, tedy tzv. práva být zapomenut.

Při pohledu na konkrétní kontrolní zjištění je zřejmé, že společným jmenovatelem dozorové činnosti byl důraz na základní principy GDPR – zejména zásadu minimalizace údajů, správnou volbu právního titulu zpracování, transparentnost vůči subjektům údajů a nezbytnost a proporcionalitu zvolených technických a organizačních řešení.

Právě proporcionalita se ve výroční zprávě objevuje jako opakující se motiv – zejména tam, kde správci zavádějí technologicky sofistikovaná řešení, aniž by dostatečně doložili, proč je nelze nahradit méně invazivním prostředkem. Typickým příkladem jsou podle ÚOOÚ biometrické docházkové systémy, u nichž upozorňuje, že sledovaného účelu evidence docházky lze zpravidla dosáhnout i standardními nástroji, jako jsou přístupové karty či jiné evidenční systémy, bez nutnosti zpracovávat biometrické údaje, které při využití k jedinečné identifikaci fyzické osoby podléhají přísnějšímu režimu ochrany.

Biometrické údaje pod zvýšeným dohledem

Jedním z nejvýraznějších témat výroční zprávy je využívání biometrických technologií, a to jak ve veřejném, tak v soukromém sektoru. Biometrické údaje, tedy například otisky prstů, snímky obličeje nebo jiné jedinečné fyzické znaky nebo charakteristiky chování, které umožňují identifikaci konkrétní osoby, představují z pohledu ochrany osobních údajů zvlášť citlivou kategorii údajů, jejichž zpracování podléhá přísnějším podmínkám.

Pozornost vzbudila zejména kontrola systému automatického biometrického rozpoznávání obličejů provozovaného Policií České republiky na Letišti Václava Havla v Praze. Policie v rámci provozu kamerového systému využívala technologii automatického rozpoznávání obličejů („*facial recognition*“), kdy byly biometrické údaje osob zaznamenaných kamerovým systémem porovnávány s referenční databází tzv. „zájmových osob“. ÚOOÚ dospěl k závěru, že zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby nebylo založeno na výslovném zákonném oprávnění. V návaznosti na legislativní změny byl systém k 1. srpnu 2025 deaktivován a biometrické údaje byly smazány.

Stejně důležitá byla i kontrola zpracování záznamů z osobních kamer nošených příslušníky Policie ČR. ÚOOÚ v této souvislosti konstatoval nedostatky v oblasti logování přístupů k pořízeným záznamům, tedy v evidenci toho, kdo, kdy a z jakého důvodu k nahrávkám přistupoval. V praxi mohlo docházet ke zpřístupnění nahrávek bez odpovídající auditní stopy, což Úřad vyhodnotil jako pochybení v oblasti zabezpečení osobních údajů.

Obdobně přísný přístup ÚOOÚ zaujal i vůči zaměstnavatelům využívajícím biometrické docházkové systémy. V několika případech Úřad konstatoval, že zaměstnavatelé nedoložili odpovídající právní základ zpracování biometrických údajů nebo porušili zásadu minimalizace, protože stejného účelu evidence docházky bylo možné dosáhnout méně invazivními prostředky, například přístupovými kartami nebo jinými evidenčními systémy. ÚOOÚ v této souvislosti výslovně doporučuje před zavedením obdobných systémů důsledně posoudit nezbytnost a proporcionalitu takového řešení a upřednostnit méně invazivní alternativy.

Minimalizace údajů jako trvalá priorita

Vedle biometrie zpráva potvrzuje pokračující silný důraz ÚOOÚ na zásadu minimalizace osobních údajů podle čl. 5 odst. 1 písm. c) GDPR.

Významným příkladem je kontrola provozování věrnostního programu obchodního řetězce, v jehož registračním formuláři byl povinně vyžadován údaj o pohlaví, přičemž zákazník neměl možnost tento údaj neuvést. ÚOOÚ dospěl k závěru, že k plnění smluvního vztahu vyplývajícího z účasti ve věrnostním programu není takový údaj nezbytný. Vedle toho ÚOOÚ analyzoval i samotný právní titul zpracování a upozornil, že určení správného právního základu nelze mechanicky spojovat s formálním označením zpracování jako „souhlas“, ale vždy musí odpovídat skutečné povaze vztahu mezi správcem a subjektem údajů.

Obdobný regulatorní přístup je patrný i v oblasti realitních služeb. ÚOOÚ zde kritizoval nadbytečné shromažďování údajů, včetně údajů o rodinném stavu, místě narození, kopií občanských průkazů nebo údajů shromažďovaných pro účely, které ve výsledku vůbec nenastaly (například příprava nájemní smlouvy, která nebyla uzavřena). Úřad v této souvislosti výslovně upozornil, že příliš obecné a plošně nastavené procesy zpracování osobních údajů bez zohlednění konkrétního případu mohou vést k porušení zásady minimalizace.

Pro správce osobních údajů jde o důležité připomenutí, že regulatorní otázka nestojí pouze na tom, zda určitý údaj může být potenciálně užitečný, ale především na tom, zda je jeho zpracování pro konkrétní účel skutečně nezbytné.

Právo na výmaz a transparentnost procesů

V rámci koordinované evropské akce CEF 2025 se ÚOOÚ zabýval postupy správců při vyřizování žádostí o výmaz osobních údajů podle čl. 17 GDPR. Šetření odhalilo potenciální nedostatky zejména v oblasti transparentnosti procesů – například v situacích, kdy správci subjekty údajů dostatečně neinformovali o možnosti podat stížnost u dozorového úřadu nebo žádat soudní ochranu v případě nevyhovění žádosti o výmaz. Nedostatky byly zjištěny rovněž v omezených možnostech, jak mohou subjekty údajů své právo uplatnit, nebo v nedostatečné dohledatelnosti informací o postupu při vyřizování těchto žádostí.

ÚOOÚ současně upozornil na technickou složitost samotného procesu výmazu, zejména ve starších informačních systémech, rozsáhlých cloudových řešeních nebo ve vztahu k zálohám dat, kde je třeba vyvažovat právo na výmaz s požadavkem integrity a kontinuity dat.

Ochrana osobních údajů jako součást širší digitální regulace

Výroční zpráva rovněž potvrzuje, že agenda ÚOOÚ již zdaleka nekončí u klasického dozoru podle GDPR. Úřad se v roce 2025 intenzivně věnoval také novým evropským digitálním regulacím, zejména nařízení o digitálních službách (DSA), nařízení o digitálních trzích (DMA), nařízení o umělé inteligenci (AI Act), nařízení o správě dat či nařízení o datech. Tyto právní předpisy postupně vytvářejí nový regulatorní rámec pro fungování digitální ekonomiky, který se dotýká nejen ochrany osobních údajů, ale také transparentnosti online platforem, odpovědného využívání umělé inteligence, správy a sdílení dat nebo pravidel hospodářské soutěže v digitálním prostředí. Působnost ÚOOÚ se tak postupně rozšiřuje – vedle tradiční dozorové činnosti v oblasti ochrany osobních údajů se ÚOOÚ stále výrazněji zapojuje i do širší digitální regulatorní agendy, která se dotýká ochrany práv jednotlivců v online prostředí.

Pro správce a zpracovatele osobních údajů to v praxi znamená potřebu vnímat ochranu osobních údajů v širších souvislostech než dosud. Vedle plnění povinností podle GDPR bude stále důležitější také správné nastavení interních procesů při nakládání s daty, transparentnost automatizovaného rozhodování a odpovědné zavádění nových technologických řešení, zejména systémů využívajících umělou inteligenci.

Rostoucí počet podání a vyšší očekávání od správců

Jedním z nejvýraznějších údajů výroční zprávy je meziroční nárůst počtu podání a stížností o více než 68 %, který podle ÚOOÚ představuje nejvyšší úroveň od účinnosti GDPR. Úřad současně výslovně uvádí, že tento trend významně zatěžuje jeho rozhodovací kapacity a zvyšuje nároky na efektivitu, rychlost a kvalitu jeho činnosti.

Za tímto vývojem lze spatřovat několik souběžných faktorů. Zpracování osobních údajů se stalo neoddělitelnou součástí každodenního fungování podniků, institucí i digitálních platforem. S rostoucím rozsahem automatizovaného zpracování dat, širším využíváním cloudových řešení, profilováním zákazníků, personalizací služeb a nástupem AI systémů současně roste i počet situací, v nichž mohou být práva subjektů údajů dotčena. Vedle toho je patrný i dlouhodobý růst povědomí jednotlivců o jejich právech podle GDPR, což se přirozeně promítá do vyšší ochoty obracet se na dozorový orgán.

Z pohledu správců osobních údajů je podstatné, že ÚOOÚ nadále zdůrazňuje odpovědnost správce nejen za zákonnost zpracování, ale také za schopnost soulad s právní úpravou doložit. Právě absence dostatečné dokumentace, nedostatečné odůvodnění zvoleného právního titulu nebo nepřiměřeně široce nastavené procesy se opakovaně objevují jako problematická místa.

Závěr

Výroční zpráva ÚOOÚ za rok 2025 potvrzuje několik zřetelných regulatorních trendů: silnější dohled nad využíváním biometrických technologií, pokračující důraz na zásadu minimalizace údajů, detailnější přezkum právních titulů zpracování a rostoucí význam transparentnosti a odpovědnosti správců. Současně ukazuje, že ochrana osobních údajů se stále více propojuje s širší digitální regulatorní agendou, jejíž význam bude v následujících letech dále narůstat.

Pro správce a zpracovatele osobních údajů je proto vhodný čas prověřit nejen formální dokumentaci v oblasti ochrany osobních údajů a nastavení procesů podle GDPR, ale také samotnou podstatu zpracovatelských operací – jejich nezbytnost, proporcionalitu, právní oporu a připravenost obstát při případné regulatorní kontrole.

Mgr. Jakub Málek,
managing partner

Mgr. Kateřina Vyšínová,
advokátní koncipientka

Anna Němcová,
právní asistentka

PEYTON legal

PEYTON legal advokátní kancelář s.r.o.

Futurama Business Park
Sokolovská 668/136d
186 00 Praha 8 – Karlín

Tel.: +420 227 629 700
E-mail: info@plegal.cz

Další články:

- Výroční zpráva ÚOOÚ za rok 2025: nové regulatorní priority v oblasti ochrany osobních údajů
- Vadné nařízení vlády č. 493/2025 Sb. a dopady fixace limitů drobných oprav na pronajímatele
- Nařízení PPWR: cesta do pekla dlážděná dobrými úmysly
- AML - od zákona č. 253/2008 Sb. k AMLR: co konkrétně musí česká povinná osoba změnit do roku 2027
- Podmíněné propuštění ve světle zásady ústnosti a přímosti
- Byznys a paragrafy, díl 37.: Povinná forma jednání ve smlouvách
- Poučení z krizového vývoje v kauze bitcoiny
- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi