DAGITAL LEGAL
Privacy & Technology Law Firm

SPRÁVA O OCHRANE OSOBNÝCH ÚDAJOV ZA ROK 2025

SLOVENSKÁ REPUBLIKA

Publikovaná 28. januára 2026

Vážení klienti a kolegovia,

Túto správu vydávame od roku 2020, pričom ide už o šiestu správu v poradí. Stále ide o jediný verejne dostupný zdroj a prehľad rozhodovacej činnosti oboch regulátorov na Slovensku, ku ktorému pridávame každý rok aj relevantné rozhodnutia súdov a prehľad legislatívnych udalostí.
Je smutné, že za 6 rokov túto dobrovoľnú aktivitu nijako nepodporil a nijako na ňu nezareagoval ani jeden z našich regulátorov. Touto správou sa nepriamo pýtame, prečo naše úrady sami nezverejňujú svoje rozhodnutia? Medzi ich hlavné úlohy podľa čl. 57 GDPR patrí zvyšovanie povedomia o ochrane osobných údajov a súkromia. Nevieme si predstaviť lepší spôsob plnenia tejto úlohy. Potrebujeme poznať rozhodovaciu činnosť našich regulátorov a potrebujeme ju prepájať s praxou a súdnymi rozhodnutiami.

Táto správa je určená na voľné a bezplatné šírenie na akékoľvek interné účely vrátane reportingu, školení, interných analýz. zvyšovania povedomia o ochrane osobných údajov, alebo aj na právne účely. Prosíme len o referenciu a uvedenie zdroja.
Rok 2025 priniesol viacero zásadných tém, ktoré sa dotýkajú ochrany súkromia a spracúvania osobných údajov — a to nielen cez GDPR, ale aj cez prepojené európske regulácie (najmä AI Act, DSA a Data Act), nové kybernetické predpisy a viaceré legislatívne návrhy na úrovni Slovenskej republiky.

Veríme, že Vám táto správa pomôže zorientovať sa v trendoch, rozhodovacej praxi a legislatívnom vývoji, a zároveň poskytne praktické ponaučenia pre nastavenie procesov v roku 2026.

Jakub Berthoty, za celý tím Dagital Legal

NAVIGÁCIA

Pre citácie:

Dagital Legal, s.r.o. *Správa o ochrane osobných údajov za rok 2025: Slovenská republika*. Bratislava, 2026, 25 s.

+421 911 195 133 jakub.berthoty@dagital.eu www.dagital.eu Nové Záhrady I/9, 821 05 Bratislava

Rovnako aj Úrad na ochranu osobných údajov SR (ďalej len „Úrad") naďalej vydáva vlastné výročné správy, pričom poslednú správu za rok 2024 zverejnil Úrad v septembri 2025. Výročné správy Úradu obsahujú časť „vybrané prípady z dozornej činnosti", v ktorej Úrad popisuje vybrané rozhodnutia. Druhý regulátor, Úrad pre reguláciu elektronických komunikácií a poštových služieb (ďalej len „Úrad pre reguláciu") takisto vydáva výročné správy. Jeho správy sú však orientované na telekomunikačný sektor a nevyplývajú z jeho žiadne informácie o rozhodnutiach v zmysle ePrivacy smernice (cookies a priamy marketing).

Naša správa tradične ponúka širší a prakticky orientovaný pohľad na vývoj ochrany osobných údajov na Slovensku, vrátane zásadných legislatívnych trendov, rozhodovacej praxe a príkladov, ktoré môžu byť relevantné pre súkromný, ako aj verejný sektor. Zaujímajú nás konkrétne rozhodnutia, výška pokuty, trendy a témy, ktorým sa úrady venujú. Správa je rozdelená do nasledujúcich 4 kategórií:

1. legislatívne udalosti;
2. rozhodnutia a činnosť úradov;
3. judikatúra; a
4. ďalšie udalosti.

Naším cieľom bolo zaznamenať čo najviac relevantných udalostí, ale nie je v našich silách zachytiť všetky. Ak by Vám v tejto správe chýbala zaujímavá udalosť, dajte nám, prosím, vedieť. Radi ju doplníme.

LEGISLATÍVNE UDALOSTI

Rok 2025 priniesol tému ochrany osobných údajov do legislatívnych diskusií častejšie, ako býva na Slovensku zvykom. Dôvodom tejto zmeny bol najmä **návrh nového zákona o ochrane osobných údajov**, ktorý je aktuálne vo fáze vyhodnocovania pripomienkového konania a bude nepochybne patriť medzi hlavné témy aj v novom roku a **ďalšia novela zákona o elektronických komunikáciách**. Obom sa venujeme bližšie ďalej v texte.

Vo fáze hodnotenia pripomienkového konania sa nachádza aj „dvojička" návrhu zákona o ochrane osobných údajov, a to návrh zákona o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov. Neobsahuje žiadne podstatné zmeny oproti existujúcej tretej časti zákona, a to napriek prinajmenšom problematickej implementácii a prepojeniu práv dotknutých osôb vo vzťahu k vyšetrovacím spisom, ktoré sa v plnej miere riadia trestným poriadkom.

Pripomienky sa aktuálne vyhodnocujú aj vo vzťahu k návrhu zákona o organizácii štátnej správy v oblasti AI, podľa ktorého má byť Ministerstvo investícií, regionálneho rozvoja a informatizácie SR všeobecným orgánom dohľadu nad trhom.

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR predložilo aj návrh zákona, ktorým sa upravujú požiadavky európskej regulácie údajov. Cieľom návrhu je implementovať nové pravidlá EÚ upravujúce spravodlivý prístup k údajom a ich používanie podľa nariadenia o údajoch (Data Act). Aktuálne prebieha vyhodnocovanie pripomienkového konania.

Opomenúť nie je možné ani **reformu občianskeho práva**, ktorého súčasťou je aj ochrana jednotlivých prvkov osobnosti či úprava vecí s digitálnymi prvkami a poskytovania digitálneho plnenia. Návrh komplexne modernizuje zmluvné právo, a to vrátane modernejšej úpravy zodpovednosti a digitálnych a automatizovaných služieb či upresňuje zásahy do ochrany osobnosti a zakotvuje ochranu pred deepfake, manipuláciou obrazu a online útokmi. Návrh Občianskeho zákonníka sa nachádza vo fáze vyhodnotenia pripomienkového konania.

So súkromnoprávnymi predpismi súvisí aj schválenie nového zákona o spotrebiteľských úveroch, ktorý o. i. zavádza moderné posudzovanie bonity, právo onkologických pacientov na zabudnutie, úpravu marketingových pravidiel, postup posudzovania schopnosti spotrebiteľa splácať úver či využívanie automatizovaných rozhodovacích nástrojov. Zákon nadobúda účinnosť v dvoch fázach, a to 1. decembra 2025 a 20. novembra 2026. .

Značný rozruch spôsobilo schválenie zákona o poskytovaní údajov na účel adresnej energopomoci, ktorý v októbri nahradil zákon o adresnej energopomoci doplňaný nariadeniami vlády. Zákon s ohľadom na právo MH SR získavať prakticky všetky dostupné informácie o osobách, ktoré tvoria spoločnú domácnosť, vyvolal otázky vo vzťahu k súladu s GDPR a právnom na ochranu súkromia.

Dňa 15. októbra nadobudla účinnosť novela zákona o archívoch a registratúrach, ktorá o. i. definuje transformáciu registratúrneho záznamu, ustanovuje ako vlastníka nájdeného dokumentu štát či určuje podmienky vyraďovacieho konania.

Zároveň prebieha intenzívna práca na **predpisoch zabezpečujúcich kybernetickú ochranu** v rôznych oblastiach. Vo fáze rokovania NRSR je aktuálne novela zákona o informačných technológiách vo verejnej správe. Dňa 1. januára 2026 už vstúpil do účinnosti zákon č. 318/2025, ktorý čiastočne implementuje nariadenie č. 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (nariadenie CRA). Bezpečnostné opatrenia pre siete, informačné systémy a operačné technológie upravila nová vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach. NBÚ ďalej publikoval aj vyhlášky v oblasti priemyselnej bezpečnosti a o bezpečnostnom projekte podnikateľa či k hláseniam podľa zákona o kybernetickej bezpečnosti.

Slovenské legislatívne prostredie však výrazne formovali aj **únijné predpisy.**

Najväčšou témou posledných týždňov je nepochybne tzv. digitálny omnibus, ktorý obsahuje súbor zmien s cieľom zjednodušiť pravidlá v oblasti „digitálnej legislatívy". Komisia navrhla aj samostatné zjednodušujúce opatrenia, ktoré majú zabezpečiť včasné vykonávanie povinností podľa nariadenia o AI, tzv. AI digitálny omnibus. Návrh zahŕňa aj úpravu cookies nadväzujúcu na stiahnutý návrh ePrivacy nariadenia. Mnohí vnímajú návrh ako ohrozenie zlatého štandardu ochrany osobných údajov v EÚ (napr. zúženie definície osobných údajov či sťaženie uplatňovania práv dotknutých osôb). S ohľadom na množstvo kritiky, ktoré vyplynulo z odbornej diskusie môže prejsť návrh ešte značnými zmenami. V aktuálnej podobe sa však javí, že pôjde o jednu z najvýznamnejších legislatívnych zmien v oblasti ochrany osobných údajov od schválenia GDPR.

GDPR, konkrétne jej cezhraničné presadzovanie a vybavovanie žiadostí, by mali urýchliť aj nové nariadenie, ktorým sa stanovujú ďalšie procesné pravidlá týkajúce sa presadzovania GDPR, ktoré prijala v novembri Rada EÚ. Nariadenie nadobudlo platnosť 1. januára 2026 a začína sa uplatňovať 2. apríla 2027.

Dňa 12. septembra 2025 nadobudlo účinnosť nariadenie o údajoch (Data Act), ktorého cieľom je posilniť kontrolu používateľov nad ich údajmi v kontexte internetu vecí („IoT") a pripojených produktov a služieb. Toto nariadenie v čl. 37 ods. 2 priamo zveruje časť kompetencií dozorným orgánom podľa GDPR, ktorým je predovšetkým Úrad ale aj Úrad pre reguláciu. Túto skutočnosť potvrdzuje aj návrh zákona v MPK.

Okrem toho v januári nadobudlo účinnosť nariadenie o digitálnej prevádzkovej odolnosti (DORA) relevantné najmä vo vzťahu k IT infraštruktúre finančných subjektov.

Od 29. októbra 2025 je účinný delegovaný akt Komisie o prístupe k údajom podľa nariadenia o digitálnych službách (DSA). Nové pravidlá umožnia výskumníkom prístup k údajom veľmi veľkých online platforiem, aby mohli študovať z nich vyplývajúci spoločenský vplyv.

Dňa 10. októbra 2025 vstúpilo do účinnosti nariadenie o transparentnosti a cielení politickej reklamy, ktoré dopĺňa GDPR v oblasti regulácie využívania digitálnych nástrojov v politickej sfére v snahe zabrániť netransparentnému ovplyvňovaniu voličov počas volebných kampaní prostredníctvom cielenej online politickej reklamy zahŕňajúcej spracovanie osobných údajov.

Vo februári vstúpila do účinnosti **prvá časť nariadenia o AI** upravujúca základné povinnosti ako zákazy určitých postupov či povinnosti týkajúce sa gramotnosti zamestnancov, na ktorú nadviazala v auguste ďalšia časť aj o modeloch na všeobecné účely. Zostávajúca časť nariadenia má vstúpiť do účinnosti dňa 2. augusta 2026 (s výnimkou článku 6 (1) o pravidlách klasifikácie vysokorizikových systémov).

V novom roku môžeme očakávať aj ďalšie **avizované predpisy,** medzi ktoré patrí:

1. návrh smernice o AI a algoritmickom riadení na pracovisku, ktorého cieľom je vyplniť regulačné medzery a zabezpečiť transparentnosť pri používaní systémov algoritmického riadenia zo strany zamestnávateľov a zavedenie konkrétnych mechanizmov, napr. zákazu spracúvania údajov týkajúcich sa emocionálneho stavu, súkromných rozhovorov a voľného času zamestnancov,
2. iniciatíva na obnovenie pravidiel o uchovávaní údajov na účely vymáhania práva, ktorá nadväzuje na myšlienku zrušenej smernici o uchovávaní údajov s cieľom o. i. umožniť prístup OČTK k telekomunikačným dátam,
3. návrh európskych podnikateľských peňaženiek na zjednodušenie výmeny údajov, ktorý by mohol vyriešiť viaceré problémy prevádzkovateľov s identifikáciou dotknutých osôb v rámci EÚ, keďže verifikácia bude rovnocenná s osobne vykonanými právnymi úkonmi.

Návrh zákona o ochrane osobných údajov

Úrad na ochranu osobných údajov SR publikoval v súlade s marcovým zoznamom pripravovaných právnych predpisov návrh nového zákona na ochranu osobných údajov, ktorého cieľom má byť predovšetkým odstránenie aktuálnej dvojkoľajnosti právnej úpravy. Pôvodne mal byť účinný už od 1. januára 2026, aktuálne sa však návrh od 2. júla 2025 nachádza vo fáze pripomienkového konania bez určeného termínu skončenia. Hovorí sa o účinnosti od 1. júla 2026, no je otázne, ako je táto legislatívna zmena načasovaná napríklad s digitálnym omnibusom na úrovni EÚ.

Hlavným pozitívom návrhu je odstránenie nepotrebnej a zmätočnej druhej časti existujúceho zákona. Tým sa zákon má výrazne zjednodušiť a skrátiť a súčasne sa tým odstráni stále existujúca a nesprávna prax odkazovania na paragrafové znenie druhej časti zákona namiesto článkov GDPR.

Zároveň sa však objavili aj nové ustanovenia, pri ktorých je na mieste uvažovať o neprimeranej rigidnosti. Uvedené obavy sa týkajú predovšetkým zásahu do právneho základu podľa článku 6 ods. 1 písm. c) a ods. 3 GDPR, podľa ktorého je spracúvanie zákonné, ak je spracovateľská operácia nevyhnutná na splnenie zákonnej povinnosti prevádzkovateľa. Návrh zákona však na rozdiel od GDPR nepovažuje za možné, ale nevyhnutné, aby osobitné zákony obsahovali vlastné ustanovenia o spracúvaní osobných údajov. Takúto podmienku však väčšina slovenských zákonov nespĺňa (napr. Zákonník práce, zdravotnícke predpisy, školské zákony, sociálna oblasť). Zbytočným dôsledkom by teda bolo, že hoci by prevádzkovateľ mal zákonnú povinnosť spracúvať osobné údaje napr. na plnenie povinností zamestnávateľa, musel by aplikovať iný právny základ ako plnenie zmluvy. Dotknuté osoby teda nezískajú vyššiu ochranu, vznikne však právna neistota a množstvo časových aj finančných nákladov potrebných na splnenie tejto administratívnej a formálnej zmeny. Túto námietku opakovali v rámci pripomienkovacieho konania viaceré subjekty a nie je jasné, ako sa s ňou Úrad vysporiada.

Tretiu kategóriu zmien tvoria bližšie nevysvetlené úpravy, ako napr. predĺženie funkčného obdobia predsedníčky z 5 až na 7 rokov s možnosťou opakovanej voľby bez obmedzenia 2 funkčnými obdobiami. Všetky dôležité návrhy úprav sme pre Vás zhrnuli v analytickom blogu tu.

Ďalšia novela zákona o elektronických komunikáciách („ZEK")

Dňa 12. novembra nadobudla účinnosť väčšina ustanovení zákona novelizujúceho ZEK. Primárnym cieľom novely mali byť úpravy súvisiace s nariadením EÚ č. 2024/1309 o gigabajtovej infraštruktúre, opäť však došlo aj k viacerým úpravám týkajúcich sa priameho marketingu, a to predovšetkým:

1. rozšírenie definície priameho marketingu aj na marketingové formy zisťovania a prieskumov ako analytické prieskumy či zisťovanie informácií o preferenciách (§ 116 (2)),
2. odstránenie možnosti „navolávania súhlasov" a inštitútu „odvolania námietky" (§ 116 (4)),
3. zavedenie doby 1 roka od ukončenia zmluvného vzťahu s klientom, počas ktorej má byť možné použiť výnimku „vlastných podobných tovarov a služieb" (§ 116 (16)), ktorá vyvoláva pochybnosti vo vzťahu k súladu s ePrivacy smernicou.

Väčšina úprav je pozitívna, je však zmeškanou príležitosťou, že z pôvodného návrhu vypadlo odstránenie výnimky používania predčíslia +888 pri kontaktovaní fyzických osôb podnikateľov a právnických osôb na zverejnené kontaktné údaje (navrhovaný § 116 (12)).

Na rozporuplnosť tejto výnimky sme upozornili už v roku 2021 v analytickom blogu tu. Bližšie vysvetlenie zmien ešte z fázy pripomienkového konania nájdete tu.

Ustanovenie § 116 ZEK podľa nás stále obsahuje časti, ktoré sú v rozpore s GDPR a ustálenou praxou dozorných orgánov podľa GDPR. Dokonca aj so staršími rozhodnutiami Úradu na ochranu osobných údajov. Najmä možnosť marketingovo oslovovať fyzické osoby podnikateľov na zverejnené čísla (navyše bez prečíslia +888) alebo kontaktovanie existujúcich zákazníkov aj po ukončení zmluvy s nimi, čo ePrivacy smernica nepredpokladá. Novela tak odstránila časť problematických ustanovení, ale nie všetky a ďalšie problematické zaviedla.

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Plán kontrol na rok 2025

Začiatkom roka zverejnil Úrad svoj plán kontrol. Plán kontrol Úradu na rok 2025 reflektuje kombináciu dvoch hlavných okruhov:

1. tematických kontrol vo verejnej správe v súvislosti so schengenskými a európskymi informačnými systémami a agentúrami a
2. kontrol vybraných spracovateľských činností v súkromnom sektore, pri ktorých možno predpokladať zvýšené riziko zásahu do práv dotknutých osôb.

V prvej časti sa Úrad zameriava najmä na bezpečné a zákonné spracúvanie osobných údajov v systémoch využívaných v rámci schengenského acquis a európskej spolupráce (napr. N.SIS, N.VIS, Eurodac (automatizovaný európsky systém identifikácie odtlačkov prstov), Europol a colné informačné systémy). V rámci tejto časti bolo plánovaných 8 kontrol, pričom kontrolované subjekty zahŕňajú Ministerstvo zahraničných vecí a európskych záležitostí SR, Ministerstvo vnútra SR, Dopravný úrad, Finančné riaditeľstvo SR a ďalšie relevantné orgány.

Druhá časť plánu kontrol mala za cieľ sa zamerať na vybrané spracovateľské činnosti v režime GDPR, ktoré majú potenciál významne zasiahnuť do práv dotknutých osôb, a to najmä z hľadiska zákonnosti spracúvania, plnenia informačných povinností a bezpečnostných opatrení. Konkrétne boli v pláne kontrol spracúvania osobných údajov dotknutých osôb v postavení

- zákazníkov verejných lekární;
- účastníkov kurzov organizovaných autoškolami;
- osôb vstupujúcich do reštaurácií, kaviarní a iných zariadení monitorovaných kamerovým systémom.

V tejto časti úrad naplánoval 6 kontrol, konkrétne v oblasti spracúvania osobných údajov zákazníkov verejných lekární, účastníkov kurzov v autoškolách a osôb vstupujúcich do prevádzok monitorovaných kamerovým systémom.

Právoplatné rozhodnutia Úradu

Ani v roku 2025 Úrad nezverejňoval svoju rozhodovaciu prax spôsobom, ktorý by umožňoval verejnosti systematický a ucelený prístup ku všetkým vydaným rozhodnutiam. Kým niektoré prípady sa objavia v médiách alebo vo verejnej diskusii, značná časť rozhodnutí zostáva mimo širšej dostupnosti.

Aj preto sme v priebehu roka využili postupy podľa zákona o slobodnom prístupe k informáciám a získali sme rozhodnutia, z ktorých nižšie uvádzame výber a stručné zhrnutie. V prípadoch, kde sa rozhodnutia týkajú súkromných spoločností, ich obchodné mená neuvádzame.

V porovnaní s predchádzajúcimi ročníkmi sme tento rok pristúpili k prehľadnejšiemu tematickému členeniu rozhodnutí podľa typu prevádzkovateľa, keďže sa ukázalo, že mnohé otázky ochrany osobných údajov sa v praxi opakujú najmä v rámci konkrétnych sektorov. Zároveň platí, že rovnaký právny problém môže mať odlišný kontext v závislosti od toho, či ide o obec, školu, štátny orgán alebo súkromnú spoločnosť.

Z tohto dôvodu sme rozhodnutia za rok 2025 rozdelili do štyroch kategórií:

1. Obce, mestá a kraje
2. Štátne orgány, inštitúcie a ministerstvá
3. Školy a vzdelávacie zariadenia
4. Súkromné (obchodné) spoločnosti

Takéto rozdelenie považujeme za praktické najmä preto, že umožňuje čitateľom rýchlejšie identifikovať rozhodnutia relevantné pre ich vlastné prostredie a zároveň lepšie vnímať, ktoré typové pochybenia alebo interpretačné otázky sa v jednotlivých sektoroch opakujú.

Zároveň platí, že vzhľadom na celkový počet 511 pokút je objektívne nereálne spracovať všetky rozhodnutia do tejto správy. Preto v každej kategórii uvádzame najmä tie prípady, ktoré sú z pohľadu praxe najvýznamnejšie, či už z dôvodu výšky uloženej pokuty, alebo preto, že prinášajú zaujímavý právny alebo skutkový záver použiteľný aj pre iných prevádzkovateľov.

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
	OBCE, MESTÁ a KRAJE	
1. Hlavné mesto SR Bratislava	Hlavné mesto SR Bratislava zverejnilo na svojom webovom sídle viacero zmlúv (vrátane dodatkov a splnomocnení) tak, že obsahovali osobné údaje dotknutých osôb, ktoré mali byť anonymizované, no zverejnené boli v čitateľnej podobe. Išlo najmä o údaje ako dátum narodenia, rodné číslo, číslo občianskeho preukazu, štátne občianstvo a ďalšie údaje uvedené v dokumentoch. Úrad konštatoval porušenie čl. 6 ods. 1 GDPR, keďže pri zverejnení týchto údajov chýbal právny základ (zverejnenie rodného čísla a ďalších identifikátorov ide nad rámec zákonnej povinnosti zverejňovania). Úrad uložil mestu pokutu 3 000 eur a zároveň nariadil prijať nápravné opatrenia, aby sa podobné údaje v zverejňovaných dokumentoch už nevyskytovali. **Poučenie: Povinné zverejňovanie zmlúv neznamená automatické oprávnenie zverejniť aj „citlivé identifikátory" ako rodné číslo alebo číslo dokladu totožnosti. Aj pri zákonnej povinnosti musí prevádzkovateľ strážiť rozsah zverejnených údajov a nastaviť proces anonymizácie tak, aby chyba nebola len otázkou „pozornosti konkrétneho zamestnanca".**	**3 000 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
2. Hlavné mesto SR Bratislava	Hlavné mesto SR Bratislava zverejňovalo na oficiálnom profile sociálnej siete Facebook (profil „Mestská polícia Bratislava“) videozáznamy zo služobnej činnosti mestskej polície, na ktorých boli zachytené a zaznamenané osobné údaje dotknutých osôb (najmä podoby občanov prítomných pri výkone služby). Úrad dospel k záveru, že prevádzkovateľ na toto zverejňovanie nemal právny základ, čím porušil čl. 6 ods. 1 GDPR. Za porušenie uložil pokutu vo výške 2 500 EUR a zároveň nariadil bezodkladne odstrániť alebo anonymizovať zverejnené osobné údaje a prijať opatrenia, aby k zverejňovaniu bez právneho základu v budúcnosti nedochádzalo. **Poučenie: Orgány verejnej moci nemôžu stavať zverejňovanie videozáznamov zo zásahov mestskej polície na oprávnenom záujme ani na „domnelom“ súhlase. Pri publikovaní zásahov na sociálnych sieťach je potrebné veľmi striktne posúdiť právny základ a v praxi radšej vychádzať z toho, že zverejnenie je spravidla neprípustné bez jasného zákonného oprávnenia a reálnej anonymizácie.**	**2 500 eur**
3. Košice	Mesto Košice zverejnilo v CRZ viaceré zmluvy tak, že osobné údaje dotknutých osôb síce neboli „viditeľné“ na prvý pohľad, avšak po jednoduchej operácii (napr. skopírovaním textu zo zverejneného PDF do Wordu) sa stali voľne čitateľné. Išlo najmä o údaje ako dátum narodenia, štátne občianstvo, číslo občianskeho preukazu a rodné číslo. Úrad konštatoval porušenie čl. 32 ods. 1 GDPR, keďže prevádzkovateľ neprijal primerané technické opatrenia na zabezpečenie trvalej dôvernosti osobných údajov pri povinnom zverejňovaní dokumentov. Úrad uložil mestu nápravné opatrenia (zabezpečiť reálnu anonymizáciu a preškoliť osobu zodpovednú za zverejňovanie do CRZ). Mesto uviedlo, že išlo o ľudské pochybenie pri anonymizácii a že už v minulosti zaznamenalo podobný problém ako bezpečnostný incident. Tvrdilo, že opravené zmluvy CRZ nevymenilo z dôvodu technických a procesných limitov na strane registra (mesto nie je jeho prevádzkovateľom) a napriek snahe situáciu nevedelo úplne vyriešiť bez súčinnosti CRZ. Zároveň deklarovalo prijatie personálnych aj organizačných opatrení a priebežnú nápravu.	**1 500 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
4. Košický samosprávny kraj	Košický samosprávny kraj (KSK) zverejnil v Centrálnom registri zmlúv viacero dokumentov, pri ktorých sa po následnej úprave (napr. skopírovaním textu z PDF do Wordu) stali osobné údaje dotknutých osôb voľne čitateľné, a to najmä dátum narodenia a rodné číslo. Úrad konštatoval porušenie čl. 32 ods. 1 GDPR, keďže prevádzkovateľ neprijal primerané technické opatrenia na zabezpečenie trvalej dôvernosti osobných údajov pri povinnom zverejňovaní zmlúv. Úrad zároveň uložil KSK nápravné opatrenia (zabezpečiť, aby údaje v CRZ neboli čitateľné a preškoliť osoby zodpovedné za zverejňovanie). KSK uviedol, že išlo o pochybenie bývalých zamestnancov (zlyhanie ľudského faktora), pričom má zavedené interné pravidlá a prebieha pravidelné školenie, a zároveň deklaroval, že dotknuté údaje boli z dokumentov odstránené/vymazané. **Poučenie: Nestačí „anonymizovať" iba vizuálne – treba myslieť aj na to, aby osobné údaje neboli spätne získateľné jednoduchou operáciou (kopírovanie textu, konverzia PDF, OCR). Pri CRZ je potrebné nastaviť kontrolu formátu a funkčnú anonymizáciu, nie len manuálne prefarbenie/prekrytie.**	**1 500 eur**
5. Mesto Prešov	Mesto Prešov zverejnilo nájomné zmluvy v CRZ, v ktorých boli voľne čitateľné osobné údaje dotknutých osôb, konkrétne dátum narodenia a rodné číslo (t. j. neboli anonymizované). Konkrétne išlo o minimálne tri zmluvy o nájme bytu, ktoré boli zverejnené spôsobom umožňujúcim prístup k týmto údajom verejnosti. Úrad konštatoval porušenie čl. 6 ods. 1 GDPR a zároveň porušenie zákazu zverejňovania rodného čísla podľa § 78 ods. 4 zákona č. 18/2018 Z. z., keďže zverejnenie rodných čísel nemalo právny základ. Úrad uložil mestu opatrenia na nápravu (nastavenie procesu anonymizácie a školenie osoby zodpovednej za zverejňovanie). **Poučenie: Anonymizácia musí byť nastavená systémovo a kontrolovaná ešte pred zverejnením.**	**1 500 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
6. Takmer všetky rozhodnutia boli o porušení čl. 32 ods. 1 a čl. 6 ods. 1	Takmer všetky zistené porušenia povinností zo strany obcí a miest sa týkali zverejňovania údajov v Centrálnom registri zmlúv (CRZ). Najčastejšou príčinou porušení nebolo úmyselné konanie, ale zlyhanie pri technickom spracovaní dokumentov pred ich zverejnením, konkrétne pri ich konvertovaní do elektronickej podoby určenej na publikovanie v CRZ. V praxi opakovane dochádzalo k situáciám, keď zamestnanci samospráv považovali osobné údaje za anonymizované, avšak v dôsledku nesprávneho postupu pri konverzii (napr. prekrytie textu bez jeho odstránenia, nesprávna práca s PDF formátmi) došlo k ich následnému odanonymizovaniu a verejnému sprístupneniu.	**300 eur (152)** **500 eur (160)** **600 eur (1)** **700 eur (22)** **900 eur (1)** **1 000 eur (25)** **1 500 eur (6)** **2 500 eur (1)** **3 000 eur (1**
ŠTÁTNE ORGÁNY, INŠTITÚCIE A MINISTERSTVÁ		
1. Sociálna poisťovňa	Poisťovňa spracúvala osobné údaje pri doručovaní poštovej zásielky, pričom došlo k situácii, že zásielka obsahujúca osobné údaje nebola doručená spôsobom, ktorý by zabezpečoval primeranú ochranu údajov (napr. pred neoprávneným prístupom alebo sprístupnením). Úrad vyhodnotil postup pri doručovaní ako nedostatočne zabezpečený z pohľadu ochrany osobných údajov. Úrad konštatoval porušenie najmä povinností v oblasti bezpečnosti spracúvania (čl. 32 GDPR) a zároveň vytkol aj zodpovednosť prevádzkovateľa za preukázanie súladu. **Poučenie: Aj "bežné" administratívne úkony (ako doručovanie pošty) môžu predstavovať vysoké riziko – ak zásielka obsahuje osobné údaje, prevádzkovateľ musí mať nastavený taký režim doručovania a kontroly, aby vedel preukázať, že údaje sa nedostanú k neoprávnenej osobe.**	**50 000 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
2. Ministerstvo Kultúry	Úrad sa zaoberal prípadom zverejnenia dokumentu na webovom sídle MK SR, konkrétne v časti verejne dostupných dokumentov, kde bol zverejnený Excelový súbor obsahujúci zoznam firiem s vlastníckymi a inými prepojeniami na Ruskú federáciu. Uvedený dokument obsahoval osobné údaje fyzických osôb v rozsahu meno, priezvisko, adresa trvalého pobytu a štátna príslušnosť. Dokument bol na webovom sídle ministerstva verejne dostupný bez akýchkoľvek prístupových obmedzení, a to dlhodobo, pričom sa týkal približne 2 400 dotknutých osôb. Úrad dospel k záveru, že prevádzkovateľ zverejňoval osobné údaje bez splnenia podmienok zákonnosti spracúvania podľa GDPR, čím došlo k porušeniu zásad zákonnosti, transparentnosti a minimalizácie osobných údajov. Rozhodnutie poukazuje na potrebu, aby orgány verejnej moci pri zverejňovaní dokumentov na svojich webových sídlach dôsledne posudzovali rozsah zverejňovaných údajov a uplatňovali zásadu minimalizácie, najmä ak ide o dokumenty sprístupňované širokej verejnosti bez časového alebo technického obmedzenia.	**10 000 eur**
3. ÚPSVaR	Úrad uložil sankciu povinnej osobe – Ústrediu práce, sociálnych vecí a rodiny – za porušenie povinností pri zverejňovaní dokumentov v Centrálnom registri zmlúv (CRZ). V rámci kontroly bolo zistené, že ÚPSVaR dlhodobo a systematicky zverejňoval v CRZ dohody, dodatky a zmluvy obsahujúce osobné údaje fyzických osôb, najmä meno a priezvisko, adresu trvalého pobytu, dátum narodenia, rodné číslo, štátnu príslušnosť, číslo bankového účtu (IBAN) a e-mailovú adresu. Porušenie sa týkalo približne 70 zverejnených dokumentov (najmä dohôd o poskytnutí finančných príspevkov), pričom osobné údaje boli sprístupnené neobmedzenému okruhu osôb. Úrad konštatoval, že dokumenty neboli anonymizované v rozsahu vyžadovanom právnymi predpismi a zásadami ochrany osobných údajov. K porušeniam dochádzalo naprieč viacerými úradmi práce v rámci Slovenskej republiky, čo svedčí o systémovom zlyhaní pri zabezpečení ochrany osobných údajov pri plnení zákonnej povinnosti zverejňovania zmlúv v CRZ.	**6 500 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
4. Ministerstvo vnútra	Úrad rozhodol o porušení zásady zákonnosti pri spracúvaní osobných údajov zo strany Ministerstva vnútra Slovenskej republiky ako prevádzkovateľa informačných systémov Policajného zboru. Porušenie spočívalo v spracúvaní biometrických údajov a genetických údajov fyzickej osoby bez existencie platného právneho základu podľa osobitného predpisu. Policajný zbor odobral dotknutej osobe v trestnom konaní daktyloskopické odtlačky prstov a dlaní, ako aj biologický materiál na účely analýzy DNA. Tieto údaje následne spracúval v informačných systémoch Policajného zboru, konkrétne v systéme AFIS (automatizovaný systém daktyloskopickej identifikácie osôb) a v systéme CODIS (národná databáza profilov DNA). Zároveň bol biologický materiál uchovávaný Kriminalistickým a expertíznym ústavom Policajného zboru. Úrad konštatoval, že spracúvanie týchto osobných údajov nebolo kryté zákonným právnym základom a bolo vykonávané v rozpore so zásadou zákonnosti a so zákonnými podmienkami spracúvania osobných údajov orgánmi činnými v trestnom konaní. Ide o osobitne citlivé údaje, ktorých spracúvanie podlieha prísnym zákonným podmienkam. Ako nápravné opatrenie úrad uložil Ministerstvu vnútra SR povinnosť vymazať daktyloskopické údaje a profil DNA dotknutej osoby z informačných systémov Policajného zboru a zároveň zabezpečiť likvidáciu biologického materiálu, z ktorého bol profil DNA vytvorený.	**2 900 eur**
5. Kriminálny úrad finančnej správy	Úrad konštatoval porušenie zásady transparentnosti a informačnej povinnosti zo strany Finančnej správy SR ako prevádzkovateľa informačného systému CIS, v ktorom sa spracúvajú osobné údaje na účely predchádzania, vyšetrovania a odhaľovania trestnej činnosti. Porušenie sa týkalo obdobia, v ktorom dotknutým osobám neboli pri získavaní ich osobných údajov poskytnuté dostatočné, jasné a úplné informácie o spracúvaní ich údajov. Úrad zistil, že prevádzkovateľ v rozhodnom období neposkytoval dotknutým osobám informácie v rozsahu požadovanom právnymi predpismi, najmä pokiaľ ide o účely spracúvania, právny základ, kategórie príjemcov a dobu uchovávania osobných údajov.	**2 500 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
	Informácie sprístupnené prostredníctvom webového sídla neboli považované za postačujúce, keďže neboli úplné, aktuálne a neposkytovali dotknutým osobám jasný prehľad o ich právach a o podmienkach spracúvania údajov. Zároveň bolo poukázané na to, že informácie o dobe uchovávania osobných údajov musia byť presné a v súlade s platnou právnou úpravou, pričom ich všeobecné alebo nesprávne vymedzenie nie je postačujúce.	
ŠKOLY		
1. ZŠ, ZŠ s MŠ, VŠ	V hodnotenom období boli školám uložené sankcie najmä za porušenia povinností pri spracúvaní osobných údajov. Prevažná väčšina zistených porušení sa týkala opätovného zverejňovania osobných údajov v CRZ, a to v rozsahu presahujúcom zákonné požiadavky. Ďalšou častou oblasťou porušenia bolo zverejňovanie fotografií detí bez preukázateľného súhlasu zákonných zástupcov.	**500 eur - 1 000 eur**
SÚKROMNÉ SPOLOČNOSTI		
1. Fakturačný portál	V dôsledku incidentu došlo k sprístupneniu osobných údajov uložených v databáze aplikácie neoprávneným osobám, pričom incident sa dotkol približne 8 000 až 10 000 klientov. Úrad zistil, že incident bol spôsobený nedostatočnými technickými a organizačnými opatreniami, najmä v oblasti zabezpečenia dostupnosti, integrity a odolnosti informačných systémov. Prevádzkovateľ nevedel preukázať, že prijal primerané bezpečnostné opatrenia zodpovedajúce rizikám spracúvania, a to napriek tomu, že spracúval osobné údaje tisícov používateľov v rámci komerčnej online služby. Úrad zároveň zdôraznil, že ani menší alebo stredný prevádzkovateľ nie je oslobodený od povinnosti aktívne riadiť bezpečnostné riziká pri spracúvaní osobných údajov a zabezpečiť primeranú úroveň ochrany údajov v súlade s článkom 32 GDPR.	**7 500 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
2. Webový portál s nábytkom	právne konanie bolo začaté na základe podnetu, v ktorom podávateľ namietal, že e-shop uchováva osobné údaje zákazníkov 20 rokov od uskutočnenia nákupu. Súčasťou podania bola aj námietka týkajúca sa cookies, ktorá bola postúpená príslušnému orgánu. Úrad zistil, že prevádzkovateľ neposkytoval informácie o spracúvaní osobných údajov jasne a samostatne, ale iba ako súčasť obchodných podmienok, čo nespĺňa požiadavky transparentnosti podľa GDPR. Zároveň zdôraznil, že účtovné povinnosti neodôvodňujú paušálne uchovávanie všetkých osobných údajov po dobu 20 rokov. Prevádzkovateľ opakovane neposkytol požadovanú súčinnosť, za čo mu boli v minulosti uložené poriadkové pokuty.	**5 000 eur**
3. Súkromná spoločnosť	Úrad uložil pokutu súkromnej spoločnosti za porušenie zásady zákonnosti spracúvania osobných údajov, keď bez právneho základu sprístupnila osobné a mzdové údaje 69 zamestnancov odborovej organizácii pôsobiacej u iného zamestnávateľa. Sprístupnené boli údaje v rozsahu meno, priezvisko, osobné číslo a výška mzdy za obdobie rokov 2021 a 2022. Prevádzkovateľ nepreukázal existenciu žiadneho právneho základu podľa čl. 6 ods. 1 GDPR, ktorý by takéto spracúvanie umožňoval. Úrad zároveň uviedol, že odbory sú oprávnené vykonávať kontrolnú činnosť a zamestnávateľ je povinný poskytnúť im údaje o zamestnancoch v rozsahu nevyhnutnom na splnenie tohto účelu. Poskytovanie údajov na tento účel môže byť zákonné na základe právnej povinnosti podľa Zákonníka práce. Zamestnávateľ je však povinný minimalizovať rozsah poskytovaných údajov a zabezpečiť, aby zodpovedali účelu spracúvania. V posudzovanom prípade úrad konštatoval, že namiesto agregovaných alebo anonymizovaných údajov o priemerných mzdách boli odborovej organizácii sprístupnené konkrétne mzdové údaje jednotlivých zamestnancov, čím došlo k neoprávnenému zásahu do ich práv.	**4 500 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

V rozhodovacej činnosti úradu v sledovanom období zároveň výrazne dominovali konania vedené voči obciam a mestám, ktoré tvorili podstatnú časť sankčnej agendy. Ukladané pokuty sa v týchto prípadoch pohybovali prevažne v nižších finančných pásmach, najčastejšie vo výške 300 eur (152 prípadov) a 500 eur (160 prípadov). Menej často boli ukladané pokuty vo výške 700 eur (22 prípadov) a 1 000 eur (25 prípadov), pričom vyššie sankcie sa vyskytovali len ojedinele – 1 500 eur (6 prípadov), 2 500 eur (1 prípad) a 3 000 eur (1 prípad). V jednotlivých prípadoch boli uložené aj pokuty vo výške 600 eur (1 prípad) a 900 eur (1 prípad). Podotýkame, že hodnotíme len pokuty z právoplatných rozhodnutí, ktoré nám boli poskytnuté.

Celková súhrnná výška týchto 511 pokút predstavuje 442 tisíc eur, čo objektívne predstavuje najvyšší ročný výber pokút Úradu za posledných desať rokov. No na druhej strane priemerná pokuta Úradu za rok 2025 vo výške 865 eur je najnižšia za posledných 10 rokov a teda nižšia ako posledné 4 roky pred GDPR.

Rok	Počet zamestnancov	Rozpočet (približne)	Uložené pokuty	Počet pokút so sankciou	Priemerná pokuta
2025	▲ 60	▲ 3,6 milióna eur	▲ 442 tisíc eur	▲ 511	▼ 865 eur
2024	40	1,9 milióna eur neskôr navýšený na 2,9 milióna eur	83 tisíc eur	37	2 243 eur
2023	43	2 milióny eur	94 tisíc eur	46	2 048 eur
2022	44	1,8 milióna eur	61 tisíc eur	52	1 166 eur
2021	45	1,7 milióna eur	110 tisíc eur	53	2 092 eur
2020	50	1,9 milióna eur	103 tisíc eur	54	1 913 eur
2019	50	1,7 milióna eur	75 tisíc eur [2]	9	8 367 eur
2018	42	1,1 milióna eur	132 tisíc eur [3]	38	3 489 eur

ROZHODNUTIA A ČINNOSŤ ÚRADOV

2017	40	1,2 milióna eur	27 tisíc eur	20	1 390 eur
2016	36	1 milión eur	83 tisíc eur	36	2 132 eur
2015	37	0,9 milióna eur	74 tisíc eur	28	2 677 eur

Takisto je zaujímavé porovnať tieto údaje so štatistikami českého úradu:

Rok	Počet zamestnancov	Rozpočet (približne)	Uložené pokuty	Počet pokút	Priemerná pokuta
2024	103	7,6 milióna eur	293 tisíc eur	31	9 459 eur
2023	106	7,6 milióna eur	146 tisíc eur	23	6 350 eur
2022	108	6,3 milióna eur	33 tisíc eur	30	1 100 eur
2021	105	7,1 milióna eur	148 tisíc eur	40	3 700 eur
2020	105	7,2 milióna eur	n/a	n/a	n/a
2019	103	7 miliónov eur	n/a	n/a	n/a

Z pohľadu štatistík je rok 2025 zaujímavý najmä tým, že Úrad pokračoval v trende posilňovania svojich kapacít – a to personálne aj finančne. Jeho rozpočet stúpol na rekordných 3,6 milióna eur, čo sa prejavilo na rekordnom počte zamestnancov.

Pri personálnych zmenách je potrebné spomenúť, že na poste predsedu odboru správnych konaní po dlhých rokoch skončil Juraj Mičura. Za predsedu Úradu ho v roku 2022 vybrala vláda Eduarda Hegera, no jeho voľba napokon neprešla parlamentom. Práve personálna pod-dimenzovanosť a preťaženie tohto kľúčového odboru (ktorý udeľuje pokuty) bola v minulosti skloňovaná s organizačnými problémami Úradu. Dôvody tejto dôležitej personálnej zmeny nie sú jasné. V situácii, kedy panuje nedostatok odborného personálu v tejto oblasti, na ktorí sa sťažujú klienti, ale aj orgány verejnej moci, hrozí, že skúsený personál je bude nahrádzaný ľuďmi, ktorí nemajú v tejto oblasti históriu a skúsenosť. Personálne zmeny na vedúcich pozíciách kľúčových odborov nie sú podľa nás dobrým signálom.

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Paradoxom však je, že napriek tomu, že v roku 2025 stúpol nielen počet zamestnancov a rozpočet, ale aj celková suma uložených pokút a celková vyzbieraná suma pokút, priemerná výška pokuty medziročne klesla.

Dôvod je pomerne prozaický: kým v predchádzajúcom roku Úrad uložil spolu približne 48 pokút, v roku 2025 ich uložil už takmer 500.

Inými slovami – Úrad sa zjavne posunul od menšieho počtu individuálne „ťažkých" prípadov k modelu masívnejšieho postihovania vo väčšom objeme, čo síce zvyšuje štatistický počet sankcií, ale zároveň rozrieďuje priemernú výšku pokuty.
Tento trend môže mať v praxi dva protichodné efekty. Na jednej strane je vyšší počet sankcií signálom, že Úrad chce byť aktívnejší a viditeľnejší. Na druhej strane však z pohľadu prevádzkovateľov nie je smerodajné len to, koľko pokút sa „urobí do štatistiky", ale najmä to, či rozhodnutia prinášajú konzistentné pravidlá, predvídateľné záväzné závery a systematickú metodickú činnosť. A práve táto časť z pohľadu trhu stále zaostáva.

Ďalšia činnosť Úradu

Popri kontrolnej a rozhodovacej činnosti sa Úrad v roku 2025 venoval aj viacerým aktivitám v oblasti metodického usmerňovania, osvety a verejnej komunikácie, ktoré reagovali na aktuálne technologické a spoločenské výzvy v oblasti ochrany súkromia.

Upozornenie na prenos osobných údajov používateľov TikTok do tretích krajín
V decembri 2025 Úrad verejne upozornil na pretrvávajúci prenos osobných údajov používateľov platformy TikTok do tretích krajín, vrátane Číny. Upozornenie nadväzovalo na cezhraničné vyšetrovanie vedené írskym dozorným orgánom (DPC), ktoré dospelo k záveru, že prenos osobných údajov z EHP do Číny je v rozpore s GDPR a má byť ukončený.
Úrad zdôraznil riziká spojené s prenosom osobných údajov do krajín bez rovnocennej úrovne ochrany a apeloval na používateľov, aby venovali zvýšenú pozornosť nastaveniam súkromia. Osobitne upozornil aj verejné inštitúcie na potrebu zodpovedného posúdenia používania tejto platformy z pohľadu ochrany osobných údajov.

Osvetová a vysvetľujúca činnosť – rozhovor predsedníčky Úradu
V priebehu roka Úrad posilnil aj svoju osvetovú úlohu, čo ilustruje rozsiahly verejný rozhovor predsedníčky Úradu, zameraný na praktické otázky ochrany osobných údajov. Úrad v ňom vysvetľoval základné pojmy (čo je osobný údaj, ktoré údaje sú najrizikovejšie), najčastejšie pochybenia v praxi (zverejňovanie rodných čísel, nedostatočné bezpečnostné opatrenia, kamerové systémy, marketing) a upozorňoval na rastúce riziká spojené s využívaním umelej inteligencie, biometrických technológií a deepfake obsahu.

Zároveň Úrad zdôraznil význam práv dotknutých osôb, možnosti obrany pri podozrení na porušenie ochrany osobných údajov a potrebu systematického prístupu prevádzkovateľov k ochrane súkromia ako súčasti ich dôveryhodnosti a reputácie.
Hoci Úrad v roku 2025 zvýšil viditeľnosť svojej osvetovej a komunikačnej činnosti, jej praktický prínos pre prevádzkovateľov zostáva limitovaný. Verejné upozornenia a mediálne výstupy síce pomenúvajú riziká, no len zriedkavo prinášajú konkrétne metodické usmernenia, ktoré by umožnili predvídateľné a jednotné nastavenie praxe. Práve v tejto oblasti má Úrad stále výrazný priestor na zlepšenie.

Činnosť Úradu pre reguláciu v zmysle nového ZEK

Aj v roku 2025 sme sa v rámci našej analytickej činnosti zamerali na preskúmanie stavu konaní a rozhodovacej praxe Úradu pre reguláciu elektronických komunikácií a poštových služieb („Úrad pre reguláciu") v nadväznosti na zákon o elektronických komunikáciách („ZEK"), so zvláštnym dôrazom na oblasť ochrany súkromia a osobných údajov.

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Pozornosť sme venovali najmä ustanoveniam § 109 ZEK (cookies a podobné technológie) a § 116 ZEK (nevyžiadaná komunikácia a priamy marketing), ktoré dlhodobo predstavujú najexponovanejšie časti ZEK z pohľadu kontrolnej a sankčnej činnosti Úradu.

Na základe informácií sprístupnených podľa zákona o slobodnom prístupe k informáciám sú k roku 2025 k dispozícii nasledujúce údaje:

Ustanovenie ZEK	Počet sťažností	Prebiehajúce konania	Právoplatné rozhodnutia	Priemerná pokuta	Celkové pokuty
§ 109 ods. 8 ("cookies")	8	5 správnych konaní + 3 kontroly	75	1 147 eur	86 050 eur
§ 116 ("marketing")	416	12 správnych konaní + 62 kontrol	22	7 022 eur	154 500 eur

V rámci rozhodnutí týkajúcich sa porušenia § 109 Úrad na reguláciu skúmal cookies a ich nasadenie na webstránkach, pričom najčastejšie porušenia predstavovali opäť, ako každoročne ukladanie cookies bez súhlasu, neumožnenie odmietnuť všetky cookies rovnako jednoducho ako ich prijať, vopred zaškrtnuté iné ako nevyhnutné cookies a pod.

Na účely tejto správy a pre porovnanie oboch úradov, sme – obdobne ako pri Úrade, zhromaždili a vyhodnotili základné štatistické údaje o činnosti Úradu pre reguláciu, ktoré sa týkajú jeho personálnych kapacít, rozpočtu a sankčnej činnosti v oblasti ochrany súkromia a osobných údajov podľa zákona o elektronických komunikáciách.

Rozhodnutia týkajúce sa nevyžiadanej komunikácie

V nasledujúcej tabuľke sme spracovali právoplatné rozhodnutia Úradu pre reguláciu, ktoré boli z hľadiska pokút o niečo pestrejšie.

Účastník konania	Zhrnutie rozhodnutia	Pokuta
1. Poisťovňa	Úrad na reguláciu vykonal kontrolu poisťovne na základe podnetu poistenca, ktorý namietal nevyžiadanú e-mailovú komunikáciu a požadoval, aby ho poisťovňa ďalej nekontaktovala. Kontrola sa zamerala na tzv. „welcome pack", teda sériu siedmich e-mailov zasielaných novým poistencom, ktorých obsahom bola prezentácia benefitov, mobilnej aplikácie a ďalších služieb poisťovne.	**75 000 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
	Úrad dospel k záveru, že ide o e-mailový priamy marketing, ktorý bol zasielaný bez splnenia zákonných podmienok. Porušenie sa týkalo celkovo 24 313 dotknutých osôb. Poisťovňa podľa úradu nepreukázala existenciu platného súhlasu so zasielaním marketingových e-mailov (§ 116 ods. 3 ZEK) a zároveň neumožnila jednoduché a bezplatné odmietnutie ďalšej komunikácie (opt-out) v súlade s § 116 ods. 15 ZEK. V rozkladovom konaní poisťovňa argumentovala, že ide o servisné informácie vo verejnom záujme, nie o marketingovú komunikáciu, a odkazovala aj na usmernenia EDPB a britského ICO. Úrad však túto argumentáciu neakceptoval a zdôraznil, že komunikácia propagujúca benefity alebo služby má povahu priameho marketingu, a to bez ohľadu na jej označenie ako „welcome" alebo „onboarding". **Poučenie:** **„Welcome pack" a onboardingová komunikácia nie sú automaticky považované za servisné správy. Ak e-mail propaguje benefity alebo služby, ide o priamy marketing, ktorý vyžaduje platný právny základ. Aj pri uplatnení výnimky pre „vlastné podobné služby" musí mať príjemca pri každej správe možnosť jednoduchého a bezplatného odhlásenia.**	
2. Telekomunikačný operátor	Úrad na reguláciu vykonal kontrolu telekomunikačného operátora v súvislosti so zasielaním marketingových e-mailov účastníkom elektronických komunikačných služieb. Operátor zasielal marketingové správy celkovo 16 842 osobám, avšak v jednotlivých e-mailoch neposkytol možnosť jednoducho a bezplatne odmietnuť ďalšiu marketingovú komunikáciu. Úrad zistil porušenie § 116 ods. 15 zákona o elektronických komunikáciách, keďže v marketingových e-mailoch chýbal priame dostupný opt-out mechanizmus (napr. odhlasovací link typu „unsubscribe"). **Poučenie:** **Opt-out musí byť „jednoduchý" a priamo dostupný v každej marketingovej správe. Odkaz na call centrum alebo všeobecnú e-mailovú adresu nie je postačujúci, a to ani v prípade nízkeho počtu sťažností.**	**50 000 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
3. Telemarketingový subjekt / agent	Úrad na reguláciu začal konanie z vlastného podnetu na základe viacerých oznámení občanov podaných prostredníctvom platformy na hlásenie nevyžiadaných volaní. Predmetom kontroly bol telemarketing poisťovacích produktov realizovaný telefonicky. Úrad zistil, že prevádzkovateľ vykonal marketingové volanie osobe, ktorá mala telefónne číslo účinne zaregistrované v zozname „nekontaktovať" (DNC register), a to napriek tomu, že registrácia bola platná už od 1. 7. 2023. Zároveň bolo preukázané, že telemarketingové volania neboli realizované z čísla s vyhradeným prefixom (0)888, ale z bežného telefónneho čísla. Subjekt namietal, že volania boli uskutočnené na základe výnimky z predchádzajúceho súhlasu, keďže dotknutá osoba mala vzťah k telekomunikačnému operátorovi a marketingový súhlas. Úrad však túto argumentáciu odmietol s tým, že poisťovacie produkty nemožno považovať za „podobné služby" k telekomunikačným službám, a výnimku marketingu vlastných podobných služieb tak nie je možné automaticky uplatniť. **Poučenie:** **Telemarketing nemožno vykonávať voči osobám zapísaným v DNC registri a musí byť realizovaný výlučne z čísiel s vyhradeným prefixom (0)888. Výnimka „marketing vlastných podobných služieb" sa uplatňuje striktne a nemožno ju rozširovať na iné odvetvia, ako sú poisťovacie produkty.**	**8 000 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Rozhodnutia týkajúce sa "cookies"

V nasledujúcej tabuľke sme spracovali najrelevantnejšie rozhodnutia v zmysle § 109 ods. 8 ZEK, pričom podstata týchto rozhodnutí spočívala v ukladaní nepovinných cookies alebo zle nastavenej cookie lišty.

Účastník konania	Zhrnutie rozhodnutia	Pokuta
1. E-shop	Úrad na reguláciu vykonal kontrolu webovej stránky e-shopu so športovým oblečením, ktorý ukladal do zariadení používateľov iné ako technicky nevyhnutné cookies ešte pred udelením súhlasu prostredníctvom cookie lišty. Išlo najmä o cookies nástrojov Microsoft Clarity, Bing/Microsoft marketing a Google Analytics, spolu približne 10 cookies. Úrad zdôraznil, že rozhodujúci je moment uloženia cookies – ak sú uložené ešte pred udelením súhlasu, porušenie je naplnené, bez ohľadu na neskorú nápravu. Závažnosť porušenia spočívala v počte použitých cookies a v zásahu do súkromia neurčitého okruhu návštevníkov webu, ktorý už nemožno spätne napraviť.	**6 000 eur**
2. Web potravinového reťazca	Úrad na reguláciu vykonal administratívnu kontrolu webového sídla potravinového reťazca, pri ktorej zistil, že v dňoch 9. – 10. septembra 2024 boli do zariadení používateľov ukladané iné ako nevyhnutné cookies ešte pred udelením súhlasu prostredníctvom cookie lišty. Išlo najmä o analytické cookies (_ga, _ga_LVZ68HZ4ZX, _ga_8C9TRZ2NBQ) a marketingovú cookie _gcl_au určenú na reklamnú atribúciu konverzií. Porušenie bolo preukázané prostredníctvom nástroja Website Evidence Collector, ktorý zaznamenal ukladanie cookies pred vyjadrením súhlasu. Úrad zároveň konštatoval, že cookie lišta webu uvádzala zavádzajúcu informáciu, podľa ktorej stránka používala iba technické cookies, hoci v skutočnosti dochádzalo aj k analytickému a marketingovému spracúvaniu. Úrad zdôraznil, že súhlas s cookies musí byť preukázateľný a spĺňať podmienky GDPR, najmä slobodnosť, konkrétnosť, informovanosť a jednoznačnosť, a že analytické ani marketingové cookies nemožno považovať za nevyhnutné.	**5 000 eur**

ROZHODNUTIA A ČINNOSŤ ÚRADOV

Účastník konania	Zhrnutie rozhodnutia	Pokuta
3. E-shop	Úrad vykonal administratívnu kontrolu webovej stránky e-shopu s bytovými doplnkami, pri ktorej zistil, že v dňoch 21. – 22. augusta 2024 boli do koncových zariadení používateľov ukladané iné ako technické cookies ešte pred udelením súhlasu prostredníctvom cookie lišty. Išlo najmä o analytické a marketingové cookies nástrojov Google Analytics, Facebook a Hotjar. Prevádzkovateľ na výzvy úradu nereagoval, zistené nedostatky neodstránil ani po nariadení a počas konania sa procesne nebránil. K náprave došlo až dodatočne, po márnom uplynutí zákonných lehôt. V rozkladovom konaní prevádzkovateľ argumentoval neúmyselným pochybením, technickými a organizačnými problémami a následnou nápravou, pričom žiadal o zníženie sankcie. Úrad tieto argumenty neakceptoval a rozklad v celom rozsahu zamietol.	**3 700 eur**

JUDIKATÚRA

Ani v roku 2025 sme v rámci rozhodovacej činnosti všeobecných súdov na Slovensku nezaznamenali judikát, ktorý by zásadným spôsobom posúval výklad GDPR alebo vnútroštátnej úpravy ochrany osobných údajov. Tento stav naďalej súvisí s problematickou dostupnosťou rozhodnutí a absenciou systematického a uceleného sprístupňovania judikatúry v tejto oblasti. Takisto s tým, že len malé percento rozhodnutí Úradu je napadnuté správnymi žalobami. Významnejší vývoj však možno sledovať na úrovni rozhodovacej praxe Súdneho dvora Európskej únie („SDEÚ"). V roku 2025 SDEÚ priniesol viacero rozhodnutí, ktoré precizujú výklad kľúčových pojmov GDPR a sú relevantné aj pre aplikačnú prax na Slovensku.

Rozhodnutie SD EÚ – prenos pseudonymizovaných údajov tretím stranám (C-413/23)

Predmetom rozhodnutia Súdneho dvora Európskej únie bolo upresnenie pojmu „osobné údaje" v kontexte prenosu pseudonymizovaných údajov tretím stranám a rozsahu informačných povinností prevádzkovateľa. Spor vznikol v súvislosti s postupom Jednotnej rady pre riešenie krízových situácií (SRB), ktorá v rámci riešenia situácie banky Banco Popular umožnila bývalým akcionárom a veriteľom predkladať pripomienky k predbežnému rozhodnutiu o náhrade škody. Tieto pripomienky SRB následne v pseudonymizovanej podobe postúpila externej spoločnosti Deloitte, ktorá bola poverená vypracovaním hodnotenia dopadov riešenia banky.

Dotknuté osoby podali sťažnosť na Európskeho dozorného úradníka pre ochranu údajov (EDPS), keďže neboli informované o prenose ich údajov tretej strane. EDPS dospel k záveru, že došlo k porušeniu informačnej povinnosti podľa nariadenia (EÚ) 2018/1725. Všeobecný súd rozhodnutie EDPS čiastočne zrušil, avšak SDEÚ tento rozsudok zrušil a potvrdil právne závery EDPS.

SDEÚ v prvom rade zdôraznil, že vyjadrenie osobného názoru predstavuje samo o sebe osobný údaj, keďže je neoddeliteľne späté s osobou, ktorá ho vyjadrila. Na jeho kvalifikáciu ako osobného údaja nie je potrebné skúmať obsah, účel ani dôsledky tohto názoru. Zároveň súd potvrdil, že pseudonymizované údaje nemožno automaticky a za každých okolností považovať za osobné údaje – pseudonymizácia môže v určitých situáciách účinne zabrániť identifikácii dotknutej osoby zo strany príjemcu údajov.

Za kľúčové však SDEÚ považoval posúdenie identifikovateľnosti osoby z pohľadu prevádzkovateľa a v momente zberu údajov, nie z pohľadu príjemcu po ich prenose. Informačná povinnosť prevádzkovateľa preto vzniká už pri zbere údajov a nemožno ju obchádzať tým, že údaje budú pred prenosom pseudonymizované. Skutočnosť, že tretia strana nemusí byť schopná dotknutú osobu identifikovať, nemá vplyv na povinnosť prevádzkovateľa informovať o prenose osobných údajov.

Používanie telových kamier pri kontrole cestujúcich a informačná povinnosť podľa GDPR (C-422/24)

Predmetom rozhodnutia Súdneho dvora Európskej únie bolo posúdenie rozsahu a spôsobu plnenia informačnej povinnosti podľa GDPR pri použití telových kamier (body cameras) počas kontroly cestovných lístkov v prostriedkoch verejnej dopravy. Spor vznikol v súvislosti s praxou dopravnej spoločnosti v Štokholme, ktorá vybavila svojich revízorov telovými kamerami zaznamenávajúcimi cestujúcich počas kontroly.

Švédsky dozorný orgán pre ochranu osobných údajov uložil dopravnej spoločnosti pokutu za porušenie viacerých ustanovení GDPR, najmä z dôvodu nedostatočného informovania dotknutých osôb o spracúvaní ich osobných údajov. Spoločnosť namietala, že osobné údaje neboli získavané priamo od cestujúcich, ale nepriamo, čo by malo vplyv na rozsah a načasovanie informačnej povinnosti, a preto považovala uloženú pokutu za neopodstatnenú.

Súdny dvor EÚ konštatoval, že údaje získané prostredníctvom telových kamier sa považujú za osobné údaje získané priamo od dotknutej osoby (čl. 13 GDPR). Na takúto kvalifikáciu nie je potrebné, aby dotknutá osoba vedome poskytla údaje alebo vykonala akýkoľvek aktívny úkon. Samotné pozorovanie osoby a zaznamenávanie jej správania kamerou predstavuje priamy zber osobných údajov. Nepriamy zber údajov (čl. 14) sa uplatní len v prípadoch, keď prevádzkovateľ získava údaje z iného zdroja bez priameho kontaktu s dotknutou osobou.

JUDIKATÚRA

V prípade priameho zberu osobných údajov vzniká prevádzkovateľovi povinnosť poskytnúť dotknutej osobe určité informácie okamžite. Súd zároveň potvrdil, že informačnú povinnosť je možné splniť prostredníctvom viacvrstvového (multi-layered) prístupu. Najdôležitejšie informácie môžu byť uvedené napríklad na viditeľnom výstražnom označení (oznámení o používaní kamier), zatiaľ čo ďalšie povinné informácie môžu byť sprístupnené primeraným a úplným spôsobom na ľahko dostupnom mieste.

Rozhodnutie potvrdzuje prísny výklad pojmu „priamy zber osobných údajov" a kladie dôraz na bezprostredné a transparentné informovanie dotknutých osôb pri využívaní kamerových technológií vo verejnom priestore. Zároveň poskytuje prevádzkovateľom praktický návod, ako možno informačnú povinnosť plniť primerane aj v dynamických situáciách, akými sú kontroly vo verejnej doprave.

Rozhodnutie SDEÚ vo veci C492/23 - postavenie online platforiem ako prevádzkovateľov osobných údajov

Spor vznikol v súvislosti s fungovaním online trhoviska pôsobiaceho v Rumunsku, ktoré umožňovalo používateľom zverejňovať inzeráty. Na platforme bol zverejnený inzerát obsahujúci fotografie a telefónne číslo ženy, ktorý bez jej súhlasu nepravdivo naznačoval poskytovanie sexuálnych služieb. Inzerát obsahoval osobitné kategórie osobných údajov a predstavoval zásah do jej súkromia, cti a osobnej integrity. Hoci prevádzkovateľ platformy po upozornení inzerát odstránil, jeho obsah sa následne rozšíril na ďalšie webové stránky. Dotknutá osoba sa domáhala náhrady nemajetkovej ujmy z dôvodu nezákonného spracúvania osobných údajov.

Vnútroštátny súd sa obrátil na SDEÚ s otázkou, či je prevádzkovateľ online trhoviska možné považovať za prevádzkovateľa osobných údajov podľa GDPR, a to aj v prípade, ak samotný obsah inzerátov nevytvára, a či sa môže dovolávať výnimiek zo zodpovednosti podľa smernice o elektronickom obchode. Zároveň sa riešilo, či platformy majú povinnosť proaktívne preverovať obsah inzerátov, overovať totožnosť inzerentov a zabraňovať zverejňovaniu citlivých osobných údajov.

Súdny dvor konštatoval, že online trhovisko môže mať postavenie prevádzkovateľa osobných údajov v zmysle GDPR, pokiaľ určuje účely a prostriedky spracúvania. Takéto postavenie vzniká najmä v prípadoch, keď platforma inzeráty štruktúruje, kategorizuje, speňažuje, technicky spracúva alebo si v zmluvných podmienkach vyhradzuje práva na ich ďalšie použitie. Skutočnosť, že osobné údaje poskytol používateľ, nezbavuje platformu zodpovednosti, ak má rozhodujúci vplyv na spôsob ich spracúvania.

SDEÚ zároveň výslovne potvrdil, že výnimky zo zodpovednosti poskytovateľov hostingu podľa smernice o elektronickom obchode nepredstavujú „bezpečný prístav" vo vzťahu k povinnostiam podľa GDPR. Aj keď sa platforma môže vyhnúť zodpovednosti za nezákonný obsah tretích strán z pohľadu občianskoprávnej zodpovednosti, nemôže sa týmto spôsobom zbaviť povinností prevádzkovateľa osobných údajov, vrátane povinností zákonnosti, transparentnosti a bezpečnosti spracúvania.

Rozsudok ide nad rámec tradičného modelu „oznámenie a odstránenie" a ukladá online trhoviskám proaktívne povinnosti v oblasti ochrany osobných údajov. Súdny dvor zdôraznil povinnosť preverovať, či inzeráty neobsahujú osobitné kategórie osobných údajov podľa článku 9 GDPR, najmä údaje o sexuálnom živote alebo sexuálnej orientácii, a povinnosť overiť, či má inzerent zákonný právny základ na zverejnenie takýchto údajov, vrátane súhlasu dotknutej osoby. Ak takýto právny základ neexistuje, inzerát nesmie byť zverejnený.

V oblasti bezpečnosti spracúvania SDEÚ poukázal na článok 32 GDPR a zdôraznil povinnosť zaviesť primerané technické a organizačné opatrenia na zabránenie nezákonnému kopírovaniu, scrapovaniu a ďalšiemu šíreniu inzerátov. Takéto opatrenia môžu zahŕňať technológie proti automatizovanému sťahovaniu obsahu, vodoznaky, obmedzenia prístupu alebo zmluvné ochranné mechanizmy.

JUDIKATÚRA

Rozhodnutie predstavuje zásadný posun v chápaní zodpovednosti online platforiem v EÚ. Činnosti, ktoré boli doteraz považované za sprievodné alebo technické, môžu viesť k vzniku postavenia prevádzkovateľa podľa GDPR. Pre mnohé platformy to znamená prechod od reaktívneho k preventívnemu modelu súladu, s dôrazom na kontrolu obsahu pred jeho zverejnením a na posilnenie interných procesov ochrany osobných údajov.
Rozsudok zapadá do širšieho regulačného rámca EÚ, najmä v kontexte aktu o digitálnych službách a pripravovaného aktu o umelej inteligencii, a potvrdzuje trend smerujúci k vyššej zodpovednosti platforiem za ochranu základných práv jednotlivcov v digitálnom prostredí.

ZHRNUTIE

Pri hodnotení roka si – už tradične – vyberáme jeden pozitívny a jeden negatívny moment, ktoré podľa nás najviac vystihujú, kam sa ochrana osobných údajov na Slovensku za uplynulý rok posunula.

Pozitívny moment roka 2025:

Za pozitívny moment roka 2025 považujeme skutočnosť, že Úrad považuje za potrebné zrušiť nepotrebnú a zmätočnú druhú časť aktuálneho zákona o ochrane osobných údajov. Táto druhá časť zákona sa vzťahuje na spracúvanie osobných údajov, ktoré je vykonávané mimo pôsobnosti práva Únie. Podľa nášho názoru v praxi k takým prípadom takmer nikdy nedochádza. Táto druhá časť zákona spôsobuje, že mnohé subjekty dodnes nesprávne odkazujú na paragrafové znenie zákona namiesto článkov GDPR. Je pozitívum návrhu nového zákona o ochrane osobných údajov, že túto dvojkoľajnosť má za cieľ odstrániť.

Negatívny moment roka 2025:

Za negatívny moment roka považujeme rozhodovaciu činnosť Úradu. 96 percent všetkých pokút udelených Úradom v roku 2025 sa týkalo tej istej veci – zverejnenia rodného čísla v povinne zverejňovaných zmluvách. Prirodzene, najviac pokutovaným subjektom sú potom obce, mestá a VÚC, ktorým Úrad udelil až 382 pokút a ďalších 75 pokút udelil Úrad iných orgánom verejnej moci. Všetko vo vzťahu k zverejneniu rodného čísla. Pritom je potrebné dodať, že ide o rozhodnutia Úradu z vlastného podnetu, nie na návrh dotknutých osôb. Úrad sa teda sám rozhodol začať tieto konania. Celkovo tak bolo vedených k týmto prípadom 490 samostatných správnych konaní a spisov. Skutočné číslo je zrejme vyššie, pretože niektoré zrejme nenadobudli právoplatnosť v roku 2025.

Len 24 pokút v celkovej výške približne 45 tisíc eur udelil Úrad v roku 2025 obchodným spoločnostiam. Priemerná pokuta pre obchodnú spoločnosť bola preto na úrovni 1,883 eur.

Pokuty majú byť podľa čl. 83 GDPR účinné, primerané a odrádzajúce. Každý dozorný orgán má tieto základné úlohy podľa čl. 57 GDPR:

- monitoruje a presadzuje uplatňovanie GDPR;
- zvyšuje povedomie verejnosti a jej chápanie rizík, pravidiel, záruk a práv súvisiacich so spracúvaním;
- osobitnú pozornosť má venovať činnostiam špecificky zameraným na deti;
- zvyšuje povedomie prevádzkovateľov a sprostredkovateľov o ich povinnostiach podľa GDPR.

Odpovedzte si sami, čo z toho pomáha napĺňať vyššie uvedená rozhodovacia prax?

Zverejnenie rodného čísla je zakázané zákonom. Nie je cieľom našej správy tieto porušenia ani dané pravidlo nijako bagatelizovať. Ale skutočnosť je, ide o veľmi jednoduché pravidlo, ktoré má čisto národný charakter (nezakazuje ho GDPR). Navyše je zrejmé, že týmto porušeniam je možné predísť aj technickým riešením alebo nastavením registra, na ktoré sa rozhodnutia nezameriavajú.

Ak sa Úrad rozhodne týmto spôsobom svoju rozhodovaciu prax za celý rok venovať výlučne len jednému jednoduchému pravidlu, a to z vlastného podnetu, odborná aj laická verejnosť by sa mala pýtať prečo.

Aký je rozumný dôvod takéhoto výlučného zamerania pokút v priebehu jedného roka? Prečo vôbec táto anomália vznikla? A aký bude mať táto činnosť regulátora dopad na trh, výklad pravidiel a vývoj tejto oblasti? A čo táto činnosť regulátora stála daňových poplatníkov?

V Bratislave, dňa 28. januára 2026
Dagital Legal, s.r.o.